HACKERS' WARS

How the FBI, Pentagon, NATO and technologists staged the Arab Spring and resulting coups and wars

Or, How I Learned to Worry and Stop Loving the Arab Spring:

an argument in favor of cyber realism

by Joanna Bell, M.A. Near Eastern Languages and Cultures

Photograph on cover page taken by author in 2008.

*This book is dedicated to the goal of anticipating, avoiding, and alleviating crises.**

* Written by Herman Kahn on June 10, 1960 in his Preface to *On Thermonuclear War*

When Disraeli said in his novel *Tancred* that the East was a career, he meant that to be interested in the East was something bright young Westerners would find to be an all consuming passion; he should not be interpreted as saying that the East was only a career for Westerners.

Edward W. Said, *Orientalism*

… Their words were strong and bitter, full of frustration and anger.

“Change the station. Let’s hear the news. Gag that woman who’s singing!”

The owner reached up to tune the knob. But he did not forget to answer the man who had spoken.

“The news? You don’t know any more about politics than your good-for-nothing father did.”

“I want to find out, idiot. Are we going to go on being donkeys for the rest of our lives?”

The solemn tones of the newscaster clashed with the unabated din. No one seemed to be listening. But an occasional comment here and there revealed that the men were following what was being said.

“Sir… arrived today at Cairo Airport.”
“What does he want, that son of a bitch?”
“If I had been there I would have spat in his face and sent him home.”

Abdel-Aziz found himself speaking, quietly at first, but then excitedly at the top of his voice. As the broadcast continued its struggle with the boisterous voices of the men, his excitement increased. Everyone was talking. Someone would remark on what he had said, and he would come back with an answer or a new opinion. The room was a confused uproar of arguments, laughter, and insults.

He lost himself among them. He felt the same bitterness, anger, and pain that they did. The harsh phrases kept coming. His forehead was covered with sweat. Someone handed him a water pipe. He filled his lungs with the thick, rich smoke. It went to his head immediately. He became dizzy and coughed. But he went on talking, and he kept going back to the pipe. The taste was extraordinary, like a hundred cigarettes in a single breath. Only that heavy blue smoke could interrupt the incessant storm of his words.

THE END

Abdel-Hakim Qassem, *The Seven Days of Man* (*Ayyām al-insān al-sab’a*), 1969

ACKNOWLEDGEMENTS

This paper is several years delayed in being written. I began the research process in 2015 as an idea for a possible Ph.D. dissertation topic while living in Washington, D.C. My research included looking at material from the hacking group Anonymous on social media, attending a conference held by the US State Department on the Georgetown University campus in July 2016 titled “Threats to Religious and Ethnic Minorities Under the Islamic State”, & making contact with a former employer who served as a White House advisor on the Middle East under George W. Bush.

By the end of summer 2016, after less than a year researching the topic of US involvement in the Arab Spring, I had received threats at my home and was under heavy cyber surveillance.

Unwilling to let my efforts go to waste, I have produced this paper from that research. This research was produced freely for free, under no auspices of any institution or individual, and can be shared freely for free with proper attribution to the author.

Table of Contents

ABSTRACT

Draft of a working paper arguing that the Arab Spring and its resulting coups and wars across the Middle East were orchestrated by US law enforcement, intelligence, and the military establishment with the willing and knowing cooperation of hacker groups like Anonymous, big technology companies, major media outlets and major policy institutions.

Hackers' wars are information operations[1] incorporating electronic warfare operations[2] conducted by a state which deliberately involve populations to effect war, coup, or other policy objectives that create the conditions of civil strife. These operations are typically carried out as wargames before or simultaneously with the execution of the real-world operation. The most salient features of hackers' wars are propaganda efforts, surveillance, cyberespionage and hacking, electronic weaponry deployment, and, importantly, the misattribution of these cyber coercion and deterrence techniques. The role of cyberweaponry is most saliently concealed in hackers' wars because information operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not "considered an armed attack under international law" or "an act of war". As professor of strategy Sean McFate has put it, "irregular warfare manufactures the fog of war" present in wars of armed conflict. In short, **hackers' wars are the wars brought about by hackers.** The Arab Spring is addressed as hackers' wars in this present study.

This study looks at current events, social media, scholarly publications, cyber technology, and media trends, adapting an approach of cyber realism to the Arab Spring conversation within Max Weber's political theory of monopolies on violence and legitimate infringements. This approach emphasizes technical aspects and larger trends in cyber-politics, current events as products of the US wargame and intelligence industries, and Clausewitz's social structure of war triad in political science theory (identifying those with end-to-end control of the popular passions, operational instruments, and policy decisions of war). All of these aspects are considered in order to give this essay 'teeth' and give a timely answer to the current international security crises of media revolutions and cyberterrorism.

---

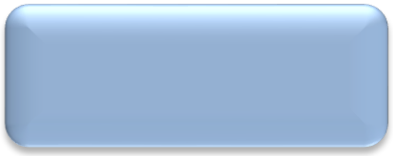
[1] From Congressional Research Service *Defense Primer: Information Operations*: While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations… which include computer network attack, computer network defense, and computer network exploitation; psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC).

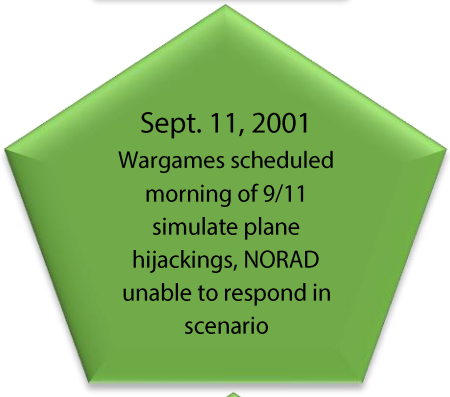
[2] From Congressional Research Service *Defense Primer: Electronic Warfare*: Electronic warfare (EW), as defined by the Department of Defense (DOD), are military activities that use electromagnetic energy to control the electromagnetic spectrum ("the spectrum") and attack an enemy… Applications include radio frequencies to communicate with friendly forces; microwaves for tactical data-links, radars, and satellite communications; infrared for intelligence and to target enemies; and lasers across the entire spectrum to communicate, transmit data, and potentially destroy a target.

Hacktivist Action

Big Tech Action

Government Action





HACKERS' WARS
How the FBI, Pentagon, NATO and technologists staged the Arab Spring and resulting coups and wars

Mar. 2003
US invades Iraq on premise it has weapons of mass destruction

Jan. 2007
US begins bombing Al-Shabab in Somalia

2008 - 2011
Facebook, Google, MTV & US NGOs begin training Arab protesters in social media protest methods

Nov. 2008
National Intel. Council report predicts emergence of coronavirus pandemic by 2025 will kill hundreds of millions worldwide

2009
Hackers use Iranian proxies to join Iranian social media protests

2009
Iran election protests coordinate via social media; Electronic Frontier Foundation crowd sources US hacking of Iranian social media accounts

Mid- 2010
Google Exec. Wael Ghonim creates "We Are All Khalid Said" Facebook page & gains large Egyptian following

Late 2000s
Ret. Army officer witnesses RAND Corp. plans to flood Arab social media with 'democracy' & 'revolution' tags

Dec. 2010
Anonymous given IRC #InternetFeds, chat focuses on revolution in Middle East

Dec. 2010
FBI uses Anonymous asset to start chat on Occupy Wall Street movement

Dec. 9, 2010
Anonymous IRCs & bot armies disappear after plans to hack Amazon.com

Jan. 2011
Anonymous reconnects Arab Spring protesters' Internet after gov'ts shut it down, stages Occupy Wall Street protests

Jan. 2011
Arab Spring protests break out coordinated via social media; Google Exec. Ghonim publicly attends Egyptian protests

Jan. 14, 2011
Tunisian revolution coordinated via social media leads to President Ben Ali's resignation

Feb. 2011
Egyptian revolution coordinated via social media leads to President Mubarak's resignation; Revolution via social media breaks out in Libya

Mar. 2011
NATO invades Libya; US backs rebels as Syrian War begins

July 8-9, 2011
UN peacekeepers enter south Sudan 1 day before the Sudan partitions into South Sudan and Sudan

Oct., Dec. 2011
UN & NATO-backed Libyan forces capture and kill Gaddafi ; US withdraws from Iraq

2012 - 2013
Former CIA officer and NSA contractor Snowden gives classified files to journalist Glen Greenwald

Mar. 2013
Saudi prince Salman bin Sultan & NSA direct Syrian rebels to 'flatten' Damascus

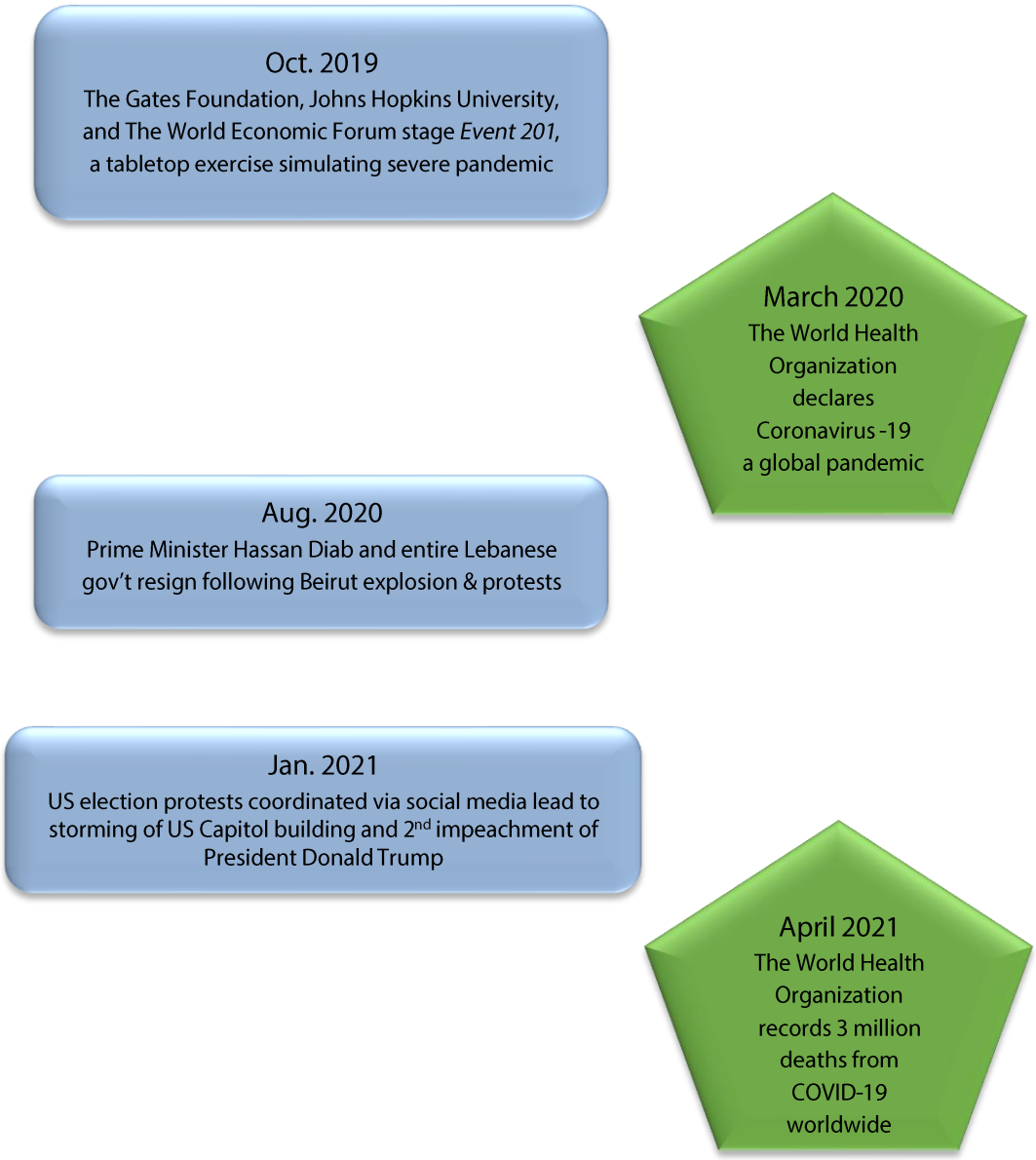
July 4, 2014
US 1st bombs ISIS camp in Syria attempting to find hostaged US journalists & NGO worker

Mid- 2014
ISIS gains large social media recruiting presence in the West via social media and declares "Caliphate"

Oct. 24, 2017
Glen Greenwald & media outlet *The Intercept* reveal 4 year-old 'Snowden file' that warned of Saudi & US-led destruction of Damascus

Dec. 2018 – Apr. 11, 2019
Revolution in Sudan coordinated via social media leads to President al-Bashir's resignation, Bashir goes on trial at ICC for crimes against humanity

Oct. 2019
Revolution in Lebanon coordinated via social media leads to Prime Minister Hariri's resignation


Oct. 2019
The Gates Foundation, Johns Hopkins University, and The World Economic Forum stage *Event 201*, a tabletop exercise simulating severe pandemic
March 2020
The World Health Organization declares Coronavirus -19 a global pandemic
Aug. 2020
Prime Minister Hassan Diab and entire Lebanese gov't resign following Beirut explosion & protests
Jan. 2021
US election protests coordinated via social media lead to storming of US Capitol building and 2nd impeachment of President Donald Trump
April 2021
The World Health Organization records 3 million deaths from COVID-19 worldwide

Introduction

As an academic subject, the American Empire is largely taboo.
Chalmers Johnson

This paper begins with many honest premises. First and foremost, that the Arab Spring protests have ended in violence and the deaths of numerous protesters, followed by state coups, the 'failure' of states, wars, sex slavery and human trafficking, refugee migrations, genocides and major destablization of the entire Middle East and beyond. Therefore, this paper does not hesitate to frame any and all discussion of the Arab Spring protests of 2011 in those terms. Further, it makes the argument that the FBI, Pentagon, NATO, and technologists of various US industries including media are responsible for these premeditated tragedies.

This paper is not a history or chronology of the Arab Spring. This is a paper about *how* the Arab Spring happened, and therefore it features much more analysis and theory than history lessons. As a result, my findings may be much more broadly applied.

I analyze the processes that created revolution, war, and genocide in the age of the cyberarms race and Web 2.0. I focus on the intersection between information technology and US foreign policy in the Middle East as an information science professional and Middle East studies expert. This is in no way a look at 'what went wrong' in the celebrated Arab Spring movement, and where my opinion is expressed, it is intolerant of the exclusion of the results of the Arab Spring.

It is a laying out of facts as they occurred with: first, knowledge of the US' military and intelligence transgressions in the Middle East, and second, a basic understanding of the history of technology in modern war crimes. It shows that the events that have unfolded before and since 2011 display a high level of strategic and tactical coordination between government and industry professionals to the end seen today. Theoretically, it is a work of realism, therefore it "assume[s] unitary governmental decision-making with a high degree of control over implementation and access to near-perfect information" over the "popular passions, operational instruments, and political objectives" of war. This created the monopolies of violence that were needed to bring about both the idealism of the Arab Spring and the devastation that would result.

As Magdalena Karolak writes in *The Social Media Wars*, the government is "simultaneously target, sponsor, and antagonist for social movements as well as the organizer of the political system and the arbiter of victory."[3]

[3] Karolak, Magdalena. *The Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Academica Press. 2014, p. 13.

Hackers' wars are irregular warfare information operations[4] incorporating electronic warfare operations[5] conducted by a state which deliberately involve populations to effect war, coup or other policy objectives that create the conditions of civil strife. These operations are typically carried out as wargames before or simultaneously with the execution of the real-world operation. The most salient features of hackers' wars are propaganda efforts, surveillance, cyberespionage and hacking, electronic weaponry deployment, and, importantly, the misattribution of these cyber coercion and deterrence techniques. The role of cyberweaponry is most saliently concealed in hackers' wars because information operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not "considered an armed attack under international law" or "an act of war".[6] In short, **hackers' wars are the wars brought about by hackers.** In the case of the Arab Spring, the hackers' wars began thusly:

> The regime responded by disrupting the flow of information, hacking e-mail and Facebook accounts, but the social revolution inside Tunisia and the solidarity movement outside Tunisia, had already a strong momentum. The Anonymous group hacked Tunisian government websites and assisted Tunisians to parry Internet censorship. In less than a month of social unrest dictator Ben Ali chose to leave the country. The combination of social media (Facebook) in the beginning of the events was critical in reaching not only millions of Tunisians, but also the local and global traditional media (Al-Jazeera). The protests in Egypt followed the successful one in Tunisia. The oppressive and corrupt regime of Mubarak forced thousands of Egyptians to organize massive social protests. The protesters demanded Mubarak's resignation and the reinstitution of democracy. Social media was used not only to spread the message, but also to share online content like online maps and encryption techniques. The Egyptian police monitored social networks, email accounts of dissidents as well as Skype and arrested dissidents that were responsible for coordinating the protests. In late January 2011, the regime, in a desperate move to control the information flow, decided to cut off access to Internet for a few days. Despite such restrictions, the movement had reached a critical mass and support, both inside and outside the country. In technical terms, Egyptians were able to employ alternative connection routes or import satellite phones. Likewise, news channels like Al-Jazeera succeeded in reaching Egyptians by transmitting via alternative satellites. Furthermore Google and Twitter released a new social media tool Speak2Tweet, that allowed Egyptians to use their mobile phones, to call a number and leave

---

[4] From Congressional Research Service *Defense Primer: Information Operations*: While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations… which include computer network attack, computer network defense, and computer network exploitation; psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC).

[5] From Congressional Research Service *Defense Primer: Electronic Warfare*: Electronic warfare (EW), as defined by the Department of Defense (DOD), are military activities that use electromagnetic energy to control the electromagnetic spectrum ("the spectrum") and attack an enemy… Applications include radio frequencies to communicate with friendly forces; microwaves for tactical data-links, radars, and satellite communications; infrared for intelligence and to target enemies; and lasers across the entire spectrum to communicate, transmit data, and potentially destroy a target.

[6] Theohary, Catherine A. *Defense Primer: Information Operations*. Congressional Research Service. 14 January 2020, p. 2.

> a voicemail, which would then be 'tweeted' on the Twitter website. In common with Tunisia, social and traditional media were closely linked and gradually even state-controlled media supported the protesters.[7]

Simply put, the Arab Spring was war profiteering and pre-existing policy enacted via social engineering. Although I will not make the comparison throughout, this perspective is also informed by now-declassified US social subversive actions taken throughout the 1950s to 1980s in Latin America. And while the Middle East is now the most war-torn area of the world, Latin American regions and cities remain by far the most dangerous and violent places in the world since those decades due to the effects of narco-terrorism, with up to 45 out of 50 of the world's highest homicide rates being found in Latin American cities. These are allegedly non-conflict zones that have not experienced declared invasion by the US. While similar US actions occurred in the Middle East decades ago as well, decades ago the Middle East was much farther away logistically from North America than it is today.

There are many similarities that can be explored between Latin American narco-terrorism and jihadi terrorism: their emergences with US policy change and their functions as US policy counterpoints; their self-perpetuating problematics; and their portrayals as culturally natural and inevitable.

+ADD "The high level of violence and the paramilitary capabilities of some cartels draw easy comparisons with modern irregular warfare. Some of the violence enacted by cartels displays a level of anomie that bears resemblance to terrorist tactics. Anomic violence relates to purposeless and gruesome acts of aggression in complete contravention of societal norms and values."[8] ; "The cartels create regional instability that foreign competitors can leverage to gain access to the Western hemisphere. The human security threat draws the attention of nearly every international and nongovernmental entity in the world."[9] ; "The enemy is made up of organizations exploiting this shortfall… The organizations exploiting the lack of human security are known by many names: violent drug trafficking organizations, transnational criminal organizations, narcos, insurgents, cartels, and criminals. The human security threat that cartels propagate resembles the mythological Hydra: immortal, multiheaded, regenerative, and poisonous. States cannot wage war, as traditionally conceived, against such a threat."[10]

+ADD quote to introduce scenario-based policymaking "Although this transfer is not zero-sum, early losers such as most of Latin America (with the exception of Brazil and a few others) and Africa are receiving neither a stake in the initial asset transfer nor any significant inbound investment from the recipient countries… Parts of Latin America will continue to be among the world's most violent areas. Drug trafficking organizations, sustained in part by increased local drug consumption, transnational criminal cartels, and local crime rings and gangs, will continue to undermine public security. These factors, and persistent weaknesses in

---

[7] "The Challenges of Social Media for the Intelligence Community" Andrew Liaropoulos, p. 9-10.
[8] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 6.
[9] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 33.
[10] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 2.

the rule of law, will mean that a few small countries, especially in Central America and the Caribbean, will verge on becoming failed states."[11]

"The pan-Arab identity underlining the Arab Spring"[12] is the reason I prefer to deal with all the Arab countries involved in the Arab Spring at once, or, individually as part of a whole. It is more reflective of the political philosophy from which it was born despite much of the activity online occurring in English, and despite ensuing wars and elections favoring the more current pan-Islamist political philosophy rather than signaling a return to pan-Arabism by the Arab youth. This is a philosophical contradiction and a structural indicator that the Arab Spring was staged.

I believe there is not much sense in tracking identity movements in the Arab World. Islamism is clearly on the rise as shown in increased homogeneity in the Middle East caused by war, persecutions, kidnapping and trafficking, genocides of religious and ethnic minorities, and partitions along such lines created by intervening countries. Pan-Arabism or Arab nationalism is likely not on the rise since a large number of Arab nations have been dismantled by wars and coups and their populations scattered since 2011.

The role of US foreign policy and the role of American popular and commercial participation before, during, and after the Arab Spring is the 'identity movement' I am interested in tracking. Through details I will discuss about the identities expressed through the technologies involved, I will show that the introduction of technology into a long-standing Orientalist trend has enabled new generations and larger numbers of Westerners to represent and intervene in the East for Easterners.

I also show that social media companies were able to conduct social engineering by committing *technical* social engineering, all of which combined to allow super-states to conduct literal proxy wars via proxied technology devices. This concept is addressed in the sections titled Social Engineering and Proxy Wars and 'Going Native'.

In addition to the effects of the Arab Spring that I directly address, a likely increase in drug growing and trafficking would be a point for further research in the region. Not only have there been ample reports of US military involvement in opium trafficking in Afghanistan, for example, but the analogy can be made between the Middle East interventions and indirect subversions in Latin America under the guise of a war on drugs or terrorism, both of which actually have the effect of increasing violence, drug use, and regional instability. [ADD quote? "We stated that our goal is to establish a 'flourishing market economy,' " said Douglas Lute, the White House's Afghan war czar from 2007 to 2013. "I thought we should have specified a flourishing drug trade — this is the only part of the market that's working." From the beginning, Washington never really figured out how to incorporate a war on drugs into its war against al-Qaeda. By 2006, U.S. officials feared that narco-traffickers had become stronger than the Afghan

---

[11] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 7, 15.

[12] Karolak, Magdalena. *Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Bethesda: Academica Press. 2014, p. ?

government and that money from the drug trade was powering the insurgency. No single agency or country was in charge of the Afghan drug strategy for the entirety of the war, so the State Department, the DEA, the U.S. military, NATO allies and the Afghan government butted heads constantly. [13]]

That the ongoing nature of these criminal conspiracies necessitate a complicity of silence from international media and expert commentators on relevant topics - to continue the example, not connecting the emergence of the Opium Crisis in the US in 2002 with the 2001 US invasion of the world's leading exporter of opium (the same strategy employed by the British against China during the Anglo-Afghan Wars of the 19th century) suggests that there is more at stake privately for the leisure class that makes up international media than maintaining a job with disposable income. To encourage this point of inquiry, I will include some facts here that will indicate a broader connection between these seemingly unrelated industry members as pertains to drug trafficking and terrorism.

It is in fact impossible now to research or write on the topic of modern genocides by technology without technologists finding out before the project has even left the research phase. This aspect of cyber realism and war - that technology corporations have a high level of state-sanctioned end-to-end control of war weaponry operations, information access, and public opinion - is important to deal with because it is the context in which *any* information will be gathered and presented to a broader audience which can be used to prove or prevent the extinction of entire peoples and nations.

The media's role as the public-facing side of the political and technologic industries is addressed under the same argument for cyber realism in the section Monopoly on Violence, Monopoly on Infringement. The media's long-time habit of conducting their investigations by use of war crime technologies and their dependence on reporting on human suffering to make revenue, known as the CNN effect, has created an extremely corrupt and biased situation in which modern media operate. Adversarial journalism cannot exist when journalists are in the same money-making industries as the Pentagon. Moreover, a Free Press, and the protection those individuals are granted in the Constitution to do their work, does not exist to provide immunity for criminal conspiracy and operation of warfare technologies.

2011 in 20/20

The initial quote from Said's *Orientalism* I mean to refer to the young people who took part in the Arab Spring from outside the country thrown into revolution. They are mostly non-experts with no career or educational experience in Middle East politics. They have no commitment to the results of their actions and experience none of the after-effects. If their projections were wrong concerning what would happen after plotting coups for regime change, it would not alter the course of their lives or careers. Deciding what the Orient should and shouldn't become is essentially their online hobby because it is exotic and escapist and has

[13] https://www.msn.com/en-us/news/world/confidential-documents-reveal-us-officials-failed-to-tell-the-truth-about-the-war-in-afghanistan/ar-BBXY8l1?ocid=spartanntp

nothing to do with their real lives, just as it was for the 18th century European novelists Edward Said wrote about in *Orientalism*. Like those writers, they show no desire to visit these countries or learn their histories and reconcile their opinions with reality. Their interest is fleeting, and soon they are on to the next polemic. Yet, at the time they can be excited into an "all-consuming passion" for regime change in those countries. They became what Clausewitz called "popular passions": one arm of the triad needed for a state to wage war.

Many of these individuals in Western hacking collectives identify politically and act as "anarchists", and the result of their actions is chaos. Anarchism can fall under two principle headings in conceptual subject hierarchies: utopia, or resistance to government. These individuals do not practice pure anarchism in the utopian sense, that is, as a political philosophy used in dialectics of law and governance, or in practice as a highly-evolved society not in need of hierarchy to function in most respects. They are contemporary or pop anarchists, or more accurately anti-hierarchists, whose political philosophy resembles a mixture of Marxist or Communist ideology by methods of civil disobedience. They are focused on extremely contemporary popular issues such as feminism, civil rights, environment, immigration across borders, and the Third World. They feel prepared to express their opinions authoritatively on every subject because they only need to be familiar with one polemical aspect which they can contradict, as if it were the crux of the issue, and magnify, as if all society were imperfect due to that aspect of that issue. When those contemporary marginalized groups named above or individuals representing those groups gain power or majority, pop anarchists tend to turn against them and attack them in the most stereotypical and therefore hypocritical fashion. In this way, they are extremely neo-liberal, serving the status quo by attacking successful reformers and practitioners of their philosophies. Pop anarchists have very progressive *and* conservative, narrow absolutist approaches to policy.

Able to be called reactionaries, their positions on these issues are formulated in resistance to status quos, and they are in constant political movement against 'what is'. They are considered anarchists still because they justify their negative or *anti-* positions as being steps in progress to an utopian society. However, these particular hacking collectives tend to envision a utopia where most people unlike themselves simply do not exist or belong in future society. Alternatively, being outnumbered by society in a democracy may represent a power hierarchy to them which must be thinned out to have an 'effective' democracy. This forms the foundation for their desire to control democracies and their willingness to take part in violent revolutions, cruel discriminations, and genocides.

When such groups do find power and solidarity or just experience longevity, things 'go psychological' and members either tend to moderate, prove unable to recognize or manage their own authority, or, their penchant for uncompromising progress is turned against their own grip on the state of affairs and they become self-destructive and even more outwardly destructive. Ironically, pop anarchists do not recognize their ability to use violence or disruption as a power monopoly over society, which usually increases their use of violence even as they increase in

power. In this sense, they are policy and power absolutists and inclined to ethnic cleansings and despotism.

It is going too far to say that these hacking syndicates deny what has occurred in the Middle East since 2011 due to their actions, in the way Pentagon or NATO officials do; it is more accurate to say that it does not even occur to them to deny, because they may feel no responsibility and possibly do not even care enough to keep up with events since 2011. My opinion of the Arab Spring Americans is best summed up in the words of the premiere literary authority on American youth F. Scott Fitzgerald:

> It was all very careless and confused. They were careless people,... – they smashed up things and creatures and then retreated back into their money or their vast carelessness, or whatever it was that kept them together and let other people clean up the mess they had made.

I believe the Arab Spring Americans' combination of popular passion, political ignorance, and carelessness is a dangerous combination, and what makes them so potent a political tool for states. Chronicler of Anonymous, Parmy Olson, writes similarly that,

> Anonymous was 'Legion,' after all. 'It didn't seem sketchy at all,' said one source who knew about the botnets being used to support AnonOps in December 2010 and January 2011. 'More fun trickery I guess.' The upper tier of operators and botnet masters also did not see themselves as being manipulative… online vigilantism meanwhile became his [an Anonymous member's] full-time job. It was fulfilling and effective. He didn't need to hack people's computers to get their private data - he just needed to talk to them, to employ the subtle art of 'social engineering,' that fancy way to describe lying… It wasn't that people in Anonymous were shallow or that there was little value to their experiences - it was just that events and relationships on the Internet moved far more quickly and dramatically than in real life. The data input for Anons [members of Anonymous] could be overwhelming, and often the result was detachment - from emotions, from morals, and from awareness of what was really going on.[14]

+ADD *Business Insider*: "Some among America's military allies believe Trump deliberately attempted a coup and may have had help from federal law enforcement officials"[15]

"a collection of U.S. military documents from 2016 obtained by *TomDispatch* via the Freedom of Information Act. "That drone-launching terror group, PAL, for instance, is neither Islamist nor a right-wing terror group, but an organization supposedly formed in 2017 in hopes of defeating "globalism and capitalism throughout the world by rallying the proletariat to orchestrate the overthrow of capitalist governments and global conglomerates." [description of FBI-created Occupy Movement protesters] Its ideology, an amalgam of increasingly stale leftist social movements, belies its progressive ranks, a rainbow coalition

---

[14] Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. London: William Heinemann, 2013, p. 120; 37-38; 124.

[15] https://www.msn.com/en-us/news/world/some-among-america-s-military-allies-believe-trump-deliberately-attempted-a-coup-and-may-have-had-help-from-federal-law-enforcement-officials/ar-BB1cypbi?ocid=Peregrine 1/7/2020

consisting of "most of the globe's ethnicities and cultures," all of whom seem to be cyber-sophisticates skilled in fundraising, recruiting, as well as marketing their particular brand of radicalism. As of 2020, the audacious drone strike on CENTCOM's headquarters was PAL's only terror attack in the tangible world." . Then there's Anonymous. In the Pentagon's fictional war-game, this real-world hacktivist group is characterized as a "loose organization of malicious black-hat hackers" that employs its digital prowess to "distribute bomb-making instructions, and conduct targeting for options other than planes, trains, and automobiles." In the past created by the military's imagineers, Anonymous was declared a terrorist organization after it conducted an August 2015 digital attack on Louisiana's power grid with something akin to the Stuxnet worm that damaged nuclear centrifuges in Iran. That cyber-assault was meant to protest the state's restrictions on online gambling -- an affront, according to the fictional Anonymous, to Internet freedom. (In the real world, Louisiana lawmakers actually just deep-sixed online gambling without an apparent terrorist response.) Taking down that power grid "resulted in the death of 15 elderly patients trapped in a facility denied air conditioning as a result of the power outage."[16]

As commentary on the US military's careless posture towards modern warfare: *War Is Boring*[17]; "The Future of War is Boring" by the Modern War Institute[18] and "It's the Boring Things That Will Win the Next War"[19]: "Yet the contours of conflict will not be entirely defined, and victors not solely decided, by new technology. There are a range of other factors that will also prove important—from doctrine to personnel policies to facilities management and beyond. Collectively, these things are more mundane than virtually any technology expected to play a role in future wars. With the exception of specialists with certain professional interests, most people find them comparatively boring. But getting them right could mean the difference between victory and defeat in future conflict… even though it's virtually impossible to know what technology will be available far into the future. Harrison [the command innovation officer of Army Futures Command] emphasized that point. 'If I could tell you what the technology landscape is going to look like in 2025, or next year,' he said, 'I would be all in in the stock market.'"[20]

Cyber defense strategist Daniel Steed writes concerning democratic challenges in cyberspace:

> Beyond the incessant and insidious challenges posed by criminals in cyberspace, which are very considerable indeed, it is the political challenges that carry the greatest concern moving ahead in cyberspace. By examining the growing competition between competing political visions - authoritarian versus liberal democratic - a clear geopolitical contest becomes clear with a dominating concern now emerging that the Internet is being leveraged to undermine democracy itself. This is first seen in the broad societal sense, with concerns about the influence of technological addiction and social media platforms among the general populace, a flood of digital information that instead of making us

---

16 Turse, Nick. "Tomgram: Nick Turse, Tomorrow's Terror Today". *Tom Dispatch.* 29 May 2018.
17 https://medium.com/war-is-boring
18 https://mwi.usma.edu/future-war-boring/
19 https://www.ausa.org/articles/it's-boring-things-will-win-next-war
20 https://www.ausa.org/articles/it's-boring-things-will-win-next-war

> wiser is 'making us more susceptible to nonsense, more emotional, more irrational, and more mobbish.'[21]

Steed's argument that social media can be used to undermine democracy is not as counterintuitive as some democracy-utopists may assume. For example, **Alexis de Tocqueville's principle critique of democracy was that it was a "tyranny of the majority". The manipulability of the Internet's readily apparent statistics and resulting statistical analyses make it all too easy to create a *seeming* tyranny of the majority by falsifying data and figures. When the Internet is deemed an incorruptible, open democratic tool for population sampling and policy decision-making, without skepticism, the result is a government and society vulnerable to information manipulations.**

In reality, Internet protocol is controlled by US government functionaries and its online communities are populated by government-sponsored bot armies. Considering the overwhelming presence English-speaking youth with disposable incomes provided them by wealthy bureaucrats and other financiers populating the Internet, it is completely logical to expect that a new tyranny, demographically very similar to the one de Tocqueville studied, would emerge anew.

+ADD "Chapter 1 — the secret American funding and orchestration of the so-called "color revolutions" in Eastern Europe , with particular focus on Serbia (2000), Georgia (2003), Ukraine (2004) and Kyrghizistan (2005). In each case, pro-Soviet governments were overthrown by mobilizing disaffected, pro-Western young people — financed by the CIA, State Department, and Pentagon **linked "democracy manipulating" foundations.** The latter include National Endowment for Democracy (NED), National Democratic Institute for International Affairs (NDI), the International Republic Institute (IRI),Freedom House (FH), the Albert Einstein Institution, the Center for Non Violent Action and Strategies (CANVAS), the United States Agency for International Development (USAID) — and George Soros' Open Society Institute (OSI). Several "color revolution" veterans were used to help organize Arab Spring protests."[22]

+ADD "A pattern of behaviour has been established that relies on implausible deniability, combined with an apparently new operational method that is actually an echo of past Russian strategic culture."[23]

It is by such recognitions of the threats to democracy posed by cyberspace, infrastructurally and socially, that I analyze the Arab Spring.

+ADD NIC use of phrase "causing democracy **to break out**" (as in 'violence'), using 'democracy' synonymously with 'protests' and 'revolutions'.

… **The "setback" of 1967 fatally injured the legitimacy of secular Arabism, facilitating the rise of the Islamist alternative in the 1970s**… He [Nasser] resigned before his loyal people fully realised the scale of the defeat, only to be called back by popular demonstrations**. His radio**

---

[21] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 3.

[22] https://stuartbramhall.wordpress.com/2014/01/18/the-cia-role-in-the-arab-spring/ [from ***L'Arabesque Americain***e by Ahmed Bensaada]

[23] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 47.

station, however, had been convicted of deceit out of its own mouth, and could only be disavowed quietly."[24]
+ADD *After the Arab Spring:* ***How Islamists Hijacked the Middle East Revolts*** (2012) by John R. Bradley, foreign correspondent for *The New York Post, The Washington Quarterly*. Reviewed on cover by Robert Baer, former Middle East-based CIA operative: "*After the Arab Spring* is indispensable to understanding why the Middle East uprisings aren't going where we want. John R. Bradley has a better pulse on the reality than anyone."

Just as a democratically-themed media blitz, followed by US-NATO led military intervention, managed the end of Nasserism/pan-Arabism and led to political Islamism in the late 20th century, the failure of the Arab Spring was a 21st century failure of nationalism and a hand-over to Islamism. This facilitated the rise of political Islamist militias. In 2012, before the Syrian Civil War had even begun, US media personalities were calling the Arab Spring a "hijacked" win for Islamists in the region.
The US and theocratically-governed allies in the Middle East "poured hundreds of millions of dollars and tens of thousands of tons of weapons into anyone who would fight against Assad, except that the people who were being supplied were al-Nusra, and al-Qaeda, and the extremist elements of jihadis coming from other parts of the world."[25]

The argument in favor of cyber-realism in this essay acknowledges theoretical realism as it applies to policy and war, such as Clausewitz's triad of war, or assignation of end-to-end control of operational equipment, popular passions, and policymaking. It also acknowledges realism in its primary sense, as it applies to cyber realism. I acknowledge the atrocities of policy and war committed by technologists. This includes recognition of: real-time knowledge of war crimes committed via synthetic aperture radar and camera drones; the commission of scientific and technological institutions in policymaking which results in warfare; the US's near complete control of the Internet; the use of satellite weaponry by media corporations; the planned proliferation of technological weaponry by the US intelligence agencies; the Pentagon ownership of companies involved in media revolutions; and the planned policy failures of policymaking institutions.

I acknowledge illustrative historical examples of technologists' war crimes. These illustrative examples include shocking examples of war crimes commissions. For example, it is known that Auschwitz prisoners' tattoos corresponded with the IBM punch-card ID numbers created by Dehomag (an IBM subsidiary) to identify and classify the populace for extermination. The definition of the Information Age I use is defined by Holocaust researcher Edwin Black:

> The Information Age is the individualization of statistics. Not only can I count you as a member of the crowd, I can individualize the information I have about you. And the Information Age was invented not in Silicon Valley, but in Berlin in 1933.[26]

Targeted genocides today are likely based on a wide scope of *de-aggregated* data on individuals. Therefore, groups targeted for genocide may defy traditional concepts of 'group' or 'community'. Persecutions may be based on other information collected, which was the case in

---

[24] James, Laura. "Whose Voice? Nasser, the Arabs, and 'Sawt al-Arab' Radio". *Arab Media and Society*. Kamal Adham Center for Television and Digital Journalism of The American University in Cairo. 1 June 2006.
[25] https://foreignpolicy.com/2014/10/07/joe-biden-is-the-only-honest-man-in-washington/
[26] Black, Edwin. "IBM and the Holocaust". 26 February 2012. Presentation at Yeshiva University, New York, NY.

the European Holocaust, wherein IBM cross-indexed career, place of residence and other factors with race, religion and ethnicity in order to identify targets.

In the 21st century Information Age, concepts of 'group' may include groupings of individuals by web queries, Internet search history, IP addresses, purchases, payment methods, location check-ins, software downloaded, e-books viewed, languages enabled on computer, disability plug-ins, voice recognition identification, and a host of other behavioral traits collected regularly by technology corporations and governments.

For example, a surveillance State could feasibly choose to target for genocide all individuals who search "symptoms of cancer", "international adoption agencies", "secret government societies", "how to tell if your phone is hacked", "side effects of PTSD medication", "how to apply for a foreign work visa". A surveillance state could target individuals who download an encrypted browser, install firewall software, language learning software to study Chinese, or audio books regularly used by the disabled.

A state may find reason to target individuals who regularly make late bill payments, listen to songs with violent lyrics, routinely do app check-ins at expensive retailers, shop for restricted products like tobacco online, have more than two children identified in a contact list, visit government subsidized healthcare websites, do not use social media at all or use it excessively, or who telecommunicate so infrequently as to be termed anti-social. Without there being an apparent link to religion, race, ethnicity, or disability, these behavioral traits are regularly grouped in demographic categories for targeted advertising.

These demographics, as specific as they may seem, may be produced and purchased by government agencies and contractors in order to identify, target and eliminate undesirable targets, high-value targets, or rising targets (such as children, young adults, or persons in change), without fitting existing definitions of genocide as the intended destruction of "national, ethnical, racial or religious groups." Such behavioral traits may be used to identify and exterminate the least desirable or only highest-value subgroups within national, ethnical, racial or religious groups, and thereby avoid the appearance of genocide. Additionally, such behavioral traits may be used to identify members of the dominant national, ethnic, racial or religious groups who may associate with or favor groups targeted for genocide, thereby allowing the surveilling state to eliminate individuals who would intervene or oppose the extermination measures.

[TOPIC – the role of personal computers, user identification, and targeted genocide]

+ADD "**The usage data corresponding to one or more users may receive from a social medium account (e.g., Facebook.TM., Twitter.TM., or WhatsApp.TM. account) of the user. Alternatively or in addition, the usage data corresponding to one or more users may be received from a resonant electromagnetic radiation device, where the user has been exposed to radiation from that device. The usage data corresponding to one or more users may be received via a network, e.g., the Internet. One or more user characteristics of one or more users may include user's temperature, pulse rate, respiration rate, blood pressure, and/or electroencephalogram (EEG).** The indication of usage may include a frequency of usage and/or an effectiveness measure… **the method also includes selecting a user characteristic from the recipe database that matches with the user characteristic received separately, and transmitting to a destination at least one recipe from the set of recipes corresponding to or correlating with the selected user characteristic. The destination can be a social medium account of a user and/or a controller of a resonant electromagnetic radiation device… One or more usage data elements corresponding to a user may be**

received, via a network, from a social medium account of the user and/or a controller of an resonant electromagnetic radiation device used by the user. The modulation style may include audio modulation, and **the recipe may further include an audio file identifier, such as a reference to a memory location in storage, a link to a song file on the Internet, a home network, etc**… In one embodiment, the output voltage of the power supply 108 can be adjusted to any value **within the range of 50-300V DC**… In some embodiments, alternatively or in addition, **an audio signal can be received from an external source (e.g., a smart phone, CD player, etc.) at an audio input port 130, and can be used to modulate the carrier in a manner similar to amplitude modulation** using the stored audio signal. **The audio signal may be received or streamed via a network (such as the Internet, a user's home network, etc.)**, as well."[27]

+ADD Brack to Himmler Nuremberg Trials 1941 letter: "One practical way of proceeding would be, for instance, to **let the persons to be treated approach a counter, where they could be asked to answer some questions or to fill in forms**, which would take them 2 or 3 minutes**. The official sitting behind the counter could operate the installation in such a way as to turn a switch which would activate the two valves simultaneously (since the irradiation has to operate** from both sides.) With a two valves installation about 150-200 persons could then be sterilized per day, and therefore, with 20 such installations as many as 3000-4000 persons per day."[28]

+ADD General Michael Hayden, former CIA and NSA director: **"We kill people based on metadata."**[29]

Sen. Rand Paul Floor Speech Against Patriot Act Reauthorization:

> "The reason why we should worry about whether a warrant is individualized is we have had some tragic times in our history. During World War II we didn't individualize the arrests of Japanese Americans. We didn't say: That is so-and-so who lives in California, and we think they are communicating with Japan and telling our secrets. We indiscriminately rounded up all of the Japanese and incarcerated them.
>
> **There have been times in our history when we haven't acted in an individualized manner.** It happened throughout the South in the old Jim Crow South. We told people that we were going to relegate them to a certain status based on a general category.
>
> So **when we talk about individualizing warrants [in the Fourth Amendment], we are talking about trying to prevent bias from occurring. Now, bias can occur for a lot of different reasons.** I tell people that you can be a minority because of the color of your skin or the shade of your ideology. You can be a minority because of your religion. **You can be a minority because you are home-schooled.** But the thing is, **if you are a minority, if you are a dissenter, if you dissent from the majority, you need to be very, very aware** of your constitutional rights. Be very, very aware of the Bill of Rights.

---

[27] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10,252,072.PN.&OS=PN/10,252,072&RS=PN/10,252,072

[28] *Trials of War Criminals: Before the Nuremberg Military Tribunals under Control Council Law, No. 10. Vol. I, The Medical Case.* U.S. Government Printing Office. 1946-49, p. 719-20.

[29] https://www.youtube.com/watch?v=kV2HDM86XgI ; https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

> The Bill of Rights isn't so much for the prom queen. The Bill of Rights isn't so much for the high school quarterback. Many people in life always seem to be treated fairly. The Bill of Rights is for those who are less fortunate, for **those who might be a minority of thought, deed or race**. We have to be concerned about **the individualization of our policies** or we run the risk and **the danger of people being treated in categories**.
>
> **Right now we are treating every American in one category.** There is a general veil of suspicion that is placed on every American now. **Every American is somehow said to be under suspicion, because we are collecting the records of every American**.
>
> We talk about metadata and whether or how much it means or what the government thinks it can determine from metadata. There are some people who say: Don't worry. It is just your phone logs. It is no big deal. It is just boring old business records. We should be a little bit concerned by the words of one former intelligence officer who said, that 'we kill people based on metadata.' He wasn't referring to Americans. He was talking about terrorists. But we should be concerned that they are so confident of metadata that they would kill someone. Instead of our believing that metadata is no big deal and it just should be public information and anybody can have it, **realize that your government is so certain of metadata that they would kill an individual over it.** That seems to me to make the point that **metadata is incredibly important, if we would make a decision to kill someone based on their metadata."**[30]

+ADD Yershov vs. Gannett Satellite Information Network case defines "identifying information" as "someone who _" rather than regular personal identifying information.[31]
"*Yershov v. Gannett Satellite Info. Network, Inc*., No. 15-1719 (1st Cir. 2016)
Justia Opinion Summary:
Gannett Satellite Information Network, Inc. is an international media company that produces news and entertainment programming through a proprietary mobile software application (the "App"). Plaintiff downloaded and installed the App on his Android mobile device. **Every time Plaintiff watched a video clip on the App, Gannett shared information about Plaintiff with Adobe Systems Incorporated**. Plaintiff brought this putative class-action lawsuit against Gannett for allegedly disclosing information about him to a third party in violation of the Video Privacy Protection Act (VPPA). The district court dismissed the action under Fed. R. Civ. P. 12(b)(6), **concluding that that information disclosed by Gannett was "personally identifiable information" (PII) under the VPPA but that Plaintiff was not a "consumer" protected by the VPPA. The First Circuit reversed, holding that the complaint adequately alleged that Plaintiff was a "consumer" under the VPPA."**[32]

+ *Denial of Violence*

Condoleezza Rice on the US's justifications post-Iraq invasion in 2006 "But we somehow seem to think back on an Iraq that was a pristine Iraq, where the Iraqi people were somehow thriving. That wasn't the Iraq that we found. We were dealing with an Iraq with a brutal dictator [Hussein], with 300,000 people in

---

[30] *Sen. Rand Paul Floor Speech Against Patriot Act Reauthorization*. 20 May 2015.Federation of American Scientists. https://fas.org/irp/congress/2015_cr/paul-patriot.html
[31] *United States Court of Appeals For the First Circuit No. 15-1719 ALEXANDER YERSHOV v. GANNETT SATELLITE INFORMATION NETWORK, INC., USA TODAY.* Accessed 9 July 2019.
[32] https://law.justia.com/cases/federal/appellate-courts/ca1/15-1719/15-1719-2016-04-29.html

mass graves, who had used weapons of mass destruction, who'd attacked his neighbors,"...
Rice: "It's not civil war when you have a prime minister of Iraq, who is himself a Shia, who sits with the defense minister, who is a Sunni, with an interior minister who's a Shia, with a president who is Kurdish. That's not civil war."[33]
In fact, that has been the colonizer's set-up for civil war in the Middle East since the early modern political era. The US-created Iraqi Constitution is the first Iraqi Constitution to have designated sectarian representations along French colonial requirements, like those found in Lebanon, which did lead to civil war in Lebanon beginning in the 1970s.[34]

Those whose job it is to analyze the events of the Arab Spring outside of the countries of revolution are divided into three major opinion groups according to the RAND Corporation (Research and Nuclear Development Corporation), the policy institute most closely connected with the US Department of Defense. Their appraisal of existing opinions is echoed in other works on the Arab Spring including but not limited to works published by *Small Wars Journal*, *The Washington Post*, The Brookings Institute, *Al-Jazeera*, Harvard University[35], Amnesty International, the Middle East Institute[36], Dewey and Kaden et al.'s Stanford report for the American Defense Intelligence Agency,…
+ADD from NIC *Global Trends 2030* (2012): "The Future of Terrorism: Several circumstances are ending the current Islamist phase of terrorism… Moral Resurgence of Secular Democracy. The Arab uprisings have demonstrated the moral and strategic legitimacy of nonviolent struggle. Protestors acted in the name of democratic values, not in the name of religion. Evaporation of Imagined War. Although warfare is very real, it is also an imagined state, based on a narrative of an enemy and conflict between fundamental values. These perceptions can change—sometimes quickly. A new generation may simply view things differently and be less interested in an old narrative."[37]

These camps delineated by RAND analysts are "Cyber-Enthusiasts", "Cyber-Killjoys", and "Anti-Imperialists".

+ADD In an article from National Defense University titled "NATO and the Arab Spring" it is plainly stated, "In the spring of 2011, dramatic events unfolded in the southern rim of the Mediterranean. Countries from Egypt to Libya were swept by significant popular uprising and political change. The events led to regional upheaval and ultimately armed conflict, resulting in a NATO-led operation in Libya," in the section titled "NATO Inherited Libya". This begs the question - inherited from whom? The article was published by the Institute for National Strategic

---

[33] http://www.nbcnews.com/id/14189415/ns/msnbc-hardball_with_chris_matthews/t/condoleezza-rice-iraq-lebanon-cuba/#.XXJcO0xFyM8
[34] See: Mackey, Sandra. *A Mirror of the Arab World: Lebanon in Conflict.* (2008); Trablousi, Fawwaz. *A History of Modern Lebanon.* (2012).
[35] "Notably, while the January 25 protests were initiated by a group of opposition activists, the Egyptian Arab Spring did not have a centralized leadership and no single element of the opposition was in control." https://rlp.hds.harvard.edu/faq/arab-spring-egypt
[36] https://www.mei.edu/publications/arab-spring-implications-us-policy-and-interests
[37] https://www.dni.gov/files/documents/GlobalTrends_2030.pdf p.68

Studies in October 2011, eight months after Anonymous publicly took credit in its *Al-Jazeera* opinion piece for the uprisings in North Africa. One day after Anonymous' publication on February 16, there broke out "serious unrest, which began on February 17," and the UN Security Council instituted an arms embargo, froze assets and restricted the travel of Libya's leaders (Resolution 1970). By March 27, NATO had sided with the military actions already taken by the US, UK and France on March 19 (Resolution 1973).[38]

"Such a connection is critical for the CNN effect, because it is important not only to demonstrate that the policy changed after such events, but to also link the policy change to the media images and framing of the events."[39]... "the CNN effect, using Nick Wheeler's distinction, does not necessarily need to by 'determining,' but can often be 'enabling,' creating a short-term environment or window of opportunity in which policy can move forward."[40] The interplay in fomenting coups between social media and broadcast media is well expressed by RAND analysts in the following: "Without social media there would have been no demonstrators passing by and no events for Al-Jazeera to report. Social media brought a critical mass of people into the streets; once they were place, then word of mouth, text messaging, telephones, and media coverage were able to exponentially grow the number of participants."[41]... "Perhaps this impulse to challenge social media's political import is due to the frivolity of most social media use, or to the concerns of anti-imperialists that the 'Facebook Revolution' label was concocted by Western countries to claim responsibility for the heroic acts of Arab youth."[42]

+ "In, 2011, Obama deployed U.S. military power to protect protesters in Libya who faced the threat of slaughter by Muammar Gaddafi. With Gaddafi hamstrung in his efforts to suppress the uprising, rebels forced him from power and sent his loyalists fleeing. Soon after, New York Times columnist Nicholas D. Kristof visited Tripoli and began his August 31 column this way: Americans are not often heroes in the Arab World, but as non-stop celebrations unfold here in the Libyan capital I keep running into ordinary people who learn where I'm from and then fervently repeat variants of the same phrase: 'Thank you, America!'".[43]

The RAND Corporation analysts declare themselves to be Cyber-Enthusiasts. Cyber-enthusiasts constitute a group of individuals that strongly support the role of technology in coordinating the Arab Spring revolutions. RAND's official stance is that "without social media, Mubarak's overthrow would not have occurred... So while one can imagine a revolution starting

---

[38] Francois, Isabelle. "NATO and the Arab Spring". *Transatlantic Current*, No. 1. National Defense University Press. October 2011.

[39] Bahador. *The CNN Effect*, p. 35.

[40] Bahador. *The CNN Effect*, p. 35.

[41] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. RAND Corporation. 2013, p. 64-65.

[42] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. RAND Corporation. 2013, p. 71-72.

[43] **Sound the Trumpet: The United States and Human Rights Promotion** By Lawrence J. Haas, 42-43.

somewhere else without Facebook, it is hard to see how the one that happened in Egypt could have developed absent that technology."[44]

By RAND's own definition, Cyber-killjoys are the section of the scholarly and journalistic community that minimize the role social media played in the Arab Spring revolts and emphasize on-the-ground action. When exactly the RAND Corporation became proponents of joy remains unclear. Nevertheless, RAND analysts do feel displeased with the notion that others believe the Arab Spring would have been possible via on-the-ground action only.

RAND declares Anti-imperialists in the Arab Spring conversation to be those who attribute regime change in the Arab Spring to the Arab youth entirely and deny the role Western media played in the revolutions. Analysts write that, "Perhaps this impulse to challenge social media's political import is due to the frivolity of most social media use, or to the concerns of anti-imperialists that the 'Facebook Revolution' label was concocted by Western countries to claim responsibility for the heroic acts of Arab youth."[45] With this, RAND analysts stop just short of declaring the Arab Spring a product of indigenous knowledge.

With all of *three* options laid out, the Department of Defense's think-tank neatly classifies all the world's conceivable reactions and stances on the nebulous interactions that occurred over two weeks which prompted revolution over one-fourth of the planet, and the decade-long conflicts which resulted from those regime changes. So such institutions like RAND are able to set the framework and shape all ensuing conversation in the field, neatly removing themselves as actors from the equation, which I have witnessed in lecture halls and in journals for a decade. This think-tank-for-hire framework and its byproduct in scholarly discussion on the Arab Spring have been wholly insufficient in its explanatory prospects and does not merit serious consideration in a detailed cyber-realist conversation.

In contrast to RAND's official publications and statements, whistleblower Scott Bennett claims that he took part in Arab Spring-related projects at RAND in the late 2000s, funded by George Soros' Open Society Foundation. Bennett, a retired US Army officer, alleges he "sat in on briefings where the Arab Spring was discussed as an operation being planned in the United States to break up Arab societies and governments to be 'rearranged' by the Western powers, NATO etc." He specifies that within RAND, there was talk of flooding Arab social media with 'democracy' and 'revolution' tags and promotions. He claims that the Arab Spring was "a RAND product".[46]

This is an example of authoritarian information operations former National Security Council and State Department official Rosenberger and emerging technologies researcher Gorman have detailed in "How Democracies Can Win the Information Contest", saying:

---

[44] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. RAND Corporation. 2013, p. 45.

[45] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. RAND Corporation. 2013, p. 71-72.

[46] The a-Infos Radio Project. "US Army Whistleblower says Arab Spring was a RAND Corporation 'Product'". *State of the City Reports.* 21 April 2017.

> Engagement-driven metrics guiding the algorithms that organize, prioritize, and display information—and the opacity surrounding them—allow malign actors to degrade the information space by manipulating search results and promoting divisive content. Popular social media platforms that adhere to authoritarian censorship rules by removing or demoting certain content can also subtly shape public perception, even in democracies. Reports of video-sharing app TikTok censoring content related to Hong Kong pro-democracy protests is a case in point. Without transparency requirements for the way information is displayed on information platforms, this manipulation is difficult to detect and assess… This holistic view stretches across society and includes the full complement of authoritarian information efforts: targeted media and diplomatic narratives, coercion of public and private sector actors, the manipulation of personal data for influence or control, the deployment of surveillance technologies, and international engagement to advance sovereign internet norms.[47]

The 2020 protests in Hong Kong and many other instances of nascent and full-blown hackers' wars are addressed in the present study, as well as common hacking techniques like SQL injection and proxy hijacking which can be used to assess these manipulations. Aiming for inclusive and objective foreign policy analysis which respects diverse forms of sovereignty and change, I will highlight the civil conditions provoked by such information operations to delineate between hackers' wars, other occurrences, and situations that may not be determined yet.

Ret. Army officer Scott Bennett goes on to describe the 2010 Arab Spring information operations briefings at RAND:

> Well, I was there. I know – I know. I was in the briefings. I was there. I was at the RAND Corporation. I was in the building. I saw the people. I saw the people from Syria. I saw the people from Egypt. I saw the people coming around with radio broadcasts, and journalists, and people that were disc jockeys, and all of the conversations about *infecting* the communications with the words 'democracy' and 'human rights' and things like that… it was funded. When I go back into my analysis and my experience, I saw George Soros and the Soros organizations as funder for a lot of those activities and conversations that RAND was having. So, putting the big piece of this jigsaw puzzle together is dauting but at the same time with these little pieces we find, they say George Soros, the Open Society Foundation, and of course you have CIA, Mossad, MI6 all stepping in. I think, again, the promise was democracy and capitalism and human rights was going to evolve out of the broken cement where the dictators were crushed. And the opposite seems to be coming true.[48]

+ADD https://www.globalresearch.ca/the-arab-spring-made-in-the-usa/5484950 & book review (book translated yet?) https://stuartbramhall.wordpress.com/2014/01/18/the-cia-role-in-the-arab-spring/

The field of Middle Eastern studies has a long history of speaking for Middle Easterners, going back centuries to when it was referred to as Oriental Studies. This role of Western participation in Middle Eastern affairs is part of what Edward Said defined as Orientalism in the

---

[47] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 82, 84.
[48] The a-Infos Radio Project. "US Army Whistleblower says Arab Spring was a RAND Corporation 'Product'". *State of the City Reports.* 21 April 2017.

West. From Rudyard Kipling's Kim,- about a young Irish boy who acts as a spy by disguising himself in the garb and languages of various Indian ethnicities and religions,- to Anglo actors in black face portraying Othello, to T.E. Lawrence's legacy as Lawrence of Arabia, the idea of representing the Orient has fascinated "bright young Westerners". The introduction of technology into this long-standing Orientalist trend has enabled new generations and larger numbers of Westerners to represent the East for Easterners. After all, "social media, by its very nature, is only an extension of the social context in which it operates." And the unusually high level of participation displayed by foreigners in the Arab Spring who otherwise do not concern themselves with events in the Middle East demands explanation. [REWORD - repeated]

In this work, I suggest that multiple avenues available to "bright young Westerners" to represent Orientals are used today to reorganize the Middle East in accordance with US policy objectives. On the deliberate side of this Orientalist policymaking are wargames – wargames in which US intel-security roleplay and strategize as Middle Eastern regimes. Secondarily, unwitting Westerners (so-called "useful idiots" in intelligence parlance) assume the Internet proxies and even political voices of Middle Easterners, as happened in the 2009 Green Revolution in Iran and the Arab Spring of 2011.

In the section Unusual Games, I show how the wargaming community deliberately mobilizes the Internet and masses of people in information warfare operations; that is, citizens and companies are acting, knowingly or not, as government assets or militia, in roles cast for them in wargame scenarios which are used to start wars, stage coups, and achieve other policy objectives.

I explore in this essay the notion that game theory is very likely the precursor of the mediatization of war. Since I have not encountered other discussion of the strategic origin of the CNN effect or use of media to incite civil strife and war, game theory developed by RAND is a very reasonable origin. This is supported by discussion of a US government disaster scenario training news broadcast channel called "VNN". VNN is not a proper news channel nor is it supposed to broadcast actual events. It is used in FEMA disaster training exercises to prompt government workers to perform some action in the training session. In the sections Out of the Blue: Wargames and Wars and Monopoly on Violence, Monopoly on Infringement, I draw a parallel which should convey the blurring lines between the CNN effect in private media and the "VNN effect" in government scenarioist media. The blurred distinctions between reality and fiction, scenarios and plots, and cause and effect are discussed while **attempting to trace the origins of the CNN effect to what I term the VNN effect. The VNN effect is the use of wargames/scenario-based media to set policy agendas, impede opposing agendas, and push decision-makers into action.**

As most of the security and intelligence state game play, war games scenario conduction, and gamification of warfare came out of the RAND Corporation's game theory developed in the 1950s, the Department of Defense funded corporation makes an ideal environment in which such a plot may be hatched for the sake of alleged research. Such plots disguised as mental exercises

is discussed explicitly and also labeled as dangerous to conduct by RAND's own Herman Kahn in his 1958 *On Thermonuclear War.*

Far from being a scenario which can be walked back, the effects of social engineering in the Arab Spring have been irrevocably devastating. Among some of the most heinous crimes against humanity are the appearance of slave markets in post-intervention Libya under NATO and the sex slave trade under ISIS, organ harvesting from Syrian child refugees and genocide of Armenians in Turkey, and the transportation of live Syrian civilians by chilled meat trucks to torture prisons equipped with crematoria. These are the real results of Twitter and Facebook revolutions. Why companies would continue to brand these events in their names is beyond any legal understanding of what media corporations are really advertising and selling.

[Subsection?]

On the Mediterranean, very near Tunisia, slave auctions are now held in Tripoli, Libya. Following the NATO attack on Libya, slave markets emerged out of refugee camps where Libyan and other Africans have attempted to go north to escape yet another 'failed' state at the hands of NATO.[49]

Despite the uprisings of the Libyan African youth at the encouragement of US media companies during Arab Spring and NATO's military action creating the conditions for open-air slave markets, French President Macron suggests to the media further military intervention by NATO will solve the situation. He has placed the onus of blame on the African youth, saying, "Who are the traffickers? Ask yourselves – being the African youth – that question. You are unbelievable. Who are the traffickers? They are Africans, my friends. They are Africans."[50]

Macron's statement displays a total lack of realism; he demands of others the confidence that NATO can intervene in Libya because it has end-to-end control and knowledge of events, despite evidence he cites to the contrary. According Macron's anti-realist policy agenda, if only locals would stop intervening in NATO's omnipotence, NATO would be capable of perfectly administrating other nations' problems which NATO itself caused through previous interventions.

Following the fall of Syria, the Islamic State emerged in western Iraq and Syria. Almost immediately, it became synonymous with institutionalized sex slavery. However, the reality is that ISIS does conduct oil trade[51] and its slave trade with other nations. Amnesty International responds to accounts of ISIS sex slave trade saying:

> It is not the first time the accusation that ISIS sells rape victims to Saudi Arabians has emerged. An 18-year-old Yazidi sex slave who escaped ISIS claims she was sold in an international auction. … She said dozens of women were being held in a large room, and it was not only Iraqis and Syrians trading women but also Saudis and Westerners, whose actual nationality was not clear. Potential buyers...would inspect the women 'like livestock'. The cruelty of ISIS terrorists against Yazidi women and girls is nothing new. … ISIS extremist

---

[49] Clark, Neil. "Op-Ed: Slave Markets in 'Liberated' Libya and the Silence of Humanitarian Hawks". *RT*. 1 December 2017.

[50] "Macron urges military action in Libya to fight human trafficking". *RT*. 30 November 2017.

[51] OIL TRADE ISIS article

> burnt alive 19 Kurdish women for rejecting sex slavery. The victims, who had been taken by ISIS as sex slaves, were placed in iron cages in central Mosul and burned to death in front of hundreds of people [52]… Victims told Amnesty International the majority of the 'buyers' were men from Iraq and Syria, but there were some from other countries such as Australia. Other buyers were not Islamic State fighters, but only supporters of the terrorists. A Mosul resident said the men 'are local businessmen, not fighters.'[53]

The descriptions of the ISIS sex slave trade match descriptions from American child trafficking victims collected since the 1970s by individuals like University of Texas Professor Tom Philpott, author of documentary *Boys For Sale* (1981), and FBI administrator Ted Gunderson. Philpott was found dead while researching the child sex slave trade. Key descriptions include pedophilia, being sold in Saudi slave markets to international businessmen, politicians and celebrity sex slave buyers, witnessing cruel and unusual murders committed by the slave traders, and the use of global telecommunication systems in these acts.

These similarities suggest that the ISIS sex slave trade functions within the existing sex trafficking markets as they have existed for decades in the US. Technologists, the FBI and Pentagon's involvement in human trafficking and tracking is discussed in the sections Out Of The Blue and The Hacker's Arsenal.

It is also noted that the US has repeatedly taken military action to support the expansion of ISIS and therefore its institutionalized sex slavery market. This has included arming ISIS fighters to oust the Syrian government under the Obama Administration and killing Iran's leading military strategist against ISIS under the Trump Administration. The US State Department and Defense Department's roles in human sex trafficking in the Yugoslav War is discussed as well in the section The Bosnia Model, The Rumsfeld Model.
+ADD The repeated occurrence of mass murder and sex crimes following US-NATO "intervention": ISIS foreign fighters, Hazelwood theory underpinning, UK profilers' assessment that ISIS foreign fighters recruited online in the West "typically look at porn… are severe onanists... literally wankers".[54]

The pedophilic and theatrical element of ISIS's sex slavery are exemplified in the following account: "Two [Yazidi] girls aged 10 and 12, told Amnesty International: 'One day we were given clothes that looked like dance costumes and were told to bathe and wear those clothes.'" The account goes on to detail the suicide of one of the girls in the bathroom where they were told to put on their dance costumes.[55] I have encountered similar accounts that detail such dance costumes as being of a belly dancer design, which carries with it heavy connotations of orientalist subjugation in this sex slave trade.

---

[52] AHT Staff. "Picture shows ISIS Yazidi sex slaves sold in horrifying auctions to Saudi Arabia". *American Herald Tribune.* 25 September 2016.
[53] Chastain, Mary. "Amnesty International: ISIS Driving Yazidi Women to Suicide Through Rape, Sex Slavery". *Breitbart.* 23 December 2014.
[54] Perraudin, Frances and Shiv Malik. "Boris Johnson: jihadis are porn-watching 'wankers'". *The Guardian.* 30 January 2015.
[55] "Iraq: Yezidi women and girls face harrowing sexual violence". *Amnesty International News.* 23 December 2014.

Additionally, child victims and the forceful use of theatrical costumes characterizes ISIS sex slavery as highly mediatized, possibly televising criminal acts and selling audiovisual access to victims to a secondary audience. It has been confirmed that ISIS trades so-called sex slaves via the Internet.[56] The industries which profit off of what Jean Baudrillard called "televised holocausts" are the major issue discussed throughout every section of this book.

.https://law.vanderbilt.edu/academics/academic-programs/international-legal-studies/Yazidi_Genocide_Opinion_KRG_4.15.pdf

In 2014, an UN Human Rights Council official was questioned in a press conference about medical crimes taking place in Turkish hospitals and refugee camps. Estimates of up to 18,000 Syrian children have been medically executed or allowed to die in order for their organs to be harvested and sold. The UN official claims that the UN has little information or access to what is taking place on the ground on Syria, obstructing the premise of the question over crimes that are taking place in Turkey, a NATO country, and ignoring that major UN member countries have end-to-end control of global surveillance satellite systems over areas like Syria in which they are engaged in combat. Nevertheless, this remains the explanation the UN gives for not reporting to the world and to member countries on the medical murders and illegal organ harvesting. The UN official admits to his organization's awareness of genocide taking place against Armenians by rebel groups in Syria, but has not published any reports on this genocide either.[57] The likely origin of these crimes is elucidated by other reports of Turkey and NATO's facilitation of such groups in Syria[58], and Turkey's 1915 genocide of Armenian Christians inside Turkey by the Young Turks party and Turkey's continued denial of those crimes. [+ADD Congress passing resolution again after 90 years or already mentioned in Intro?]
[+ADD UN official's essay on Rwanda and Bosnia from *This Time We Knew,* neo-realism: "While claiming that security-seeking behavior may be used to describe the primary goal of all states, however, Waltz betrays a distinctly status-quo bias. Only in reference to satisfied countries can it be said that the first concern of states is to maintain their positions in the system… According to the neorealist perspective, states pursue secondary and tertiary goals only when the primary objective, survival, is ensured".[59]]

The ascendancy of ISIS, especially as it became obvious on social media and news media, created what has been termed the CNN effect to facilitate US-NATO military action. Along with the ensuing revelations of human rights abuses against, usually, minority groups, **the CNN effect** – that is, **media manufactured public consent to war** – launched the world's public into military action in several Arab Spring countries which had already been earmarked

---

[56] Ghandour, Christel. *ISIS's Use of Sexual Violence in Iraq.* Washington: Academica Press. 2019, p. 69.
[57] "18,000 Syrian Children Victim to Organ Harvesting - UN Questions 2014". *YouTube*. 6 May 2018.
[58] Nafeez, Ahmed. "Whistleblower exposes how NATO's leading ally is arming and funding ISIS: 'I am the police chief who was asked to guard ISIS terrorists'". *Insurge Intelligence.* 16 September 2016.
[59] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 103.

for US military invasion even before 2001 when Secretary of Defense Rumsfeld's office issued the memorandum Gen. Clark described to *Democracy Now!*.

As it serves the policymaking objectives staging the social media revolutions, the media are cast as being either at a stage of heightened awareness of atrocities against humanity to facilitate military intervention, or as in the next examples, witnesses to policymakers' ignorance of events. [follow with quotes from ch 6 Bahador, pgs 97-127 +ADD in Social Engineering 'VNN effect']

The last issue I will bring up to highlight the crimes against humanity which proceeded from the Arab Spring - the crimes taking place in Syrian detention facilities, - show that complicit media technologists and the US State Department have contradicted their own narratives by claiming lack of access to information on crimes.

Two news articles, one published August 2016 by *The Guardian* and the other in May 2017 by *BBC*, both feature satellite images from Google Earth, DigitalGlobe, Amnesty International, and the US State Department of the Saydnaya military torture prison and crematoria, which people are transported to by "meat fridge trucks" and whose bodies are buried in mass graves.[60]

The town name Saydnaya is said to be of Syriac or Aramaic origin, with the meaning being either "hunting place" (from Syriac *suayd dinaya*), or "our new Lady" (from Greco-Aramaic *sayidat naea*).[61] Chilled meat trucks and directed microwave energy, as I will discuss at length, are both weapons of choice of the groups behind these acts. This should not be surprising in a discussion of genocides. Holocaust survivor Elie Wiesel and others wrote about forced and assumed cannibalism and other commercial consumptions of human body parts used as torture against concentration camp prisoners by European Nazis. Religious symbolisms in genocide is shortly discussed in the final section The Greater Middle East Plan, focusing on the political philosophy known as millenarianism or political messianism.

Rather than lacking any information, the article by *The Guardian* relates many details on not only the circumstances of the crimes, but the sordid details of the crimes as continually repeated processes, even using the words "initiation" and "ceremony" to describe the constantly repeated, well-documented stages of tortures and their deeper significance. It does not however attempt to name or describe any of the perpetrators or their organizations, but reduces culpability by distributing guilt to the entire Assad regime, Russia, and Iran. This is vagueness through specificity, a deflection rhetoric; the everyone-is-to-blame strategy is often used by global organizations since their coming into existence in the 20th century to permit and distribute responsibility for genocide. I address this in detail in the section The Bosnia Model, The Rumsfeld Model.

---

[60] Wainwright, Oliver. "'The worst place on earth': inside Assad's brutal Saydnaya prison Syria's most notorious jail has been a journalistic blank spot. Now ex-detainees and architects have built an accurate model, using 'ear-witness' testimony, of the president's hellish torture house". *The Guardian*. 17 August 2016.

[61] "Ṣaydnāyā". *Wikipedia (Arabic).* Accessed 2 January 2020.

The Guardian article describes the process of building a 3-D virtual model of the prison with descriptions from former prisoners of Saydnaya. The article, however, also begins with satellite images of the prison and mentions images collected from Google Earth, which, if imaged using radar imaging known as through-the-wall imaging or ground penetrating radar as many are and the image appears to be, this would reveal the internal structure of the complex and what is directly underground. Technologists building a 3-D model would then be unnecessary to ascertain nearly any information about the structure. Forensic architects, in this case Goldsmiths out of the University of London, are experts in using satellite imaging and 3-D modeling and would be aware of wall and ground penetrating capability of satellite imaging. This raises major red flags over why that information would not be used in a 3-D reconstruction for use in "'architectural forensics', using the designer's spatial toolkit to build damning bodies of evidence used in both UN investigations and trials in the international criminal court."

Likewise, the *BBC* reports that these crimes in Saydnaya are done in "total secrecy", which of course is impossible since the same article also states that, "The [US] state department has released satellite images of the facility which it said was used to hide evidence." Months before the *BBC* article was released, and likely years after the satellite images were collected by the State Department, "Amnesty International said that mass hangings had taken place every week at the jail between 2011 and 2015," meaning Amnesty International admits they also have held knowledge of the crimes for years. Stuart Jones, Acting Assistant Secretary for Near Eastern Affairs in the US State Department has said, "Credible sources have believed that many of the bodies have been disposed in mass graves...We now believe that the Syrian regime has installed a crematorium in the Saydnaya prison complex which could dispose of detainees' remains with little evidence… Evidence of the crematorium hiding or disguising mass murders at the prison will be presented to the international community."[62]

It is therefore impossible that the US has not been aware of this center as a torture and death camp since 2011. In fact, the US government is consistently, if not constantly, made aware by satellite imaging of any new construction or activity occurring in and around Saydnaya. +ADD pandemic crematoria

As the inconsistencies of the industry show in these media reports, I address individuals closely associated with Anonymous and hacktivism, Glen Greenwald of *The Intercept* and Edward Snowden of *Freedom of the Press Foundation*, who continue to refuse to release information collected from 2013 government leaks that would have forewarned of the coming war atrocities in Syria at the hands of Saudi Arabia and the US State Department.

Not only were the coups, wars and human tragedies that were to follow the 2011 Arab Spring movement already planned well before the 2013 Snowden 'leaks', but those events were plotted before 2001. Four-star General Wesley Clark and former Supreme Allied Commander of NATO, describes in a 2007 interview with *Democracy Now!* information he gained during a walk-through of the Pentagon in 2001, weeks after the invasion of Afghanistan began:

---

[62] "Syria's Saydnaya prison crematorium hid killings, says US". *BBC*. 15 May 2017.

> 'I just got this down from upstairs' — meaning the Secretary of Defense's office — 'today.' And he said, 'This is a memo that describes how we're going to take out seven countries in five years, starting with Iraq, and then Syria, Lebanon, Libya, Somalia, Sudan and, finishing off, Iran.'[63]

By 1998, under the Clinton administration, the US was already in talks with the UN concerning US war against Iraq.[64] The 2000 Pentagon quarterly report explicitly called for defense preparedness for US involvement "to fight two major conflicts at the same time, as called for in the national war plan."[65] Three years later, the US would be in that exact situation. And since the Iraq invasion in 2003 the US took no military action amounting to full-scale traditional warfare by US troops, yet several of the countries named by General Clark experienced cataclysmic political change permitted by the Arab Spring movement, including coups, civil war, military operations by outside forces, and partitions.

In June of 2011, former US envoy to Sudan Roger Winter recommended US military intervention in the Sudan to the House Foreign Affairs Subcommittee on Africa, Global Health and Human Rights. In reaction to what he called then-current special envoy General Scott Gration's "seemingly intimate relationship" and the Obama "Administration's commitment to 'reach out' to the Arab and Islamic world", Winter proposed limited warfare against the Khartoum government on the pretext of preventing further border unrest and aerial attacks by the northern Sudanese following the referendum that took place in January of 2011 that would create two separate countries, majorly Muslim Sudan and majorly Christian South Sudan.[66]

Major Jason B. Nicholson is a US Army Sub-Saharan Africa Foreign Area Officer currently posted to US Embassy Uganda 03/29/2013 https://smallwarsjournal.com/jrnl/art/sudan-african-sequel-to-the-arab-spring

In October 2019, protests likened by media to the Arab Spring protests of 2011 have broken out in Sudan and Lebanon…

https://www.washingtonpost.com/world/2019/07/05/sudan-may-follow-perilous-arab-spring-playbook-strongman-falls-his-allies-remain/

https://www.washingtonpost.com/politics/2019/09/05/egyptians-quickly-tired-protest-heres-why-that-matters-sudan-algeria/

https://www.realclearworld.com/articles/2019/10/23/lebanons_oligarchy_under_pressure_113108.html

In August 2020, the explosion in Beirut inexplicably has led to the Lebanese government reducing itself to "caretaker status" … https://apnews.com/article/ap-top-news-international-news-middle-east-lebanon-beirut-598da05d3907aa58399c86ff85a9babc

---

[63] Clark, General Wesley and Amy Goodman. "Global Warfare: 'We're Going to Take out 7 Countries in 5 Years: Iraq, Syria, Lebanon, Libya, Somalia, Sudan & Iran...': Video Interview with General Wesley Clark". *Global Research.* 14 June 2019; *Democracy Now!*. 2 March 2007.

[64] Knowlton, Brian. "Clinton Tries to Reassure UN Leader". *International Herald Tribune*. 12 March 1998.

[65] Cooper, Michael. "THE 2000 CAMPAIGN: THE REPUBLICAN RUNNING MATE; Cheney Urges Rethinking Use of U.S. Ground Forces In Bosnia and Kosovo". *The New York Times*. 1 September 2000.

[66] "Former US envoy calls for military action against Sudan". *Sudan Tribune*. 17 June 2011.

In an apparent compromise in US foreign policy, the situation has gone favorably neither way and has instead followed the 2001 plans relayed by General Clarke to "take out… Lebanon… Sudan." All significant contribution to the contrary has been, in the words of the great English dramatist, "but a walking shadow, a poor player That struts and frets his hour upon the stage And then is heard no more: it is a tale Told by an idiot, full of sound and fury, Signifying nothing."

In sum, my assessment of the agencies and individuals which I analyze throughout the following essay, I have chosen to express in the words of Max Weber. Written a century ago, he describes the pseudo-professional politicians I analyze at present:

> In every one of such cases, I shall draw the conclusion that they have not measured up to their own doings. They have not measured up to the world as it really is in its everyday routine. Objectively and actually, they have not experienced the vocation of politics in its deepest meaning, which they thought they had. They would have done better in simply cultivating plain brotherliness in personal relations. And for the rest – they should have gone soberly about their daily work.[67]

Out of the Blue: Wargames and Wars

The history of war games may include examples more venerable or more important, but surely no more intriguing than the campaign that Uncle Toby and Corporal Trim fight out through the pages of that wonderful and exasperating book, Tristam Shandy. You may remember that Toby, wounded in the leg at the battle of Namur, dug up the lawn, threw up breastworks and fortifications, and indoors moved lead soldiers across the map of Belgium. Next door, the widow Wadman cast eyes on Uncle Toby and gave thought to changing her nonmarital status. Before she could begin her strategic campaign against Toby, however, she had a reconnaissance campaign to conduct, for, though she knew that Toby was wounded in the leg, she lacked the essential elements of information about the extent of Toby's disability.

On second thought, I'm afraid that this is not a fit and proper subject for the scholarly discussion that you and I should be having this morning. Let me turn to another game, one that played an important role in the analysis of national strategy.

Just sixteen years ago a so-called "research institute" was set up, an institute of a very peculiar kind and with peculiarly limited aim…

Robert Specht, *War Games*, The RAND Corporation, 1957

The Arab Spring of 2011 was irregular warfare orchestrated by the US against Arab societies. In this section on wargaming, the reader will observe that the US military has been training for two decades in irregular warfare [ADD Vietnam reference]. The significance of discussing military wargaming is to show in three points that:

1) Tech companies and protesters did not act alone but alongside the Pentagon and the rest of the US intel-security state which is regularly conducting irregular warfare as official policy;

[67] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 128.

2) Wargaming is a misnomer - wargames are in fact practice for definite future military involvement or as cover for simultaneous military action, and;
3) Wargames/continuous simulated warfare act as continuous real irregular warfare.

I am suggesting here in the section Out of the Blue: Wargames and Wars that many of those in the US policymaking and wargaming industries, especially those that have a hand in both, are disruptive actors employing irregular warfare with the willingness to recreate catastrophic events in the US as they have done abroad, all under the guise of wargaming.

The wargames I describe here are criminal plots and military deception operations (MILDEC).[68] A plot is disguised as a wargame to legitimate broad conspiracy in the intel-security community. Wargames function as an alibi-genre for violent plots if the plans are discovered. They also give conspirators insight into the psychology and relationships between individuals in leadership, which they can exploit to better achieve their aims.

+ADD "**The deception target is the adversary decision maker** with the authority to make the decision that will achieve the deception objective. The deception target or targets are the key individuals on whom the entire deception operation will be focused. Within MILDEC, conduits are information or intelligence gateways to the deception target. Conduits may be used to control flows of information to a deception target. **The deception story is a scenario** that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. **It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe** to be the true situation, then decide and act on that basis. The cornerstone of any deception operation is the deception story."[69]

"Successful deception operations are those that do more than make the target 'believe' or 'think' that the deception is true. MILDEC must end in an action, or inaction, that supports the JFC operational plan… Once the planning process is complete, it is critical that constant coordination at the strategic, operational, and tactical level continues to ensure success. The potential for a tactical or operational level deception to have strategic implications is high. With this in mind, a continual process of coordination, called the deception execution cycle, must take place… The termination of a MILDEC is concerned with ending the MILDEC in a way that protects the interests of the deceiver. The objective of a successful termination is to conclude the MILDEC without revealing the MILDEC to the adversary. The DPC [deception planning cell] is concerned about terminating the overall MILDEC, as well as the termination implications embedded in each MILDEC event. Planning how to end an individual deception event in a way that does not leave suspicious traces of the MILDEC operations is an inherent aspect of MILDEC event preparation… The MILDEC role during the early phases of an operation will be based on the specific situation of the operation or campaign to help set conditions that will facilitate phases that follow."[70]

---

[68] From Joint Forces Staff College *Military Deception:* Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

[69] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. vii-viii

[70] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. xi-xiii, I-1.

"MILDEC may be conducted to: support redeployment or withdrawal operations; protect sensitive operational capabilities from being revealed; establish favorable conditions for subsequent military operations; support possible counterinsurgency operations; defend or rebuild critical infrastructure; and aid in the transition of responsibility to civil control or other authority… MILDEC often requires substantial investments in effort and resources that would otherwise be applied against the adversary in a more direct fashion."[71]

Because these wargames are plots for criminal wars entailing mass murder and sex crimes as irregular warfare, I take into account FBI profiler Roy Hazelwood's profiles of organized crime. His guiding rule states that to understand sexually motivated serial crime, one must begin by analyzing the fantasy world of the criminals. "The crimes are fantasies being acted out. The more complex the crime, the more complex the fantasy and the more intelligent the offender… All sexual crime begins in the fantasy world of the offender ."[72] This is the theoretical concept behind this essay's focus on wargames, scenarios and modelism. This methodology is applied limitedly throughout the essay, and is shown to be prevalent in irregular warfare conduction and among the groups responsible for the Arab Spring. [REWORD]

+ADD " US: Terrorism Prosecutions Often An Illusion"
https://www.hrw.org/news/2014/07/21/us-terrorism-prosecutions-often-illusion# "'Americans have been told that their government is keeping them safe by preventing and prosecuting **terrorism inside the US**,' said Andrea Prasow, deputy Washington director at Human Rights Watch and one of the authors of the report. '**But take a closer look and you realize that many of these people would never have committed a crime if not for law enforcement encouraging, pressuring, and sometimes paying them to commit terrorist acts.**'… In the case of the 'Newburgh Four,' for example, who were **accused of planning to blow up synagogues and attack a US military base, a judge said the government 'came up with the crime, provided the means, and removed all relevant obstacles,'** and had, in the process, made a terrorist out of a man 'whose buffoonery is positively Shakespearean in scope.'";

"Government agents 'directly involved' in most high-profile US terror plots"
https://www.theguardian.com/world/2014/jul/21/government-agents-directly-involved-us-terror-plots-report

+ADD "The FBI's Role in a War Zone":

"Special Agent Tom Krall: My first taste of terrorism was 9/11 standing underneath the World Trade Center as it came down. I was about a block away. I lost a lot of friends. And I know it all started right here. And it's very important for me to make sure that that doesn't happen again.
[Announcer:] Ladies and gentlemen, welcome to Afghanistan. The local time is 35 minutes past 6 a.m.
Special Agent Bob Jones: **The biggest thing we do here is protect the homeland from afar.** We know that it's a long fight against adversaries want to bring harm to the United States for whatever reason from overseas. And we need to be prepared to combat that wherever that might happen. So that's a big part of our job here.

---

[71] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-2 – I-3.

[72] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 11.

U.S. Ambassador Karl Eikenberry: The FBI is the shield in the United States of America. **What 9/11 taught us is you can't defend from the shoreline the United States of America against terrorism. You have to have the shield extended globally.**
Gen. David Petraeus: The FBI is the premiere **law enforcement and investigative** agency in the world. And so when it contributes to this kind of effort it brings unique capabilities…
Special Agent Derek Boucher: When I go back to the states and my squad in Philadelphia **I'm going to basically I think be a subject-matter expert.** I'm seeing things just with my own eyes. And that's something you can't really see in the news.
Special Agent Bob Johnson: **We've been able to bring an investigative capacity here to address corruption and kidnapping and organized crime**…
Special Agent Krall: It's awesome work. I did organized crime for 10 years in New York. And them to me, right over here, **trying to go against the Taliban is organized crime**.
Ambassador Eikenberry: It's a highly professional organization. It's disciplined, serious, mission-oriented, always focused. And so, as the United States ambassador, I've got to say when it comes to just trying to inspire **all the tribes in the U.S. mission here I like to have the FBI tribe** out front."[73]

In the paradigmatic *How Wars Begin*, A.J.P. Taylor writes on the US self-help security apparatus dependent on wargaming and scenario planning:

> I was reading just the other day a fascinating account of American military and strategic plans between the wars, at a time when neither Germany nor Russia was a danger. The American strategists had to justify themselves so they sounded the alarm that America was always in danger. After all if your country is not in danger you would not have an army or an air force or a navy and that would never do for the people who are running the army, the air force and the navy. So what did the army strategists in America discover **in the middle of the 1920s? They discovered that a country called Red, which was in fact the United Kingdom, was preparing to invade White, which was the United States, with an army of 8 million men in order to destroy the whole of American industry. This was not some fantasy of a novelist. It was the work of a serious strategical planner**, trained in the staff colleges and sitting down in genuine alarm that any day a new Armada might be sighted crossing the Atlantic, landing in Canada, and then 8 million British troops marching I suppose on Chicago**. 'Ah,' you may say, 'a fantasy; they didn't take many steps about it'. In fact they did. The Americans recast their strategical thinking entirely in face of the supposed danger** from the British on the one side and Japan on the other, and the reason why in 1941 the Americans put Germany first was simply that they had put the other European danger – England – first fifteen or twenty years before… All the world statesmen now are rather humdrum secondary people who are unlikely to aspire to be world conquerors. **The one force which still aspires to conquer the world is the planning staffs. They will produce the alarms and frights.**[74]

+ADD RAND publication 10 Common Pitfalls definition of modeling "MODELISM: We shall start by considering what is to many people, the heart and soul of Systems Analysis—the use and abuse of models. We have already explained that it is necessary to use idealized

[73] Federal Bureau of Investigation. "The FBI's Role in a War Zone". U.S. Department of Justice FBI webpage. 18 April 2011.
[74] Taylor, A.J.P. *How Wars Begin.* Ebenezer Baylis & Son Ltd. 1979, p. 159-161; 174-175.

models which abstract essentials and make assumptions explicit." RAND's foremost founder then goes on a lengthy explicit analogy of a young (in 1957) systems analyst who may end up looking at pin-up pictures of female models rather real women, and adds an equally lengthy footnote stating that:

> There are delectable girls all around to tempt our 'mature heterosexual adult' away from this dummy, but what can our poor Systems Analyst replace his model with? Another one! Even if he wanted a war he couldn't have one. (Of course, as any psychologist will tell you, the comparison is not so unfair. Some fantasies are nicer than some real girls.)

Researchers looking at early RAND Corporation publications for information on foundations of their methodologies, concerning Modeling or otherwise, will encounter little of use on the actual topic, and instead a lot of posturing drivel meant to mean practically nothing of use. This is likely intentional in order to hide how they have in fact practiced and how they have no true methodologies at all. Except of course what is revealed – that analysts have been trained since the existence of such jobs to treat their jobs as opportunities for sexual exploitations and are trained to consider war as opportunity for personal sexual predation.

This is an example of how brazenly ridiculous think-tanks like RAND have been since their inception, and they have been encouraged and funded only by the like-minded. The highly sexualized frameworks in which their analysts have long been encouraged to view war and analysis is explained in recent US war histories. It is no mystery at all why sex crimes of human trafficking, pedophilia, rape, and sexual tortures of prisoners are so ubiquitous today in American security-intel and military industries. US security analysts have been trained for 70 years to treat their appetite for war as a sexual appetite and their sexual appetite as an appetite for war. I however do not call this orientation 'mature', 'male', nor 'heterosexual'.[75] [REWORD repeated]
+ADD [on rise in child kidnappings immediately following US invasion in 2003] https://www.csmonitor.com/2003/0910/p05s02-woiq.html "Kidnapping in Iraq on the rise Amid unrest, Iraqi gangs have begun abducting women and children for ransom." September 10, 2003 By Ilene R. Prusher ; https://www.theguardian.com/world/2003/oct/15/iraq "Child kidnapping on the rise in Iraq" by Dominic Nutt Wed 15 Oct 2003 ; https://reliefweb.int/report/iraq/iraq-focus-increase-kidnappings "Iraq: Focus on increase in kidnappings" 11 April 2005 ; https://www.rand.org/blog/2005/04/kidnappings-in-iraq-strategically-effective.html "The RAND Blog Kidnappings in Iraq Strategically Effective" COMMENTARY (Chicago Tribune) by Brian Michael Jenkins, Meg Williams, Ed Williams April 29, 2005

+ UK criminal profiles of Westerners who join ISIS as "typically watch porn… literally wankers… severe onanists."[76]

To illustrate the deviant criminal nature of the US intel-security industry, Special Agent Roy Hazelwood describes FBI Quantico's intel-security culture in 1976, which spurred in part the formulation of his theory on deviant sex crime. He describes the study of sex crimes as practically nonexistent in the FBI when he first assumed his position.

---

[75] Kahn, Herman and Irwin Mann. *Ten Common Pitfalls.* The RAND Corporation, Santa Monica, California. 17 July 1957, p. 1-2.
[76] Perraudin, Frances and Shiv Malik. "Boris Johnson: jihadis are porn-watching 'wankers'". *The Guardian.* 30 January 2015.

Hazelwood was instructed to make his lectures "porno shows for cops" and to never allow women in his lectures. His predecessor left him an empty broom closet with a desk in which to work. The FBI's so-called Behavioral Science Unit Office was filled with pornography magazines and videos, bottles of personal lubricants, sexual fetish toys, and a sado-masochist's whip hanging on the wall under a sign that read "Without Pain There Is No Pleasure".[77]

As Hazelwood's experience indicates, the US intel-security industry itself is populated and governed by deviant criminality. The profession, which gives access to weapons, control and sex acts, is a vital part of those groups' deviant criminal fantasy world. Wargaming, scenario acting and surveillance facilitate these deviant groups' desire to act out their dark imaginings.

This characterization is not simply speculation but is supported by International Criminal Court (ICC) accusations that US intel-security members "committed acts of torture, cruel treatment, outrages upon personal dignity, rape and sexual violence against conflict-related detainees in Afghanistan and other locations." In response, former CIA Director and Secretary of State Mike Pompeo has volunteered the entire US government to do anything to defend the deeds of his own deviant colleagues. [78] This account displays the ways in which the intel-security industries' deviant crimes are legitimized at the policy level by individuals of the same industry. Professor and Editor of *Security Studies* journal Randall Schweller has termed this "the inescapable self-help nature of the system."[79]

Hazelwood's rule is adapted to the war context along with theory on rape as a weapon of war, also known as the strategic rape concept.[80] These concepts for analyzing sexually motivated and deviant serial crime at the organizational level are the impetus for beginning this essay with an extensive discussion of wargames and wargaming culture, as wargames are the "fantasy world" prelude to US military and policing action, and the basis for establishing irregular warfare as policy.

+ADD "Sexual sadism is a persistent pattern of becoming sexually excited in response to another's suffering… Inflicting pain is a means to create suffering and to elicit the desired responses of obedience, submission, humiliation, fear, and terror… The critical issues are whether the victim suffered, whether the suffering was intentionally elicited, and whether the suffering sexually aroused the offender… Only sexual sadists intentionally inflict that suffering, whether physical or psychological, to enhance their own arousal. Neither the severity of an offender's cruelty nor the extent of a victim's suffering is evidence of sexual sadism. Acts of extreme cruelty or those that cause great suffering are often performed for nonsexual purposes, even during sexual assaults."[81]

---

[77] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 85-87.

[78] Shesgreen, Deirdre. "Pompeo says US will take 'all necessary measures' to bar war crimes probe of military". *USA TODAY*. 5 March 2020.

[79] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 90.

[80] ISIS's Use of Sexual Violence in Iraq ADD CITE

[81] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 12-13.

+ADD "The behavior of sexual sadists, like that of other sexual deviants, extends along a wide spectrum. Sexual sadists can be law-abiding citizens who fantasize but do not act or who fulfill these fantasies with freely consenting partners. Only when sexual sadists commit crimes do their fantasies become relevant to law enforcement. Sadistic Fantasy: All sexual acts and sexual crimes begin with fantasy. However, in contrast with normal sexual fantasies, those of the sexual sadist center on domination, control, humiliation, pain, injury, and violence, or a combination of these themes, as a means to elicit suffering. As the fantasies of the sexual sadist vary, so does the degree of violence. **The fantasies discerned from the personal records of offenders are complex, elaborate, and involve detailed scenarios that include specific methods of capture and control, location, scripts to be followed by the victim, sequence of sexual acts, and desired victim responses. Sexual sadists dwell frequently on these fantasies**, which often involve multiple victims and sometimes include partners… Consenting or Paid Partners: **Sexual sadism may also be acted out with freely consenting or paid partners, e.g., prostitutes who specialize in roleplaying the "submissive" for sexually sadistic clients. The nature of the acts varies from simulations of discomfort to actions that result in severe injury**… **Careful planning epitomizes the crimes of the sexual sadist**, who devotes considerable time and effort to the offense. Many demonstrate cunning and methodical planning. **The capture of the victim, the selection and preparation of equipment, and the methodical elicitation of suffering** often reflect meticulous attention to detail. **The overwhelming majority of offenders we studied used a pretext or ruse** to first make contact with the victims**. The sexual sadist would offer or request assistance, pretend to be a police officer, respond to a classified advertisement, meet a realtor at an isolated property, or otherwise gain the confidence of the victim**. Almost invariably, the victims were taken to a location selected in advance that offered solitude and safety for the sadist and little opportunity of escape or rescue for the victim. Such locations included the offender's residence, **isolated forests, and even elaborately constructed facilities designed for captivity**… These offenders retained a wealth of incriminating evidence. **More than one-half of the offenders in our study kept records of their offenses, including calendars, maps, diaries, drawings, letters, manuscripts, photographs, audio tapes, video tapes, and media accounts of their crimes**."[82]

+ADD "A member of the Bureau's elite Behavioral Science Unit, based at the FBI Academy at Quantico, Virginia, Roy's domain is the sexual criminal's mental and emotional planes, the deviant mind's hot zones where lust and rage are fused, and deadly fantasies flower."[83]

There are six major ways in which the crimes of organized criminal sexual deviants and the crimes committed through wargames may be understood under the same criminological profile:

---

[82] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 13-14; 19-20.

[83] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 4.

1) "most dangerous of deviant criminals, marked by their wildly complex fantasy worlds, unequaled criminal cunning, paranoia, insatiable sexual hunger, and enormous capacity for destruction".[84]
2) characterized by experienced, mature, highly organized planning.[85] [86]
3) thrive on the publicity and community impact surrounding the crimes.[87]
4) "whole new criminal character emerging from power assertive to 'anger excitation' sadist" whose "level of violence applied is matter of satisfying self, not overcoming resistance" (Clausewitzian total warfare; individual profile of domestic rapists as military forces – the Ski Mask Rapist – ski masks common to battlefield deviant crimes).[88]
5) use of term 'the Games' by individual deviant criminal veteran to indicate ritualized, scenarioed crimes involving sodomy, cages, torture, recording devices, post-mortem violation, incinerator for bodies – "'the Games'…were really reenactments" [relate to modelism] in which victims said they "rehearsed their own deaths."[89]
6) "The more complex and sensational the case, the more likely the perpetrator is a male of European descent."[90]

"Hazelwood returned to the prosecutor's office and advised him to indict [John Kenneth] Register for the phone calls. 'That's ridiculous!' Wilson said. 'I'm faced with trying to convict a man for the most heinous murder this county has seen in a century, and you want me to convict this same person for obscene phone calls?' 'Yes!' Roy answered, '**because he was verbalizing his fantasy.** That young man was masturbating to those fantasies, which he later acted out in the murder. **You can show the jury what he did, and also show them what he said he was going to do years earlier.**'"[91], "Hazelwood and Douglas felt that **over a period of time the fantasy grew increasingly important to him even as it became ever more untenable**. He began to feel betrayed. **'She was his girlfriend,' explains Hazelwood. 'She didn't know that. But *he* knew it.'** The agents told the Canadian investigators that the killer would have been very agitated in the days following the double murder. **He'd be obsessed by the press coverage. He quite likely attended Chloe's funeral**… She had been further troubled by Antoine's **obsessive interest in the crime's aftermath**. He carried around a photo of Chloe in **a notebook he**

[84] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 11.
[85] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 68-69.
[86] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 74-76.
[87] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 68-69.
[88] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 106-109.
[89] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 219-221.
[90] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 13.
[91] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 169.

filled with newspaper clippings about the case."[92] This criminological phenomenon in wargaming and scenario-based policymaking is explored in the section Horseshoes and Hand Grenades.

+ADD "The prosecutor then produced the coded three-by-five cards and spiral notebook seized from [James] Ray Ward's house. Roy looked over the material and said he had carefully examined seventy-six of the cards. He told the jurors Ward **had put together a highly organized cross-referenced rating system for erotic photos…** A spiral notebook contained a complementary classification system… The notebook's code was the same as for the cards… 'Those cards and that notebook were amazing,' John Bass recollects. 'Ward had everything indexed, cross-referenced, and organized. He would have made a perfect file clerk.'**… 'The primary functions of an MO [modus operandi] are to protect the identity of the offender, ensure control the victim, and facilitate his escape**.'"[93] This criminological phenomenon in wargaming and scenario-based policymaking is discussed in the section Cyber Realism and throughout this essay. [relate to Snowden NSA article, MAXAR NewsBureau & Clooney int'l security surveillance article]

"[Harvey 'The Lonely Hearts Killer'] Glatman's victims believed he was photographing them for detective magazine covers."[94] The criminological phenomenon in wargaming and scenario-based policymaking of explaining away publicized crimes by presenting the crimes as fiction, or plotting to-be-publicized crimes under the guise of speculative fiction, is addressed in the section The Spectacular Security State.

"The organized offender, by contrast, is **a planner**. He **brings his own weapons**, or restraints, **hunts away from where he lives or works, normally has no traceable association with his victim,** and **takes steps to conceal the body**, as well as **to remove evidence**. He'll take care not to leave fingerprints, body fluids such as blood or semen, or spent cartridges and shells. He is usually older, as well as more mature, than the disorganized offender. He prefers to commit his crime in seclusion, and **often transports his victims to a second location** for disposal. He is **not necessarily concerned if she ultimately is discovered, because the publicity surrounding her death and its impact on the community can be highly exciting to him**… **This was an experienced, mature, and highly organized offender. He planned his crimes, brought what he needed with him**, concealed his identity, chose an advantageous moment (closing time) to strike, eliminated half the possible witnesses against him (the other were left for dead, his single oversight), **and removed potential physical evidence (the shells) before leaving**."[95]
"For the past year, Baton Rouge and jurisdictions in many **other states had shared a common problem, a particularly vicious traveling sexual criminal and thief known**

---

[92] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 101.
[93] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 171-172.
[94] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 102c.
[95] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 68-69.

as the Ski Mask Rapist… The level of violence applied by a sex offender is part of his ritual, not his MO. 'How much physical force a rapist uses against his victim is a matter of satisfying himself, not simply to overcome her resistance,' Hazelwood explains. The Ski Mask Rapist therefore seemed to Roy to be **evolving from a power assertive rapist, who applies moderate force or coercion, toward sexual sadism**. His psychosexual needs were changing. **A whole new criminal character was emerging**… Roy speculated that the rapist had served in **the military and had chosen the ground forces – the army or marines** – because to him those were the most manly services to join… The Ski Mask Rapist was single and never married, Roy believed, for the same reasons… His demonstrated ability to learn indicated he was at least of average intelligence. Based on the BSU's familiarity with other offenders who fit this profile, Hazelwood further **believed the rapist's education or training extended beyond high school, possibly including college. He either was currently employed in a job requiring some sort of special skill**, Roy thought, or once had worked in such a position. Although never married, the Ski Mask Rapist had ongoing consenting relationships with various women, again a conclusion based on BSU research, but he would never be faithful to any of them. Roy's final conclusion was in fact an admonition. **The Ski Mask Rapist was growing ever more violent.** Hazelwood predicted that unless he was caught, he seemed likely someday to cross the threshold and become **the Ski Mask Killer**."[96]

"Roy's key finding was DeBardeleben's criminal sexual sadism. For such offenders, sex and suffering are one and the same. This perversion, or paraphilia, is surpassingly unusual, even among sexual criminals. But those who harbor it are **the most dangerous of all aberrant offenders**. They are the great white sharks of deviant crime, **marked by their wildly complex fantasy worlds, unequaled criminal cunning, paranoia, insatiable sexual hunger, and enormous capacity for destruction**… **Hazelwood commenced my tutorial where all sexual crime begins, in the fantasy world of the offender**. As he explains it, 'I teach police officers what I call **Hazelwood's Golden Rule of sexual crimes. 'The crimes are fantasies being acted out. The more complex the crime, the more complex the fantasy and the more intelligent the offender**… On the other hand, consider an impulsive offender… you'll probably find this guy is of average, or less intelligence. He'll have little, if any, criminal sophistication. He's only got one thing on his mind, as opposed to this other offender **who has all this stuff mixed up with what he *calls* sex**.'… In Hazelwood's experience, white males of European descent predominate among aberrant offenders to an extent unrivaled in any other crime category, save perhaps white-collar crimes. 'Every single sexual deviation is overwhelmingly dominated by white males,' he says. 'And most sexually related ritualistic crimes are committed by white males.'… **The more complex and sensational the case, the more likely the perpetrator is a male of European descent**."[97] [Relate as insight into the media spectacle of war proven by CNN effect – mediatized violence excites to action and becoming involved in the violence. The implicit sexual and sadistic nature of crimes in wartime and the visualization of corpses and suffering which

---

[96] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 106-109.

[97] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 11; 13.

excites/promotes action in the viewer into becoming a participant was not addressed in *The CNN Effect in Action*].

"The most dangerous to all his victims **is the 'anger excitation rapist,' the sexual sadist who is sexually stimulated by his victim's suffering**. None of these rare and enormously destructive offenders has left a fuller record of himself than Mike DeBardeleben… He left behind sheaves of handwritten notes, underlined passages in text, drawings, and tape recordings in which he created a detailed record of his desires and deeds. 'This is a tape regarding my goals,' DeBardeleben begins on one undated tape recording. 'Number one on my list of goals is to establish a new identity, complete with background, school records, employment records, driver's license, Social Security card, passport, checking accounts, savings accounts… **This new identity would not be traced to me under *any* circumstances. It may have to be set up in a different location, a different city**… Naturally, of course, I would need as a requirement secret hidden compartments built into the house for stash areas, for various things… along with the **secret work area for a press and darkroom facilities, a fun area – secret fun area – which would include a cage** so that I could have an SMB [DeBardeleben's code for sadomasochistic bitch] locked up! Also of prime importance – **top priority – would be an incinerator** capable of incinerating at extremely high temperature – total incineration'… 'Sadism,' DeBardebelen wrote: 'The wish to inflict pain on others is not the essence of sadism. The central impulse is to have complete mastery over another person, to make him/her a helpless object of our will, **to become the absolute ruler** over her, **to become her god**, to do with her as one pleases, to humiliate her, **to enslave** her are means to this end. And the most radical aim is to make her suffer. Since there is no greater power over another person than that of inflicting pain on her. To force her to undergo suffering without her being able to defend herself. The pleasure in the complete domination of another person is the very essence of the sadistic drive.' 'Investigators,' explains Hazelwood, 'find **no other sexual crime as well planned and methodically executed as that committed by the anger excitation rapist. Every detail is carefully thought out and rehearsed, either literally or in the offender's fantasies. Weapons and instruments, transportation, travel routes, recording devices, bindings – virtually every phase has been pre-planned**…"[98].

+ADD "Then one day she decided to clean and straighten Jack's '**War Room.**' 'It was his personal shrine to two tours of duty in Vietnam,' she says. 'The walls were covered with certificates, maps, guns, ammunition belts, knives, and **photographs of dead Vietnamese soldiers**.' As Michelle was cleaning, she came upon a ratty old reddish pink suitcase in a closet. She opened it to find it stuffed with sadomasochistic pornography, most of it **depicting women being sexually brutalized.** She found Ace bandage rolls and scalpels in the worn suitcase, too. There also were broken arrows. She'd soon learn their use… 'He assured me it was only a game, and that no one really gets hurt.' Jack explained what he required in detail. **He called his fantasy 'the Games,'** and said they unfolded in five episodes: (1) Capture, (2) Struggle, (3) Torture, (4) the Final Kill, and (5) Postmortem Rape. The moment he began describing what he wished for her to do, Michelle had the feeling that Jack had done this many times in his past – **that 'the Games' were really a reenactment.** 'I always felt deep in my heart that he'd done this

[98] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 74-76.

before, that he'd killed women,' she says. 'I felt I was **rehearsing for my own death**.'… Sometimes 'the Games' were played under strobe lights to the accompaniment of sixties-era hard rock… Although Jack at first said 'the Games' would be an infrequent thing, in time they became **nearly constant**."[99]

On the sexual sadist attracted to "ground forces" work: "While he envies **the power and authority associated with the police, he does not respect it**… **Because offenders retain incriminating evidence and crime paraphernalia**, these items should be listed in search warrant applications. This would include **records and mementos,** as well as **photographic equipment, tape recorders, reverse telephone directories, and weapons or other instruments used to elicit suffering. Pornography, detective and mercenary magazines, bondage paraphernalia, women's undergarments, and sexual devices** are other materials commonly collected by sexual sadists."[100]

"Interrogative Cruelty: Torture during interrogation may involve sexual areas of the body, which is sometimes misinterpreted as being sexually sadistic in nature. Case: A government agent was captured in another country. During his months in captivity, he was continually subjected to physical torture, including beatings with clubs and electrical shocks to all parts of his body, even his genitals. The victim was tortured in this manner to obtain information concerning his government's activities in that country, not to enhance sexual arousal."[101]

"Sanctioned Cruelty: History is replete with **reigns of terror during which powerful institutions sanctioned atrocious behaviors. Consider the rape and plunder of defeated populations** during the Crusades of the Middle Ages, or **the execution of women during the Salem witch hunts** in colonial America. One of the most notorious times of cruelty occurred in the 20th century, when millions of people fell victim to **the Nazis**… **In an likelihood, sexual sadists volunteered to perform such deeds, but the widespread deployment of such tactics was politically and racially motivated."[102]**

"Sexually sadistic offenders commit well-planned and carefully concealed crimes**. Their crimes are repetitive, serious, and shocking, and they take special steps to prevent detection**. The harm that these men wreak is so devastating and their techniques so sophisticated that those who attempt to apprehend and convict them must be armed with uncommon insight, extensive knowledge, and sophisticated investigative resources."[103]

"The absence of a common feature among crimes does not eliminate the possibility of a single serial offender, for **he may be experimenting with various techniques in search of the perfect scenario or may be attempting to mislead** investigators. **The 30 sexual sadists studied also inflicted psychological suffering** on their victims. **Binding, blindfolding, gagging, and**

---

[99] Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood's Journey into the Minds of Sexual Predators.* St. Martin's Press: NY. 1998, p. 219-221.

[100] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 15.

[101] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 16.

[102] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 16.

[103] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 20.

holding a victim captive all produce psychological suffering, even if not physically painful. Other **psychological tactics** used included threats or other forms of verbal abuse, **forcing the victim to beg, plead**, or describe sexual acts, telling the victim in precise detail what was intended**, having the victim choose between slavery or death, and offering the victim a choice of means by which to die.** Offender Characteristics: **All 30 of the sexual sadists in the study were men, and only one was non-white.** Fewer than one-half were educated beyond high school. One-half used alcohol or other drugs, and **one-third served in the Armed Forces**. Forty-three percent were married at the time of the offense… Forty-three percent of the men participated in homosexual activity as adults, 20 percent engaged in cross-dressing, and **20 percent committed other sexual offenses, such as peeping**, obscene phone calls, and indecent exposure. Case: As a teenager, one sexual sadist "peeped" throughout his neighborhood, masturbating as he watched women undress or have sex. At home, he masturbated repeatedly to fantasies in which he incorporated what he had seen while peeping. As a young adult, he made obscene telephone calls, which lead to his first arrest when he agreed to meet a victim who informed the police. He later exposed himself to a series of victims, which he eventually explained was **for the purpose of eliciting their "shock and fear."** He followed women home from shopping malls, determined how much cover was available for **peeping and entering the residence**, and eventually raped a series of women. In his early rapes, he depended on weapons of opportunity, but later, carried with him a rape kit, which consisted of adhesive tape, handcuffs, precut lengths of rope, and a .45- caliber pistol**. He became progressively violent in his sexual assaults, torturing his victims** by beating, burning, and pulling their breasts. His violence escalated to the point that he so severely pummeled one victim that she lost both breasts. He forcibly raped more than 50 women and was contemplating murder when he was finally apprehended."[104]

The scientific fields' heavy contribution to deviant crimes in the modern age makes relevant the link between animal cruelty, in this case in laboratory settings, and deviant serial crime committed against people. "animal abuse crimes need to be taken seriously by all levels of the criminal system is that these types of offenses are often co-occurring crimes with other offenses such as domestic violence, child abuse, elder abuse, or sexual abuse or serve as precursors to other more violent offenses up to and including homicide… in late 2014 the FBI announced that it would upgrade animal cruelty crimes to class A, putting them in the same category as felony crimes such as homicide and assault… animal cruelty can be an indicator of future violent crimes—as noted in the next section relating animal abuse to sexual assaults, school shootings, and serial killers… Animal fighting in particular has been linked to gang, weapons, human trafficking, gambling, and narcotics offenses… Since the 1960s, criminologists, psychiatrists, and other investigators have focused on animal cruelty as symptomatic of individuals' later tendency to violence in general and to extreme violence in particular. The FBI and other law enforcement agencies have recognized the high incidence of repeated animal abuse in the adolescence of the most violent offenders including serial killers, serial rapists, and sexual homicide perpetrators… the malicious youngster rehearses his sadistic attacks—perhaps on animals, perhaps on other people, perhaps on both—and continues into his adult years to perpetrate the same sorts of sadistic acts on human beings… In fact, animal cruelty appears earlier than bullying, cruelty to people, vandalism, or setting fires… [7 criminological

[104] Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. "The Criminal Sexual Sadist". *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. United States Department of Justice Federal Bureau of Investigation. February 1992, p. 17-18.

motivations identified by Utah State University Psychology Professor Frank R. Ascione and colleagues relevant to scientific war crimes and crimes against humanity:]
1) Curiosity or exploration (i.e., the animal is injured or killed in the process of being examined, usually by a young or developmentally delayed child).
2) Peer pressure (e.g., peers may encourage animal abuse or require it as part of an initiation rite).
3) Mood enhancement (e.g., animal abuse is used to relieve boredom or depression)…
5) Forced abuse (i.e., the child is coerced into animal abuse by a more powerful individual)…
9) Post-traumatic play (i.e., re-enacting violent episodes with an animal victim).
10) Imitation (i.e., copying a parent's or other adult's abusive 'discipline' of animals).
12) Rehearsal for interpersonal violence (i.e., 'practicing' violence on stray animals or pets before engaging in violent acts against other people)."[105]

The COVID-19 pandemic is addressed in the section 'A Live Exercise' as a premeditated scenario carried out in the real world with, not a viral pathogen, but electronic warfare. Because the physical and emotional damage caused by electronic weaponry may be surveilled and covered by media, it is criminologically prudent to allow that the persons executing the electronic operations and informational sabotage of medical intervention may be sadists. On this observation, COVID-19 has repeatedly been described as creating "a world of pain": https://njbiz.com/a-world-of-pain-hospital-revenues-covid-19/ ; https://www.nreionline.com/retail-cre-market-study/exclusive-research-world-pain ; https://www.irishtimes.com/life-and-style/health-family/melbourne-in-a-world-of-pain-as-coronavirus-lockdown-bites-1.4344789 ; https://www.fsg.org/blog/end-year-reflections-2020 ; https://9now.nine.com.au/60-minutes/update-coronavirus-a-world-of-pain/04ec59b3-b989-48be-93f7-e5cb07a5766e ; https://www.ft.com/content/97c51a2a-e600-402e-9015-95d3ba32ab05 ; https://finance.yahoo.com/news/coronavirus-augurs-world-pain-stock-163413843.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJeRCOHm7RW4kHaHU71cBASKxS1BEDD7zQHvAUxMMKQiRxI6gfVjZadpIC6-DgU4Jt03FesLvigXlmeKGW8a9UA8VqVJgsxhEK1pGATgwdEjxyPgU5SWpxk0q30e2u5SZY4li_QrgnH_BP4nSMESySraUTIX5yTQjGNe7MNQtK52 ; https://www.washingtonpost.com/health/covid-athletic-injury-therapy/2020/09/04/5feeee3c-d736-11ea-9c3b-dfc394c03988_story.html ; https://www.counterpunch.org/2020/09/16/smoke-and-mirrors-in-a-world-of-pain/ ; https://www.nbcbayarea.com/news/local/south-bay/chachos-restaurant-in-san-jose-closes-for-good/2427498/ ; https://www.crikey.com.au/2020/09/17/coronavirus-pandemic-punishments/ ; https://www.christushealth.org/trinity/foundation/giving/grateful-patient/stories ; https://9now.nine.com.au/60-minutes/coronavirus/6422bd57-ccb2-46f7-a5f7-ffb0f4ec6a13 ; https://nj.gov/governor/news/news/562020/approved/20201209b.shtml ; https://www.king5.com/article/news/health/coronavirus/san-diego-county-board-of-supervisors-discuss-ways-to-help-small-businesses-during-pandemic/509-be178a79-8456-4b0d-9a2a-6b52cafc20e3

[105] National Sheriffs' Association. *Animal Cruelty as a Gateway Crime.* Office of Community Oriented Policing Services U.S. Department of Justice. 2018, p. 2-3; 5-6; 11-12.

This is to say that if the COVID-19 pandemic is driven by a sufficient number of strategically placed sadists, one should expect the suffering inflicted to escalate in violence and events to grow increasingly traumatic. This is echoed again and again by policy analysts who state that "things will get much worse before they get better." This should not be expected to happen. Sadists, sexually motivated or not, typically do not stop on their own, but only escalate. The persons responsible for the operations and the failed policies creating the pandemic-related crises would have to be stopped by external forces. The COVID-19 pandemic, scenarioed as other real-world pandemic had been before it, can be seen as the culmination of multiple staged pandemics which went unaddressed as deliberate. The topic of escalating violence premeditated through wargaming is addressed in the section 'Total' Speculative Fiction.

[TOPIC- wargames as policymaking]

Wargames are sold for profit earning the security and intelligence industries hundreds of millions every year. Wargames, but especially real violent events, create high revenue topics for media coverage. Throughout this essay, the intel-surveillance and public policy industries are shown to be the real creators of news media coverage, as they are the legitimate monopoly holders on satellite telecommunications and information distribution.

If the media event can be portrayed as a failure of elected government and current policy, it will undermine free governance, meaning tax-payed officials. This creates more demand for private industry, and empowers the private sectors to eventually eclipse elected government's role as free and primary governors of the nation. Entire government departments which exist on unlawful premises, especially those occupied with warrantless surveillances and undeclared wars, are empowered as public demands for 'greater transparency' and 'immediate action' grow in response to news stories and real events.

Once the wargame is conducted and the beyond-coincidence real event occurs, it is no surprise that the same people who constructed the scenario are poised to offer policy solutions to the ensuing crisis. Real world policy is sold for enactment for that crisis as well, constituting more [$ - find estimate] worth in contracts. When the policy is enacted, it invariably empowers the intel-security industry which sold it. Because the attack or crisis occurs as predicted by intel-security scenarioists, it gives the industry credibility and inspires confidence in their risk forecasting. The more often violent attacks occur, the more the intel-security apparatus is funded and expanded.

In material industries, the production of a faulty product intended to become obsolete earlier than advertised is known as planned obsolescence. However, the risk inherent for material industries that produce with planned obsolescence does not exist for the intel-security policy industries. Because the industry's entire function is to identify and eliminate threats, competition is easily scoped out and neutralized for profit. Information about the policy 'product' as ill-designed, and soon to be made obsolete by another crisis or media report, is easily withheld, also for profit, because withholding and releasing information is another legitimate role of the intel-security industry. Behind it all, of course, is that managing risk and steering risky policy is the forte of intel-security specialists, and minor economic risks like those created by product planned

obsolescence are child's play to such experts. In this case, current conditions of the market are made obsolete in order to recreate the market for new policy product.

Policymakers would only risk exposure of their techniques between policymakers and politicians purchasing the policy because politicians' careers rely on being the ones who take credit publicly for policy decisions. So, if it appears policy decisions are manipulative, worthless, purposely ill-designed, or that a competing politician has better policy to offer, the politician's career suffers. Meanwhile the same policymakers are writing policy for the competing politician. So, writing pitfalls into one or the other's policy that the competition may take advantage of makes little difference to the policymaker, as they will only create business with one by harming business with the other. This is planned obsolescence in that it shortens the replacement cycle of politicians as *products* of the policy industry to the taxpayer – one disgraced politician creates public demand for ten more, which means all new contracts and 'product' designs for the policy industry.

By the time a politician has figured out their own planned obsolescence in the policy industry system, they have lost their role as *customer* to the policy industry. If a politician does not politely exit the purchase line when they do not have a policy purchase to make, or if they will not make room for new politician customers, a policy failure will be sold to them by the policy industry. After this sandbagging, the politician can do little to recoup losses or disclose who is really behind the failure because the policy failure will be specifically chosen to be one which will divest him or her of information credibility and public trust. The whole process can create a great amount of entertainment for the policymakers as well, which helps to inspire the political storylines. This effervescence serves to benefit the politician's career charisma, that is, until it is time for more policy earnings and a plot change.

Understanding the basic underpinnings of the industry between policy and action can help one understand how wargames function as a career and policymaking tool. +ADD RENUNCIATION OF WAR AS AN INSTRUMENT OF NATIONAL POLICY (KELLOGG-BRIAND PEACE PACT OR PACT OF PARIS) Treaty signed at Paris August 27,1928.[106] Ostensibly, that is wargames' only purpose. However, as I present below, highly diversified policy institutions like the RAND Corporation (many RANDites become politicians themselves) are aware, as I am, how the industry can be engineered and exploited to profit off of the increased rotations of the replacement cycle in every single political industry and subject matter arena.

Wargames are simply an expedited way to game a new political cycle, and if analytic results are favorable, to compel a full revolution of that political replacement cycle. And, without a doubt, if any group could, RAND analysts could answer: What are the odds that RAND analysts, generation after generation, could accurately predict seventy years of warfare, technological and scientific threats and progress, and regime change around the world with such

[106] Bevans, Charles I., comp. "Renunciation of War as an Instrument of National Policy (Kellogg-Briand Peace Pact or Pact of Paris)". *Treaties and other international agreements of the United States of America, 1776-1949.* Vol. 2, p. 732-736. Department of State. U.S. Government Printing Office. 1968-76.

unwaveringly accurate detail, across every government and subject matter discipline, without having provoked and prepared the policy-changing events themselves? My humble estimate is: infinitesimal. Wargames, their circumstances, and their resultant wars come from out of the 'blue team'.

I show how this pattern of wargame-war-research-policy has been repeated over and over again in US policy and military action in the Middle East. I also argue that the shape which the Arab Spring took aligns precisely with US foreign and military policy projections for the region outlined long before 2011. Naturally, this argument implies that when one takes US action timelines to begin with wargames (the earliest public manifestation of Pentagon policy usually), followed by wars and research development and public policy, the understanding one arrives to excludes the possibility of the Arab Spring ever having been organic events.

Out of the Blue, the chapter title, is a play on wargame terminology - blue team indicating "us", and red team indicating the "enemy". Out of the Blue means that *real world action* is intentionally taken by US and allied forces ("blue") that are traditionally enemy ("red") actions. These actions, policies, and games provoke war, violence, threats to US lives, and damage international relations. They prompt major government investment in research into new threats and cures and in development of new war weaponry – all the industries think-tanks like the RAND Corporation have to profit off of.

If one could also sell the impetus for investment, such as a wargame scenario needing new weaponry or technology and new bad policy that will start a war, one could completely dominate the political economy and its cycles end-to-end. This is exactly what has occurred. I mean that the real attacks, plots and threats directed at the US, and all the redirected economy that ensues from wargame analytics, real crises and real wars come out of American policy institutes as products for the benefit of the institute.

The length to which the 'blue team' will go has depended on how much it stands to gain in the cycle. That today Pentagon wargaming experts are publicly rejecting wargames should be indicative that the give-and-take around the political cycle has become exhausted.

The title is also meant to indicate that the attacks do not come from out of the blue, that is, without warning. The attacks are scenarioed, calculated and their simulations purchased by the superiors of the people who will die in the actual fighting that ensues shortly afterwards. Much of wargaming is simply open-faced plotting and premeditated terrorism by arrogant subversives who, after decades of immunity and profiteering, have become increasingly dangerous around the world and increasingly so in the US as they near their end-game of eclipsing US democratic institutions.

Unlike Amazon, Blackwater or other defense contractors, think-tanks have had few public trials or exposures for their criminal activity. For example, Amazon, product and computing contractor to the Department of Defense, was recently exposed for strategically placing its former employees in positions of importance in the DoD. The company's ethics were called into question along with the maintenance of their contracts. (add cite) Blackwater was the now infamous security force contracting company in Iraq in the early 2000s. Since then, multiple

Blackwater contractors have been convicted for war crimes committed against Iraqi civilians. Wargame institutes have not faced public trials or exposures, and most people are not even aware that such institutes exist.

+ADD "Development of the Repository began in late 2015, and it currently houses over 750 completed and future DoD wargames entries. **Access to details about these wargames is open to all DoD personnel via the Secret Internet Protocol Router Network**, and the details include summaries of results from over six hundred wargames and full-length reports from over one hundred wargames."[107]

[TOPIC – wargames as psy-ops]

"Only in the late 2000s did disinformation begin to pick up speed again. By 2015 and especially 2016, the old playbook had been successfully adapted to a new technical environment."[108]

"Psy Ops, or the basic aspects of modern psychological operations, have been known by many other names or terms, including Psychological Warfare, Political Warfare, "Hearts and Minds," and even Propaganda."[109]

"Notably, Psy Ops have been as applicable to mass modern armies as they have been to the guerrilla, the freedom fighter, and the terrorist. We currently see the use of Psy Ops as common to both sides of the 'Long War,' with our present foes, such as al Qaeda, making the psychological impact of an attack a hallmark of their actions."[110]

https://orientalreview.org/2018/02/27/rand-corporation-proves-link-us-military-hybrid-war/ "As it relates to the RAND study, there's a clear relationship between US troops in "**Lead From Behind**" proxy states and an outbreak of Hybrid War in the theater, though the organization of course portrays this as not being related in any way [due to] the US' own policies but instead as a reaction to the so-called "potential US adversary" that was being targeted all along."

The well-known quotation by sociologist Durant "A great civilization is not conquered from without until it has destroyed itself within" is more aptly understood in context, as he continues, "Rome was conquered not by barbarian invasion from without, but by barbarian multiplication within", and when understood as an expression of the progenitor of sociology Ibn Khaldun's theory of historiography of empire in *Al-Muqaddimah* - that of cyclical civil decay in settled generations and their conquest by mobile groups - both can be simultaneously applied to chaotic yet well-delineated global conflicts. They can consistently fill in gaps of proof, rendering a coherent basic method for understanding the double nature of geopolitical current events.

To elaborate, when Durant wrote the beloved quote "A great civilization is not conquered from without until it has destroyed itself within", he made it in reference to the Roman Civilization as civilized in contrast to those "barbarian" cultures which destroyed it, - German

---

[107] Heath, Garrett and Oleg Svet. "We Run Wargames Programs for the Joint Staff. Here's What We've Learned". Modern War Institute at West Point website. 19 October 2018.

[108] Rid, Thomas, p. 2 https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

[109] Clow, Ryan. "Psychological Operations: The Need To Understand The Psychological Plane of Warfare". *Canadian Military Journal (CMJ), Vol. 9, No. 1*. 2008, p. 22.

[110] Clow, Ryan. "Psychological Operations: The Need To Understand The Psychological Plane of Warfare". *Canadian Military Journal (CMJ), Vol. 9, No. 1*. 2008, p. 24.

nomadic hordes and mixed Oriental-Italians, - through "rapidly breeding" while the Romans remained in "the comforts of sterility".[111]

That is to say, despite his socio-political insights and canonical status, Durant did not intend the obvious meaning of the quote. Rather, as Edward Said's *Orientalism* might interpret it, the "great civilization" is not itself when it is conquered; it has become Other. In the cases I will discuss, this is meant very literally, though the Other maintains the meaning of a false construct born of the socio-imaginative abstract brought to life, ironically here through transnational cooperation in wargaming international policy.

I will show that several real socio-political crises of the past several years are best understood as coordinated covert actions between Western and Eastern states which play to historiographical stereotypes to threaten civilizations with mobile foreign forces (similar to what Ibn Khaldun outlined as the course of civilization). All of this is done in order to effect change in that civilization, constituting state-sponsored terrorism - *terrorism* meaning the use of violence to effect political policy change. Importantly, those mobile forces' limited successes and obsolescence are planned in advance and carefully managed to maintain the states' monopoly on power. Neorealism's 'self-help' security mechanism.

One example of this is the form of political Islam today considered orthodox Sunnism in the Muslim World, known imprecisely as Wahabism, Salafism, or sometimes just Islamic fundamentalism. Firstly, it is not representative of the ideas and writings of its namesake 'Abd al-Wahāb. Secondly, this form of Islam is not Sunni orthodoxy because it does not recognize as legitimate all four of the jurisprudential schools (*mathhab*) of Sunnism. Rather, Islamic fundamentalism precisely fits Said's description of Western Orientalists' view of Islam. Said describes the Orientalist perspective that,

> If Islam is flawed from the start by virtue of its permanent disabilities, **the Orientalist will find himself opposing any Islamic attempts to reform Islam, because, according to his views, reform is a betrayal of Islam**: this is exactly [H.A.R.] Gibb's argument [in *Modern Trends in Islam* at the University of Chicago in 1945].[112]

Viewing reform as a betrayal of Islam and being opposed to reforms is a common description of 'what's so terrible' about Islamic fundamentalists, Salafis, and Wahabis today. But in fact, in 1945, it was Western Orientalists' interpretation of Islam.

At the time, Western scholars held the view that 'reform is a betrayal of Islam' in contrast to Islamic world interpretations of Islam. Today, Islamists are accused of believing that reform is a betrayal of Islam. This is an example, using political Islam, of what I am claiming is an intel-policy guided process in which cultures cease to hold their own ideas, and begin to take on

---

[111] Durant, Will and Ariel. *The Story of Civilization, Part X: Rousseau and Revolution*. Simon and Schuster. New York, 1967, p. 665-66.

[112] Said, p. 103-104.

detrimental cultural ideas originally conceived of by the 'Other', followed by overt destruction from outside forces.

+ADD quote from *The Last Empire* book on Islamism, economy used as pretext during cold war to deflect appearance of stalemate, proxy wars between nuclear powers. Framed as communism vs capitalism between nuclear powers. Framed with Islamists (mujahidin, for example) as atheism vs. religiosity.

The National Intelligence Council uses in its most recent prospective report *The Paradox of Progress* the loan word *sinariu* (سيناريو) to translate the English "scenario".[113] I suggest interpreting the word "scenario" as the Arabic *dawriyyah* (دورية) meaning "patrol, round; patrol reconnaissance squad".[114]

Dawriyyah finds its root in the word *daur* (دور) meaning "round (of a patrol; in sports); role, part (played by s.o. or s.th.); film role, stage role; periodic change, rotation, alternation".[115] The word *dawriyyah* means effectively 'a single instance of *daur*'. This conveys the true purpose of conducting (counter)intelligence reconnaissance continuously through scenarios, amounting to military deception. It also conveys that the fictionalized roleplay and theatrical showiness of scenarios function as counterintelligence policymaking operations. These aspects of wargaming are discussed further in the subsections 'A Live Exercise' and 'Lessons Learned'.

Wargames have become a regularly used method of training national security states to act against the interests of their own nation. Taking on the mentality, identity and actions of the Other persists throughout non-scenarioed policymaking and military action, and normalizes acting on behalf of enemy objectives. This confusion even persists in international joint wargame exercises in which multiple nations are actually participating. **The problematics of perception in wargaming explored within hypergame theory may expand on this real-world terroristic phenomenon.**

[TOPIC- Hypergame Theory and Military Deception]

+ADD "One plus for HT [Hypergame Theory] is its explicit commitment to representing different views of any competitive situation for each of the players. **HT explicitly breaks game theory's requirement on consistent alignment of beliefs among opponents/players**, which is needed for the calculation of Nash Equilibrium Mixed Strategies, hereafter NEMS. Another plus is that plan dynamics reflected in the HEU [Hypergame Expected Utility] effectiveness measure can be used to delay action and gather more information to attempt to reduce uncertainty by exploring plan vulnerabilities. The additional reasoning in HT reduces the modeling parsimony of GT [game theory] normal games, which can be a minus. Since competitive situations often include a number of factors which cause opponents **to view the options and results of game situations differently, HT appears more suitable to real world situations.** Some of these considerations include:
(1) Differences in player knowledge, expertise
(2) Differences in player starting situation assessment

[113] FIND Arabic Paradox of Progress PDF
[114] Hans-Wehr 3rd edition, p. 300.
[115] Hans-Wehr 3rd edition, p. 299.

(3) Differences in player on-going assessment capability (evidence processing)
(4) Differences in player understanding of plan projection (what beats what?)
(5) Differences in player information (both at the commitment phase and during the operations)
(6) Differences in robustness, resilience of each player's plans
(7) Player Constraints because of time
(8) Differences in player creativity (what tricks can be added) such as feints, hidden reserves, denial and deception operations
These considerations motivate HT's extension of the GT normal form **to account for situational aspects that might arise in real competitive situations."**[116]

On hypergame of wargaming, in the room where it happens – Arab Spring was 'gamed' societal collapse which took place, in reality, over multiple generations of 'great-gaming':
"it becomes clear how the **Rosca mechanism [for reciprocity games] enables us to study the direct relationship between surveillance intensity in a society and the scope of cooperation**: ni(pi , δ) captures the scope **of cooperation in a society as a function of the density of informer activity**. A large scale and depth of the penetration of people's lives as well as of the institutions of state and society may lead to a strong reliance on transactions within the immediate family ('amoral familism') as opposed to transactions with unknown, more distant third persons. As a result, the 'amoral familism' that Banfield (1958) observed in the Mezzogiorno may, in fact, be not irrational but the only rational strategy for survival in a society that is characterized by a highly intrusive state security body as in the GDR. Now let us turn to the expected payoffs… under the assumption that p1 << p2 it follows for any n that A >> B, so the expected return is positive and much greater if the population is 'trustworthy' than if it is plagued by a high intensity of spying activity… a 'pessimistic' prior reduces the scope of cooperation. A sufficiently pessimistic prior may even lead to no investment at all… To be specific, people choose scope of cooperation n1 until their priors are sufficiently depressed and choosing n2 becomes the preferred option. (The threshold prior π below which n2 becomes the preferred scope of cooperation is in Appendix A.4.) Consequently, in our model, the more optimistic individuals' priors in a society are (that is, the greater their πe) the greater will be their scope of cooperation. Conversely, where people have a greater reason to believe that they live in an informer environment (that is, they have a greater 1 − πe) their scope of cooperation is more limited on average… An individual who in the first period finds his reciprocity game successful will have an updated prior π > πb (see Appendix A.2), and in the second period she will invest in at least a same size-n reciprocity game. But if she experiences a defected reciprocity game and has sufficient reason to believe that she lives in a highly infiltrated society (that is, π < π) then in the second period she will invest only in a smaller-n reciprocity game. This illustrates the important model dynamic. The more often the experience from these social experiments is frustrating for individuals the more downward they will correct their priors about the trustworthiness of the society, and as a result their scope of cooperation in social and economic interactions ultimately collapses… To check our theoretical predictions of a significant negative relationship between the pervasiveness of the network of informants and social capital, we use actual data on the informer density in the GDR and simulate our model in MatLab. **All simulations involve 20 generations** (about 500 years assuming a generational gap of 25 years). Each generation is composed of 500 people. As in the real case of East Germany, we specify our

[116] Vane III, Russell R. "Advances in Hypergame Theory". *General Dynamics Advanced Information Systems*. 2006, p. 1.

model such that in the first three generations the true regime is the oppressive regime with share of informants p2**. In generations 4-20 we make the democratic society the true environment.** We assume that the number of informers is negligible in a democratic society, and that the first-generation prior is diffuse (both society types are equally likely). Figure 3 illustrates the outcome of the basic principle underlying our model. If the informer environment is the true world then for positive or insufficiently negative priors (that is, $\pi > \pi$) individuals will perceive larger size-n1 reciprocity games optimal, for these transactions offer superior expected returns**. However, scope of cooperation n1 is an inappropriately high choice if the true world is the 'oppressive' environment, because with almost perfect certainty individuals will encounter informers**… In Panel A of Figure 3 we take into account only the 91,015 full time Stasi officers in the GDR and simulate the priors about trustworthiness and **scope of cooperation for an informer density of** p2 = 0.0055 (**91,015 officers on a population of 16.675 million**). **Our model predicts that the scope of cooperation collapses in the third generation under the oppressive regime** and only gradually recovers under democratic institutions. To be specific, the scope of cooperation recovers by approximately 20% in the first generation after democratization but **takes another 4 generations to reach pre-regime-shock levels**… In Panel B of Figure 3 we increase the surveillance intensity by additionally including the 173,081 regular Stasi informers, leading to an informer density of p2 = 0.0158**. The higher density of secret police activities leads to a much narrower scope of cooperation than in Panel A after collapse of cooperativeness in the third generation under the oppressive regime.** In fact, in this scenario priors depress so much that the positive initial small n2 scale transaction experiences in the generation immediately after democratization do not suffice to push priors above the threshold π that make large scale cooperation attractive… In this paper we present rare empirical **evidence of social capital destruction through state action.** Putting forward a formal model and investigating empirical evidence from the districts of the former GDR, we find that people's experience of living in a regime in which state security informers had their tentacles in every aspect of people's lives has resulted in a strong and lingering sense of mistrust of members of society outside the immediate family circle. The erosion of trust and cooperativeness in the former GDR is manifest in lower current levels of social capital in post-communist East Germany. We furthermore find robust evidence that surveillance intensity has a strong negative effect via social capital on current economic performance in these regions… The results presented in this paper invite scholarly research on other postcommunist **economies with substantial secret police activities to confirm the relationship between surveillance intensity, social capital and economic performance** detected in this paper."[117] [REMOVE symbols – did not copy correctly]

Today's security state incompetency and hyper secrecy are the product of *simulations* begun generations earlier. In the section "The Bomb and the GNP", I explain the way in which this has depressed the US and global economy by making all aspects of society subject to the security state, thereby creating something of a **security-banana republic**. I define this as a politically unstable country, or globe, operated as a private commercial enterprise with an economy entirely dependent on exploitative national security industries. The Banana Wars (1898-1934) which resulted from the Roosevelt Corollary on the Monroe Doctrine (1904), promising "the exercise of an international police power", suggests a causal connection between security states and

[117] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010, p.13-16, 39.

banana republics. In the section The Bosnia Model, The Rumsfeld Model, I further address multigenerational planned strategic incompetence in the US security state. [Also applicable to use of wargaming as informer/(counter)intelligence operations, discontent reported in the wargaming industry. Also applicable to this chapter's argument that wargaming/scenario-planning is deception for state-sponsored terrorist activity.]

[TOPIC – 'terrorism in practice']

The National Commission on Terrorist Attacks Upon the United States, convened 2002-2004 in response to the September 11th attacks, inaccurately defines terrorism in the following way: "Terrorism is a tactic used by individuals and organizations to kill and destroy." [118] This is not correct and in no way distinguishes terrorism from any other type of violence.

Terrorism is accurately defined as the use of violence to effect policy change or alter political outcomes. Terrorism is "any deliberate attack against innocent civilians in order to put pressure on a government or a society."[119] It may involve a variety of methods, including state sponsorship. In fact, members of the state are the most likely to be interested in producing policy change and altering political outcomes.

Terrorism occurs within a dynamic. It depends on the existence of a dynamic I describe below as terrorism in practice. I would suggest that a holistic definition of terrorism would be comprised of the common tactical definition, like that used by the 9/11 Commission, and the expert definition, like that quoted above, written by former French Foreign Ministry and UN political consultant Roy Oliver.

While the public experiences terrorism as indiscriminate killing and destruction, policymakers and politicians experience terrorism as violent coercion or deterrence by political actors. Therefore, terrorism in practice is *any deliberate politically motivated attack on a civilian population which experiences the attack as indiscriminate killing and destruction, and whose response puts pressure on a government to respond*. Typically, the public demands government action according to what it knows about the attack, not how government members understand the situation to really be. The situation as it really is develops over decades in a conversation taking place in classified cables and closed-door negotiations between politicians and terrorists.

This incongruity can be exploited by policymakers and politicians to achieve their own policy agendas, delivering no remedy of the situation – and in fact, encouraging repeated attacks - doubling public frustration and terror. In a sense, terrorism's job is only complete without a competent response from the government and the public. This is a pattern used in situations of state-sponsored terrorism, warmongering and war profiteering, and lesser situations of governmental corruption over public security which can, with increased systematization and sophistication, evolve into full-blown state-sponsored terrorism.

Professor and Chair of National Security Studies at the Mershon Center for International Security Studies John Mueller writes in *Overblown*: *How Politicians and the Terrorism Industry Inflate National Security Threats:*

---

[118] https://govinfo.library.unt.edu/911/report/911Report_Ch12.htm

[119] Roy, Oliver. *The Politics of Chaos in the Middle East*. Columbia University Press. 2008, p. 53.

> Something comparable might hold for the U.S. war on Iraq in 2003. Quite a few people in **the administration had been yearning for such a war for years, and they clearly seized the opportunity provided by the trauma of 9/11 to push their agenda**… In such cases, **the terrorist act is used as an excuse for, or is seized on to carry out, a policy that has been desired for other reasons.** To say that World War I or the Iraq War were 'caused' by terrorism, or even by overreaction to terrorism, really stretches the distinction. The terrorist acts do not 'trigger' such ventures, but rather facilitate them by shifting the emotional or political situation, potentially making a policy desired for other reasons possible but no more necessary than it was before the terrorist act. In addition, regimes have often allowed their participation in peace talks to be critically affected by terrorists. By stating that they will not negotiate as long as terrorist attacks continue, both the Israeli government and the British government (over Norther Ireland) effectively permitted individual terrorists to set their agendas… dramatic acts of terrorism very often have negative reverberations because they stimulate or service the politician's natural desire and propensity to play to the galleries, to wallow in the art of the rhetorical flourish. Some of that can be seen in instances discussed earlier: Carter with his hostages in Iran, Reagan with his in Lebanon. If an act of fulmination proves to be a productive exercise in security theater by somehow reducing fears, it could be a desirable, and certainly inexpensive, palliative: cheap talk, indeed.[120]

In effect, the dynamic of terrorism in practice is the deprivation of terrorism of its intended political message, and the supplantation of that message with a policy agenda dictated by a government. Were policymakers and politicians to make the public aware of the coercive or deterrent political motivations of attacks, such a move would deprive terrorism of the wide effect it has on the public, which is to terrorize through seemingly indiscriminate killing and destruction. Parallelly, were policymakers and politicians not aware of the political motivations behind an attack, the attack would fail to send a message and hit its mark, politically.

To be effective, terrorism must have a public which views the attack as merely a tactic to kill and destroy, and a political elite, who view themselves as solely responsible for responding to the political message sent by the attack. The political elite must withhold intelligence from the public that would allow the public to react appropriately to the situation, even if only to identify or exclude themselves as possible targets. An informative response would drastically reduce the psychological effect that perceived indiscriminate killing has. It would prevent policy responses which were inappropriate to the situation or that compel the populace to function on high alert. In effect, it would deprive terror attacks of inspiring widespread terror - how the public experiences it. It would deprive terrorism of being an effective political tool - how policymakers and terrorists experience it.

+ADD "The high level of violence and the paramilitary capabilities of some cartels draw easy comparisons with modern irregular warfare. Some of the violence enacted by cartels displays a level of anomie that bears resemblance to terrorist tactics. Anomic violence relates to purposeless and gruesome acts of aggression in complete contravention of societal norms and values. For example, in April 2011, cartel gunmen raided an apartment and executed an entire

---

[120] Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. Free Press. 2006, p. 167.

family, including a 22-month old toddler, to incite fear in the populace and rivals. Mexico's attorney general's office reported 1,303 beheadings between 2007 and 2012 as part of a campaign to instill fear and demonstrate dominance. Cartels typically leave the heads and decapitated bodies in view of the public. Some beheadings are posted on the internet to intimidate rivals and the populace to acquiesce to illicit activity. Other anomic violence behaviors include the use of torture, car bombs, marking corpses with targeted messages, dismemberment, assassinations, the use of mass graves, and kidnapping… Anomic violence facilitates the acquiescence of state agents and the local community through fear. In this regard, the presence of anomic violence resembles the tactics employed by nonstate terrorist organizations like Islamic State of Iraq and Syria or al-Qaeda… The presence of clientelism and ungoverned spaces share similarities with an insurgency, where opposition groups hold legitimate authority and influence over a population in the absence of the government."[121]
[MOVE]

+ADD quote from *The Last Empire* book on Islamism, reframe on state-public terrorism dynamic, re: indiscriminate killing and destruction deprived of political message

[TOPIC – Weber addresses demagoguery's proclivities toward terrorism and terroristic spectacle] "…**the demagogue is compelled to count upon 'effect'. He therefore is constantly in danger of becoming an actor** as well as taking lightly the responsibility for the outcome of his actions and of being concerned merely with the 'impression' he makes… The mere 'power politician' may get strong effects, but actually his work leads nowhere and is senseless… In this, the critics of 'power politics' are absolutely right. From the sudden inner collapse of typical representatives of this mentality, we can see what inner weakness and impotence hides behind this boastful but entirely empty gesture. **It is a product of a shoddy and superficially blasé attitude towards the meaning of human conduct; and it has no relation whatsoever to the knowledge of tragedy with which all action, but especially political action, is truly interwoven. The final result of political action often, no, even regularly, stands in completely inadequate and often even paradoxical relation to its original meaning."[122]**

[REWORD] In a section titled "Long-Range Projections: A Cautionary Tale", the US National Intelligence Council writes in 2008 on the benefits of scenario-based non-linear policymaking, "In the early 1920s, few envisioned the lethal situation about to unfold, ushered in by the Great Depression, Stalin's gulags, and an even more bloody world war encompassing multiple genocides."[123] The NIC alleges speculative fiction based-scenarios can anticipate and preclude lethal situations, while I argue that fictional scenarios are military-style deceptions that create such situations.

The wargame, distinguished from traditional military drilling, is game theory applied to war. Wargame-based strategy is the epistemology particular to the RAND Corporation, which helped to innovate the modern US concept of wargaming. RAND has an entire center dedicated to the practice called the RAND Center for Gaming, and has declared that wargaming is "a

---

[121] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 6-8.
[122] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 116-17.
[123] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 5.

renaissance in the Department of Defense."[124] (audio?[125]) The Department of Defense has the Office of Modeling and Simulation. The War College, etc.

Game theory is an academic discipline that applies "the mathematical structure of parlor games such as poker… and apply it to economics, politics, foreign policy, and other spheres of activity… one of the favorite games developed by RAND analysts in the 1950s was called the prisoner's dilemma," which involved another term coined by RAND game theorists "zero-sum game". Game theorist economist John Nash formulated his Nobel Prize winning game theories in economics while employed at RAND.[126]
+ADD here from *The Analytics of Uncertainty and Information* (2013):

[TOPIC – criticisms of wargaming]

In the October 2019 article "The Obstacle on the Road to Better Analytical Wargaming" Jon Compton, senior analyst of wargaming in the Office of the Secretary of Defense, writes that "frustration with the professional wargame community of practice is real and growing among many of us in the department [of Defense]." He specifically cites informal meetings, "BOGSAT – bunch of guys sitting around a table" rather than "multistage efforts created [with] end-to-end narratives". He also cites the emphasis on cyber warfare and cyber modeling, and sloppy analysis meant only to feed the need for research publications by specific groups.[127] This is the topic I cover in the section Recent Developments and Research and Development.

In the response article "Rolling the Iron Dice", other members of the wargaming community defend their analytic processes. More interestingly though, the authors confess that "the wargaming community is not without sin. As Compton points out, there are bad wargames – and even worse events masquerading as wargames – being perpetrated on the department [of Defense]."[128]

Herman Kahn and Irwin Mann detailed similar criticism in 1957 in *Ten Common Pitfalls*. They wrote in the section titled Modeling:

> For this reason, it is usually sterile to emphasize technical tools in an analysis which is designed to influence policy. In spite of this, many analysts do become enamored of intellectual and mechanical gadgets, particularly the more modern ones, such as high-speed computers, war gaming, information theory, linear and dynamic programming, differential analyzers, game theory, Monte Carlo, etc. They are easily seduced into emphasizing the use of such tools rather than focusing attention on the real problems. People so oriented are sometimes just salesmen; more often they are serious technicians who may advance the state of the art—in this case they may even turn out first rate component studies. However, they rarely turn out good complete and realistic analyses. This is a criticism only if the analyst is trying to influence policy; if he is trying to advance the state of the art or consciously

---

[124] Bartels, Elizabeth M. "Getting the Most Out Of Your Wargame: Practical Advice for Decisionmakers". *The RAND Blog*. 26 January 2016.
[125] https://www.rand.org/multimedia/audio/2017/03/23/the-serious-role-of-gaming-at-RAND.html
[126] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, p. 53-54.
[127] Compton, Jon. "The Obstacles on the Road to Better Analytical Wargaming". *War on the Rocks.* 9 October 2019.
[128] Perla, Peter P. et al. "Rolling the Iron Dice: From Analytical Wargaming to the Cycle of Research". *War on the Rocks.* 21 October 2019.

> introducing new tools, then his activities should presumably be judged on a technical basis and it is not necessary for him to introduce substantive considerations.[129]

Peter (?) and Compton, or any in the wargaming industry, are not alone in their suspicion of wargame exercises. In 2015, there was significant uproar in the Southwest of the United States over the conduction of wargame exercise Operation Jade Helm-15 which simulated the hostile invasion of the US via its southern border. The wargame staged thousands (#?) of US troops throughout California, Arizona, New Mexico, Nevada, Utah, and Texas (?). The local responses were mixed, with the most significant official protests being Texas State Guard deployed to oversee national troops in the state, and rampant rumors of armed federal takeovers being plotted against the citizenry of those areas. In return, CIA Director Michael Hayden predictably blamed a Russian misinformation campaign for the hostile responses to the wargame exercise.[130]

+ADD *On Thermonuclear War*: "From the viewpoint of deterring cheating and making more certain and **dramatic our response if we happen to detect cheating by clandestine intelligence…** Most important of all, it would have been of real value to have had in existence in 1958 an experienced organization of 'hiders and finders' with practical and theoretical experience on the problems. We still have no such organization, and 1961 is likely to see us entering **arms control** conferences uneducated and unprepared. The test-suspension negotiations at Geneva [in July and August 1958] illustrate the importance of doing our homework… **['hiders and finders' is] Amrom Katz's term. He has suggested that we set up two organizations and turn over a large area – like the state of Texas – to them and let these two organizations play seriously various kinds of Arms Control games**. We would thus build up some intellectual and experimental capital, on which our negotiators and planners could draw. **The 'hiders' organization** has another value, one which would all by itself justify the expense of the organization. It **could create a credible capability for evading an Arms Control agreement.** Fred Iklé has pointed out the value of creating such possibilities. **Raising the apprehension among Soviet planners that we might cheat should make them much more interested in reliable inspection procedures**."[131]
["Amrom Harry Katz (August 15, 1915 – February 10, 1997) was an American physicist who specialized in aerial reconnaissance as well as satellite technology. Katz developed methods for aerial reconnaissance supported by space satellites. His work was used by military intelligence, and for locating disaster victims. On August 18, 2000 he was acknowledged as one of the ten Founders of the National Reconnaissance Office. Between 1954 and 1969 he worked for the RAND Corporation in Santa Monica, California." *Wikipedia*]
+ADD The Finders as secret intelligence organization which appeared during the Cold War involved in child trafficking, re: frequency jamming, electronic weaponry, information operations, untraced/jammed human trafficking, telecommunications-enabled pedophilia
https://www.tallahassee.com/story/news/local/state/2019/10/29/fbi-vault-the-finders-conspiracy-theories-florida-tallahassee-child-abuse-case-files/2487934001/ ;
https://www.vice.com/en/article/7x53vg/the-finders-cult-from-the-80s-was-patient-zero-for-

---

[129] Kahn, Herman and Irwin Mann. *Ten Common Pitfalls.* The RAND Corporation, Santa Monica, California. 17 July 1957, p.3.
[130] https://www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/
[131] Kahn, p. 454.

epstein-and-pizzagate-conspiracies ; https://vault.fbi.gov/the-finders/the-finders-part-01-of-03/view ; **"One critical aspect of the freeze, the deployment of new nuclear weapons systems, can be verified with high confidence through national technical means – that is, satellites and listening posts equipped with sensors – and through data exchange and restrictions on concealment.** A **second element of the freeze, testing, can also be verified by national technical means, together with unmanned seismic stations and opportunities for onsite inspection**… **The third aspect of the freeze, production, may be more difficult to verify, but our intelligence is so highly developed that, according to former Under Secretary of Defense William Perry, we have been able to 'monitor** Soviet activity at the design bureaus and production plans well enough so that we have been able to predict ever ICBM before it began its tests.'… But **on the question of verification, we should remember one important aspect of the nuclear freeze that was described be the former Deputy Director of CIA, Herbert Scoville: A Freeze is Actually Easier to Verify than A Treaty** Like SALT I or Salt II. Such treaties contain complicated limits on numbers and on modifications of missiles and planes; to detect a violation requires continuing and exact measurements of a vast array of possible prohibited activity. **With a freeze, however, a violation would occur and be discovered the instant the other side does anything new at all**… Our overriding goal should be to secure **a nuclear weapons freeze** that prevents any further escalation of the nuclear arms race – across the board – not only in Europe but **in every region of the world."[132] [Repeated in Research and Arrested Development]**

Public and professional revulsion is owed to recent changes in war policy from training for conventional warfare to irregular warfare training since September 11th, increasing to dominate the training by 2010. +ADD "This study concludes that both national interest and bureaucratic politics influenced the strategic shift since 9/11, albeit to varying degrees—national interest had the strongest effect in 2001, and then different components of the bureaucratic politics model intertwined with the national interest motivation as new "players" entered the "game" along the way. [ADD cite]

RAND's game theory heavily influenced aspects of American domestic life. "Vernon L. Smith, a RAND consultant in 1959, laid the theoretical foundation for the deregulation of energy markets in the United States, Australia, and New Zealand; he was corecipient of the Nobel Prize in Economics in 2002. Finally, William Vickery, a consultant at RAND during 1967 and 1968, who shared the 1996 Nobel Prize in Economics with British economist James A. Mirrlees, provided the rationale for the high fees charged by electric and telephone companies and airlines during peak periods of use. He also originated the theory of road pricing, that is, that charging motorists tolls and assorted fees for the use of roads will show consumers what the true costs of road upkeep are, with the consequence of lessening traffic congestion."[133] This clearly was not effective in southern California where RAND is headquartered.

Game theorists from RAND convinced the Nixon administration against funding universal free health coverage in the US by conducting and reporting on their own study, a study in which RAND posed as a health insurance company to thousands of Americans. +ADD more

---

[132] Kennedy, Sen. Edward M. "Statement of Senator Edward M. Kennedy on the Nuclear Weapons Freeze Amendment to the Debt Ceiling". *Office of Senator Edward M. Kennedy of Massachusetts*. 5 October 1984.
[133] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, p. 258.

It should be reiterated here that RAND not only determined the global model for private health insurance but it is also the world's leading nuclear research corporation. What should also be noted is the astronomical rise in the world's cancer rates in the past decades and the earnings for those treatments accrued by private healthcare corporations. To plainly state what many have avoided saying over almost a century, the RAND Corporation is a policy, research, and implementation nexus of the developed world's cancer epidemic, cost prohibitive healthcare, as well numerous other global genocidal epidemics mentioned in this essay. In the 1950s, the Soviet publication *Pravda* likewise described the RAND Corporation as the "academy of science and death".[134] [REWORD]

President Reagan showed the tale-tell signs of RAND influence "starting with his 1980 campaign promise to abolish the Department of Education and the Department of Energy, Reagan propelled an ever-growing national tendency toward deregulation, following RAND-inspired reform policies to encourage the growth of free markets." +ADD Trump Administration's early plan to close Dept. of Education and Parks Dept. (in Abella's book on RAND, find quoted already) https://www.businessinsider.com/how-donald-trump-could-eliminate-the-department-of-education-2016-11 ; https://www.theguardian.com/environment/2017/jun/25/us-national-parks-privatized-trump-administration

Donald Rumsfeld, as a former RAND board trustee and then-Secretary of Defense, introduced the RAND-developed economic game theory that lower income tax results in higher tax revenue. These practices of deregulation, less anti-competitive prosecutions, and lower tax rates created the loan bubble which burst and resulted in a government bailout of $125 billion to private corporations. "We live under the shadow of the consequences of another RAND-inspired event: the defeat of the Soviet Union in Afghanistan, a debacle that pointed the way to the horror of September 11, 2001."[135] In fact, in September 2001, RAND had just established the plan for a brand new RAND base in Qatar.[136] These are just a few examples of social engineering, what they call rational choice game theory, that have come out of the RAND Corporation. [REWORD] +Connect to CNN effect / +ADD VNN effect

Such points cannot be overstated. The nature of irregular warfare is such that what seem to be concomitant features may in fact be the principle motivating factors for the action. Such an example is detailed on the topic of radio broadcasts as psychological *and* kinetic weaponry in the section titled Radio-logical Warfare. Irregular warfare could just as easily be called 'indirect warfare', 'active measures', 'unpeace',[137] 'small wars', or to 'fight a war without actually being at war'[138]. [REWORD]

+ADD From U.S. Marine Corps. *Small Wars Manual* (1940): "The term 'Small War' is often a vague name for any one of a great variety of military operations. As applied to the. United States,

---

[134] Abella, p. 92.
[135] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, p. 259-61.
[136] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, p. 263.
[137] Lucas Kello
[138] Steed, p. 46.

small wars are operations undertaken under executive authority, wherein military force is combined with diplomatic pressure in the internal or external affairs of another state whose government is unstable, inadequate, or unsatisfactory for the preservation of life and of such interests as are determined by the foreign policy of our Nation. As herein used the term is understood in its most comprehensive sense, and all the successive steps taken in the development of a small war and the varying degrees of force applied under various situations are presented… [there] may be found an infinite number of forms of friendly assistance or intervention which it is almost impossible to classify under a limited number of individual types of operations. Small wars vary in degrees from simple demonstrative operations to military intervention in the fullest sense, short of war. They are not limited in their size, in the extent of their theater of operations nor their cost in property, money, or lives. The essence of a. small war is its purpose and the circumstances surrounding its inception and conduct, the character of either one or all of the opposing forces, and the nature of the operations themselves. The ordinary expedition of the Marine Corps which does not involve a major effort in regular warfare against a first-rate power may be termed a small war. It is this type of routine active foreign duty of the Marine Corps in which this manual is primarily interested. Small wars represent the normal and frequent operations of the Marine Corps. During about 85 of the last 100 years [as of 1940], the Marine Corps has been engaged in small wars in different parts of the world. The Marine Corps has landed troops 180 times in 37 countries from 1800 to 1934. Every year during the past 36 years since the Spanish-American War, the Marine Corps has been engaged in active operations in the field." [139]

The notion of 'false flag attacks', in which guilt is placed on to another nation for an inside-inside (purely domestic) attack, is indicative of wargaming origins. Wargames utilize fake nations, fake attacks, colors and emblems symbolic of real or fictional nations which attack in fictional scenarios offensively or defensively. For this reason included, the US wargame intel-security industries should be considered as sources of terrorism, especially of false flag attacks, in the US against the US. False nations, false nations attacking, false attacks, fake encounters, and false intel on attacks. False flag attacks in scenarios are the topic of the section Horseshoes and Hand Grenades.

[TOPIC – Information warfare, wargame enthusiasm vs real world implementation]

A disturbing connection between RAND's conduction of wargames involves its history with Internet innovation. As inventors of the data packet relay system as a nuclear disaster contingency communication system, RAND's greatest temptation may be wargaming a nuclear scenario to test the Internet, and actually detonating a nuclear weapon in the stratosphere as a so-called 'experiment'.

Warnings from electromagnetic pulse (EMP) planners like former Senator Newt Gingrich demonstrate that some are privy to the need to take precautions against such nuclear disasters in the US. Former CIA EMP Expert Dr. Peter Vincent Pry on the effects of EMP: "It would change the game. It would change the world order." "electronic Armageddons"[140] (obsession with Doomsday scenarios) + RAND wargame report "ready for armaggedon?" + ADD EMP reference in National Intelligence Council *Global Trends 2025*

---

[139] U.S. Marine Corps. *Small Wars Manual.* Department of the Navy: Headquarters United States Marine Corps. 1940. Reprint 22 December 1990, p. 1-2.

[140] "Nuclear Explosion in the Sky". Excerpt from *Electronic Armageddon*. National Geographic. 2 June 2010.

Intel-security analysts are extremely dangerous elements of society who have a multi-decade long track record for destruction and genocide around the world. The name should not mislead. Within their violent and paranoiac industries they are functional, but most outside of the field would describe them in the vernacular as 'mass murderers' and 'pathological liars', or even 'psychopaths' or 'sociopaths'. This criminological perspective was previously outlined in this chapter within former FBI profiler Hazelwood's theory on deviant organized crime.

The insecurity Kahn and Mann noted in 1957 in security analysts' characters has transformed today into genocidal paranoia which should not be underestimated. They are manipulative mass murderers with end-to-end control over policy and operational systems of extinction. The influence they are able to exert and the powerful weapons at their disposal render all government function void if it does not serve their purposes.

I personally have experienced falling out of favor with such persons and industries through my professional research and earlier graduate studies. Let me be clear: these individuals do not hesitate to attempt to murder, torture, stalk, sabotage, or libel anyone who questions their motives. For all intents and purposes, one can end up a non-citizen, a disappeared person, or murdered for criticizing even foreign deployments of US security-intel tactics. [REWORD]

This is attested to also by the US-Europe Joint Investigation Team, a group of intelligence and scientific experts dedicated to investigating and prosecuting applications of irregular warfare. They write in a publication titled *Directed Energy Weapons, Military Neuro/Biotechnology & Systemic Corruption: First Aid for Victims*:

> At the time of writing, all members of the Joint Investigation Team are themselves continuously physically assaulted with modern military weaponry, receive regular death threats and suffer repeated assassination attempts. Each of the investigators has been denied assistance and remedy by their respective police services, judicial offices and legislature to this day.[141]

The work of this group and others like it are addressed further in the section The Hacker's Arsenal.

Other authorities like elected officials may give the semblance of moderation but actually are very happy to give such industries full permission to violently suppress any critic in the name of national security. If the official is not completely complicit in the industry's tactics, after decades of corruption they have no sense of proportion when measuring the brutality of the industry as it really is. There is no unpunished criticism of US intel-security, and therefore there is no accountability in the industry.

Likely, most individuals cannot survive becoming a person of interest to government intel-security. The irregular warfare tactics they deploy are selected from such sources as the East German Stasi State procedure manual precisely because the tactics are insidious. Professor of security studies Thomas Rid testified before the Senate in 2017 on disinformation, opening his statement with the following:

> The most concise description of disinformation as an intelligence discipline comes from one of its uncontested grandmasters, Colonel Rolf Wagenbreth, head of the East German Stasi's Active Measures Department X for over two decades: 'A powerful adversary can

[141] https://jointinvestigation.files.wordpress.com/2018/08/jit-guide_jit-20180830-005-kh-v1_first-aid1.pdf p. 8

> only be defeated through […] a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies […] and within their elites.'[142]

If a critic somehow is able to move forward with critiquing the industry, such an example is made of their oppression that any others would be deterred. Beyond any doubt, when these tactics have been applied, it has invariably spelled the end of any nation which used them. This addressed in the section The Satellite Empire and in the Conclusion.

[MOVE to other section? - Violence in the form of 'information violence', Wartime looting industry]

+ADD UNESCO receives early warning of war/military action

+ADD reference from Organized Crime book

+ADD "On 10 April, U.S. military vehicles and tanks entered the building [Iraq's National Library and Archive]. This development coincided with the collapse of the Saddam regime. The first thing the U.S. soldiers did was to destroy Saddam's statue that stood in the front of the NLA main building. When departing, U.S. soldiers left the building without any protection whatsoever. Minutes later, several parts of the NLA building were engulfed in flames. Some people embarked on looting equipments and anything of value. Two days later, the same scenario was repeated... the remaining archival materials and rare books, some people, who were aware of their existence, began to loot these materials from the basement of the General Board of Tourism. The looters took almost all rare books as well as thousands of archival records and documents. Apparently, to cover their crime, they flooded the basement by breaking some water pipes. The remaining documents and records were greatly damaged, resulting in significant losses. Where can one find these stolen materials from NLA? **If we study the type of the missing materials, we can see that the looters must be well-educated.** They knew what to take and where to find it. All the neighboring countries acquired our library and archival materials from smugglers. The smugglers seemed to know what kind of historical documents and records that the neighboring countries wanted to obtain. Many documents and records concerning Iraq's relations with Iran, Syria, Jordan, and Saudi Arabia were missing. Many missing archival materials dealt with the sensitive issue of border disputes."[143] +ADD ISIS campaign to erase Sykes-Picot borders.

+ADD ISIS videos 'destroying' relics ; Baghdadi death along with records of ISIS (news article)

http://oi-archive.uchicago.edu/OI/IRAQ/mela/melairaq.html

"The MELA [Middle East Librarians Association] Executive Board convened the Committee on Iraqi Libraries Committee Members:

- Brenda Bickett, Georgetown University
- Aseel Nasir Dyck, [American University of Beirut and the University of California at Berkeley]

[https://www.iraqichristians.org/English/Iraqs_minorities_2_9_2005.htm]

- David Hirsch, Univ. of California, Los Angeles
- Charles E. Jones, Univ. of Chicago, Oriental Institute
- Shayee Khanaka, Univ. of California, Berkeley
- András Riedlmayer, Harvard University (Chair)

---

[142] https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

[143] Eskander, Saad. "The Tale of Iraq's 'Cemetery of Books". *Information Today*, Vol. 21 No. 11. December 2004.

- Simon Samoeil, Yale University
- Jeff Spurr, Harvard University
- M. Lesley Wilkins, Harvard University, MELA President (ex officio)

The MELA Committee on Iraqi Libraries herewith expresses its willingness to co-operate with international efforts to recover looted Iraqi antiquities, manuscripts, books and other cultural properties, and to assist our Iraqi colleagues. Many of our members, individuals with much appropriate experience and knowledge, are eager to contribute, and especially eager to reaffirm the bonds of international scholarship." The committee convened in 2005. The page has not been updated since 2007.

Unusual Games

Soldiers are close students of tactics, but only rarely of strategy and practically never of war.
Bernard Brodie, American defense theoretician

Professor of Political Science and Editor of Security Studies journal Randall Schweller writes, "In a hypothetical world that has never experienced crime, the concept of security is meaningless."[144]

+ADD "The army is investigating a psychological operations officer who led a group of people from North Carolina to the rally in Washington that led up to the deadly riot in the US Capitol by supporters of Donald Trump. Commanders at Fort Bragg are reviewing Capt Emily Rainey's involvement in last week's events in the nation's capital, but she said she acted within military regulations and that no one in her group broke the law… Rainey said she led 100 members of Moore County Citizens for Freedom, which describes itself online as a non-partisan network promoting conservative values, to Washington to "stand against election fraud" and support Trump… Rainey, 30, is assigned to the 4th Psychological Operations Group at Fort Bragg, according to Maj Daniel Lessard, a spokesman for 1st Special Forces Command. Known as Psyops, the group uses information and misinformation to shape the emotions, decision-making and actions of American adversaries."[145]
+ADD US Capitol riot January 6, 2021: "A man the FBI has identified as Grapevine resident Larry Brock is seen in the video giving instructions to people inside the US Senate. 'I love you guys. We're brothers but we can't be disrespectful,' Brock says in the video as people took photos on the dais. 'It's a PR war**. You have to understand it's an IO war. We can't lose the IO war. It's information, information operation.**'… Throughout the 12-minute video, the mob attacking the US Capitol is seen fighting with officers and can be seen at the end of the video chanting "F--- the blue."… [University dean of criminology] Del Carmen said the mob taking photos of documents once they're inside is something military members are trained to do during operations. 'The individuals that have a mission — in some cases military background, law enforcement background — they're the ones that are sort of driving this,' he said. 'It's hard to

[144] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 91.
[145] Associated Press. "Army investigates psyops officer for role in Washington on day of Capitol riot". *The Guardian*. 11 January 2021.

say if the people who were actually doing this were doing it for the sake of preserving evidence or because they had some kind of military background.'"[146]

UN *Genocide* and its indicators definition: "the deliberate targeting of civilian populations on the basis of their ethnic identity by means **of killings, abductions, unlawful detentions** or **deprivation of liberty, rape** and **sexual violence,** and the **burning of villages** and **looting**… **Warning signs and enablers for genocide** and ethnic cleansing include **the cover of an ongoing conflict to act as a 'smoke screen',** several **low-level and isolated acts of violence to start the process,** the **dehumanization of others through hate speech, economic volatility and instability, deliberate starvation,** the **bombardment of and attacks against civilians, forced displacement** and the **burning of villages**."[147]

+ADD [TOPIC – Russian-linked paramilitary contractor Wagner Group, named in homage to favorite composer of Nazi party, activities in Ukraine, Syria, Libya. Not claimed by any nation.]

Named in homage to the favorite composer of the Nazi Party, the Wagner Group is a composite group of elite Russian paramilitary units accused of committing war crimes around the world. Like the Zeta Cartel in Mexico, Wagner was formed by members of a defected special forces unit of military intelligence. It has been identified as functioning as an important arm of information warfare at multiple levels. In 2018, the UN reported that Wagner Group provides "electronic countermeasures expertise" as well as aerial observation, combat operations, sniper operations, and other kinetic operations to combat zones in Libya, Syria, Ukraine, Belarus, Madagascar, Rwanda, Sudan, Mozambique, and the Central African Republic.[148]

"**Wagner personnel are operating in a way similar to US special-operations units**, for which partnering with local forces and directing American firepower have become pretty standard around the world since the 2001 overthrow of the Taliban in Afghanistan."[149]

The paramilitary group also functions in a military deception capacity. Compounded by secrecy, the role in irregular warfare by a group not governed by any nation raises major red flags as to the extremes to which irregular warfare is being practiced.

"PMSCs [**private military security contractors**] also **pose substantial risks for a regime** determined to keep a lid **on domestic outcry** over its military adventurism **and** to manage **blowback.** The advent of the **digital age means PMSC activities are often hidden in plain sight**, and **disinformation is no longer a failsafe remedy** when the secrecy of covert operations is compromised. The **lack of a clear legal architecture** for Russian PMSCs can encourage risk taking, a dynamic that has already **led to direct confrontations** with the U.S. forces in Syria and degraded Russia's efforts to manage escalation. Consequently, Russia places **a high premium**

---

[146] Joy, William. "New video reveals more about Texas connections to attack on US Capitol". *WFAA-ABC.* 17 January 2021.

[147] United Nations General Assembly Human Rights Council. Thirty-fourth session. 27 February-24 March 2017. *Report of the Commission on Human Rights in South Sudan*. A/HRC/34/63. https://undocs.org/A/HRC/34/63 p. 17

[148] https://www.bbc.com/news/world-africa-52571777?xtor=AL-72-%5Bpartner%5D-%5Binforadio%5D-%5Bheadline%5D-%5Bnews%5D-%5Bbizdev%5D-%5Bisapi%5D ; Atlamazoglou, Stavros. "How Putin's favorite mercenaries are using secretive operations to tip the balance in Africa". *Business Insider*. 9 September 2020; U.S. Africa Command Public Affairs. "Russia and the Wagner Group continue to be involved in ground, air operations in Libya". United States Africa Command webpage. 24 July 2020; https://www.middleeasteye.net/big-story/libya-russia-wagner-mercenaries-sprayed-bullets

[149] Atlamazoglou, Stavros. "How Putin's favorite mercenaries are using secretive operations to tip the balance in Africa". *Business Insider*. 9 September 2020.

on narrative control. The Wagner Group narrative of "ghost warriors" on far flung battlefields obscures operational objectives, tactics, and the diversity of agents at work. Separating myth from fact about Russian PMSCs is critical for understanding Russia's proxy strategies. **Russian PMSCs are designed for strategic deception."**[150]

One example of a strategic deception provided by Wagner Group comes from Gen. Mattis over the bombing of a US base by Wagner Group in Deir Al-Zeor, Syria. Mattis denied any knowledge of the strategic significance of Deir Al-Zeor. Deir Al-Zeor was bombed by Israeli Air Force with CIA support in 2007 on suspicions it housed a nuclear plant. Israel admitted to bombing the strategic location as a nuclear target 11 years earlier one month (February 16, 2018, March 20, 2018) after Wagner group attacked US troops on base in Syria. [PRINTED ARTICLES - REWORD]

"But Libya is just one African battlefield where Wagner is currently engaged. Wagner mercenaries and Russian advisers can also be found in Rwanda, Madagascar, Sudan, the Central African Republic, and Mozambique. **The US's decision to reduce its footprint in Africa has opened the door for other powers**… **'Wagner also fits in the larger strategic philosophy of** Gen. Gerasimov, the so-called Gerasimov doctrine, **filling that space between war and peace**, or the 'gray zone,' Hassan [Ahmed Hassan, CEO of Grey Dynamics, an intelligence consulting firm] added".[151]

"Interior minister Fathi Bashaga said GNA [Libyan Government of National Accord] forces were 'exposed to nerve gas, paralysed and then sniped' [by Wagner Group]."[152]

[TOPIC – irregular warfare adopted by US as signal of nation's decline in power]
"**Most US operations since the 11 September 2001 terrorist attacks have been irregular**; this caused the problem of calling irregular or nontraditional what we do routinely … In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government**. The less powerful adversaries, who can be state or non-state actors, often favor indirect and asymmetric approaches, though they may employ the full range of military and other capabilities** in order to erode their opponent's power, influence, and will. Diplomatic, informational, and economic methods may also be employed. The weaker opponent could avoid engaging the superior military forces entirely by attacking nonmilitary targets in order to influence or control the local populace. Irregular forces, to include partisan and resistance fighters in opposition to occupying conventional military forces, are included in the IW formulation. Resistance and partisan forces, a form of insurgency, conduct IW against conventional occupying powers. They use the same tactics as described above for the weaker opponent against a superior military force to increase their legitimacy and influence over the relevant populations… **An enemy using irregular methods will typically endeavor to wage protracted conflicts** in an attempt to exhaust the will of their opponent and its population.

---

[150] https://d1y8sb8igg2f8e.cloudfront.net/documents/Decoding_the_Wagner_Group.pdf p. 7
[151] Atlamazoglou, Stavros. "How Putin's favorite mercenaries are using secretive operations to tip the balance in Africa". *Business Insider*. 9 September 2020.
[152] https://www.bbc.com/news/world-africa-52571777?xtor=AL-72-%5Bpartner%5D-%5Binforadio%5D-%5Bheadline%5D-%5Bnews%5D-%5Bbizdev%5D-%5Bisapi%5D

Irregular threats typically manifest as one or a combination of several forms including **insurgency, terrorism, disinformation, propaganda, and organized criminal activity based on the objectives specified (such as drug trafficking and kidnapping). Some will possess a range of sophisticated weapons, C2 systems, and support networks that are typically characteristic of a traditional military force**. Both sophisticated and less sophisticated irregular threats will usually have the advantages derived from knowledge of the local area and ability to blend in with the local population."[153]

+ADD "Irregular warfare manufactures the fog of war for victory".[154]

Analysts of the NATO Strategic Communication Centre of Excellence, "tasked to conduct a study on how social media can be used as a weapon of hybrid warfare," write in their 2015 publication *Internet Trolling as a Tool of Hybrid Warfare: the Case of Latvia*:

> It is essential to briefly outline the key concepts used for the purposes of this research on the weaponisation of online media and trolling. Recently the term hybrid warfare has been extensively used to describe the complex strategy of Russia in the Ukraine crisis. According to various political **analysts hybrid warfare is usually a combination of regular warfare with intelligence and diversionary methods, as well as information and cyber warfare**. However, hybrid warfare is neither a new concept nor a helpful one. As Damien Van Puyveld argues: "Any threat can be hybrid as long as it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as hybrid, the term loses its value and causes confusion instead of clarifying the 'reality' of modern warfare".
> **Information warfare (or information war as commonly used in the media) is a much more precise term describing a specific type of war strategy**. According to John J. McCuen, information warfare is aimed at gaining "the support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community". However, information warfare, like hybrid warfare is not a new phenomenon. Shawn Powers argues that media has been used as a weapon since at least the beginning of the 20th century. Another useful term in this context is that elucidated by Thomas Elkjer Nissen – psychological warfare. It implies "influencing the target audience's values and belief system, their perceptions, emotions, motives, reasoning, and ideally, their behaviour. It is (...) aimed at maintaining the support of the loyal; convincing the uncommitted and undermining the opposition. This is achieved through influencing people's perception of what is going on and, in turn, influencing their online and offline behaviour by playing on emotional and logical arguments drawn from conversations and history, and by tapping into an existing narrative". An illustrative example of psychological warfare was recently reported by Radio Free Europe. Just a day before Ukraine's snap presidential election on 26 October 2014, hackers accessed electronic billboards in Kyiv and broadcast gruesome images of what they portrayed as civilian losses caused by Ukrainian forces fighting pro-Russian separatists in eastern Ukraine. However, at least one of those images was proven to pre-date the conflict in Ukraine by nearly two decades. Even more, it actually portrayed a Russian soldier standing over mass graves of

---

[153] Joint Publication 1: Doctrine for the Armed Forces of the United States. 25 March 2013 Incorporating Change 1, 12 July 2017. https://www.jcs.mil/. p. I-5 - I-7.

[154] https://thehill.com/opinion/national-security/519948-irregular-warfare-with-china-russia-ready-or-not-its-coming-if-not

> civilians in Chechnya in 1995, during Russia's own war with Chechen separatists. The novelty of current information and psychological warfare is the combination of the two through the weaponisation of online media. **The factors that make this strategy so powerful are that this type of 'warfare' is continuously ongoing and hard to detect**… Nissen highlights several **military activities that use social network media: intelligence collection, targeting, psychological warfare, offensive and defensive cyber-operations, and command and control activities**.[155]

+ADD "the targets of information manipulation are largely civilian, and the battle surface non-military."[156]

+ADD The Serious Role of Wargaming at RAND: "You have an environment in which something is in dispute. That could be, who gets to own Park Place? Or that could be, who gets to own the Baltic republics?"; "Think about, for example, social unrest. Think about events that transpired in Ferguson, Missouri a few years ago… between the police department and the community… Both sides were trying to achieve their own individual goals, but neither side was looking to tip the situation over into a full blown riot, right? Neither side was looking, neither the protesters nor law enforcement, were looking to spark a situation that devolved into pure social disorder. *Well, that's actually a game.* And we've actually designed a game that lets people to explore that space. Not necessarily actors who are butting heads, its simply actors who are in an environment where their goals are not completely congruent with one another."[157]

+ADD DoD *Information Operations Roadmap* 30 October 2003
https://nsarchive2.gwu.edu//NSAEBB/NSAEBB177/info_ops_roadmap.pdf

[TOPIC – Self-play of intel-security state]

" Air Force Officer said: 'The important thing about a war game is the effect of competition – a real game is a two-sided affair'…in analysis the problem of the defense of the U.S. against air attack, the RAND analyst thought through the problem from the defense standpoint. He then changes, hats, mentally, and did his best, as the Red Commander, to beat the defense system. Then he put the defense commander's hat on once more and tried to counter the best offense theat. And so on. This use of the spirit of war gaming – of free competition – may often be the most valuable contribution that gaming has to make to a given problem. Is a staff planning the possible deployment of a mobile tactical force? Then the staff's best man should be given the thankless job of fighting the plan, of acting as obnoxious and obstreperous umpire. We have argued that the essential element in any war game is free competition – the intelligent and obnoxious opponent. But, as we have seen, it is possible to have competition without a formal game. And it is possible to go through the motions of a game with really having completely free

---

[155] Spruds, Andris, Anda Rozukalne, Klavs Sedlenieks, Martiins Daugulis, Diana Potjomkina, Beatrix Tolgyesi, Ilvija Bruge, and Alexander Fokin. *Internet Trolling As a Tool of Hybrid Warfare: The Case of Latvia*. Riga: NATO Strategic Communications Centre of Excellence, 2015. Internet resource. https://stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0 P. 7-8.

[156] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 90.

[157] https://www.rand.org/multimedia/audio/2017/03/23/the-serious-role-of-gaming-at-RAND.html @3:30 ; 4:20-5:30

competition. There is, for example, a strong tendency to avoid making the Red attack too ungentlemanly… Then all kinds of logistic and support plans get written, all based on a rosy assumption that warning was received, that the enemy has initiated hostilities in a gentlemanly manner – that efforts to attain air superiority are both possible and rewarding – and that there is also some place to withdraw to. Now I wouldn't say a war game will tell you how to write a better plan, but the exercise of a plan against a free thinking opponent may bring to light a lot of foolish optimism, lazy thinking, and sheer lack of coordination that otherwise would go unnoticed."[158]

[TOPIC – best practices ignored by wargamers]

"Most nations have some system for inspection and/or testing to determine unit readiness and capability for combat. This procedure usually consists of a written exam as well as drills to demonstrate troop knowledge of their skills and the unit's ability to perform its combat mission. In light of how this is usually done, here are a few pointers on how to insure that it won't work (it usually doesn't):

1. Don't allocate a lot of importance to combat-capability evaluation. It's much more important that the equipment and troops look good and that all those administrative items be in top shape. After all, you have to live with noncombat items every day, and a war may never come: Real soldiering is a peacetime profession.
2. Make sure the troops have memorized a lot of facts about weapons characteristics and procedures. This knowledge is easy to evaluate. Don't bother taking a lot of time working on the questions; take them right out of the technical manuals. The troops should be reading these things constantly anyway instead of spending a lot of time working with their gear and finding ways to wear it out.
3. Don't worry if the troops are able to get a copy of the tests beforehand. This will allow them to brush up and make a good showing. Don't sweat it if the officers coach the troops on how to respond to questions and drills to be used. This will make the training officer's job much easier.
4. Don't worry if the test is not realistic. Realism is too complicated and will just muddy the waters.
5. The only score that is important is the one for the entire unit. This way you can have a few ace troops carry all the duds. It's too much trouble to get all the troops up to speed anyway.
6. These evaluations are such a hassle that they should be run infrequently. Not quarterly, semiannually, or yearly, but every few years.
7. Make sure that commanders are so intent on making a good showing on the standardization evaluation that they neglect any special training to reflect their particular mission or location. Let's keep everything neat throughout the armed forces."[159]

[TOPIC – news media role in wargames]

Rightly explaining the devastating course of US policymaking, Brad Setser, a senior fellow at the Council on Foreign Relations in New York is quoted in *The New York Times* in December 2019 saying that, "'The sense that policy moves in one direction, toward more liberalization and more integration, has been replaced by recognition that policy can go backward as well as forward.'" +ADD NIC's *Paradox of Progress* report

---

[158] Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957.

[159] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 305-6.

He says this in regard to US-China trade policy. The article continues to contend that, "China's leaders have come to construe trade hostilities as part of an American bullying campaign engineered to suppress their national aspirations and deny the country its rightful place as a superpower. Nationalist sentiments and security concerns have become intertwined with trade policy..."[160] [REWORD]

The principle author of the article, Peter S. Goodman, a journalist by trade and East Asia area specialist by education, remarks in *The Washington Post* about his *New York Times* work, saying it is done in an adversarial rejoinder-style with think tanks, which he describes as "almost a process of laundering my own views, through the tried-and-true technique of dinging someone at some think tank to say what you want to tell the reader."[161] His work at *The New York Times*, however, affirms almost verbatim the think tank predictions set out in NIC's *Global Trends 2025* published in 2008.

In the National Intelligence Council report's first policy scenario "Global Scenario I: *A World Without the West,*" a "fictionalized account" in which the West loses global hegemony, the scenario names the sociopolitical "preconditions for this scenario," which unfortunately are the precise real world policies taking effect now (ten years later) at the urging of the same policymakers. These preconditions include: "Lagging Western growth prompts the US and Europe to begin taking protectionist measures against the faster-growing emerging powers," and "Tensions between the principal actors in the multipolar world are high as states seek energy security and strengthened spheres of influence."[162]

Goodman's *Times* article quotes Meredith Crowley, international trade expert at the University of Cambridge, saying, "People are dissatisfied with the complexity of policy and this feeling that those who have the levers of policy are somehow out of their reach." As I argue in the section Monopoly on Violence, Monopoly on Infringement, journalists very much fall under the category of policymaker and have been understood as such since Max Weber published his essay *Politics as a Vocation* in 1921.

The irony of journalists at *The New York Times* citing personal interviews with experts at Cambridge University to assert comradery with the average person in lack of access to the instrumental tools of policymaking is exaggerated in the article's exceedingly self-aware attempt to downplay US journalism's role in sensational fearmongering for policy leverage. The *Times* article stops just short of predicting a World War III which would be ignited by bad trade policies, framing 1939 preconditions in the West in the words "world trade disintegrated, nationalist rage spread, culminating in the brutalities of World War II."[163]

Reuters has reported on electronic weaponry defense planning in response to a US-China trade war, saying that "the Pentagon would need to spend about $50 million to build a U.S. rare earth magnet facility. 'It's a small amount of money to pay so if we go to war with China, we're not calling them up asking for supply' of rare earth magnets."[164]

The above is an example of the coordination between policymakers and journalists in order to bring about bleak policy visions that negatively affect the US. In his role as purported adversarial journalist to regular governmental policymakers, Peter S. Goodman of *The New York Times* speaks policymakers' dystopian predictions into reality, even proclaiming it a "new age" and

---

[160] Goodman, Peter S. "Brexit's Advance Opens a New Trade Era". *The New York Times.* 13 December 2019.
[161] Kurtz, Howard. "Huffington snags N.Y. Times star". *The Washington Post.* 21 September 2010.
[162] Global Trends 2025 P. 37.
[163] Goodman, Peter S. "Brexit's Advance Opens a New Trade Era". *The New York Times.* 13 December 2019.
[164] Scheyder, Ernest. "Exclusive: Pentagon to stockpile rare earth magnets for missiles, fighter jets". *Reuters.* 20 December 2019.

"new era" which have ended the economic hegemony of "the powers that be for more than seven decades". [165]

The policy objectives are brought into the real world through the media in five significant ways:

1) **bringing attention to pre-selected policy points** on US-China trade predictions of "lagging Western growth" and nationalistic "protectionist measures",
2) **prompting the pre-scripted secondary reaction** of increasing "tensions" between competing "spheres of influence",
3) **synthesizing the policy** global environment as "the end of the West",
4) **analyzing the policy as bad decisionmaking**,
5) **downplaying journalism's role in the policymaking process**.

Instances like points one, two and three discussed here on US-China trade play an important role in bringing wargaming and scenario predictions to life. **The above example discusses how US-China trade policy is currently being engineered by US Intelligence and other policymakers to create the necessary "preconditions" for a "world without the West".** This does not mean that these policies are not truly in effect; rather, the media acts as propaganda to guide and increase the desired effect of the policies.

Point four serves a purpose in the psychological warfare of government-led popular opinion-making. The policy is deemed catastrophic to hit at the "ultimate target" (a psy-op term) - usually whoever is named in the article, often public politicians and sometimes other decisionmakers. The article is published for wide readership to the "intermediate target" - individuals with influence over an ultimate target, in this case the public.

The fifth point reinforces in the minds of the ultimate and intermediate targets the role of the press as "unintended target" - "audiences that the planner did not intend to reach, but those who received the message directed at another audience."[166]

In reality, journalists are much more than incidental messengers. By downplaying journalists' role as conscripted policymakers, and by identifying more with the average uninfluential person, journalists are able to take themselves out of the equation when relaying messages to priority targets. They can thereby play a crucial role in the psychological operation theater as individuals apparently outside the theater of policymaking, while maintaining their particular hold on "unintended" policy leverage.

+ADD? https://www.nytimes.com/2019/12/08/business/trump-trade-war-wto.html / https://www.nytimes.com/2019/11/01/business/wto-china-us-trade.html

In another example of Intelligence scenarios being brought into real world: "**Imagining a surprise news headline in 2019 . . . China Buys Uninhabited Fijian Island To Build Military Base** February 3, 2019 – Beijing A Chinese development firm—with links to the Chinese Government and People's Liberation Army— today announced that it recently purchased the uninhabited Cobia Island from the Government of Fiji for $850 million. Western security analysts assess that China plans to use the island to build a permanent military base in the South Pacific, 3,150 miles southwest of Hawaii."[167] **Real world news story with admission of**

---

[165] Goodman, Peter S. "Brexit's Advance Opens a New Trade Era". *The New York Times.* 13 December 2019.
[166] Clow, Ryan. "Psychological Operations: The Need To Understand The Psychological Plane of Warfare". *Canadian Military Journal (CMJ), Vol. 9, No. 1.* 2008, p. 26.
[167] https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf 2017. p. 36

hypothetical situation to push US security policy: "'Impossible': China denies planning military base in Vanuatu… A Chinese embassy spokesman has said the idea that China is planning to establish a military base in Vanuatu is 'ridiculous'. Australia's Fairfax Media reported on Tuesday that China was eyeing a base in the Pacific nation. 'That's impossible,' said Chen Ke, a spokesman for the ambassador to Vanuatu. A senior Vanuatu government adviser concurred: 'That conversation was never on the table.' The adviser claimed detailed knowledge of relevant matters in two key ministries and insisted that the topic was never even hinted at. **They went on to suggest that the source of the Fairfax story was not the government of Vanuatu.** Fairfax reported there had been informal discussions between China and Vanuatu, but no formal offer, about a military buildup. China has diplomatic relations with many Pacific nations and is a major backer of development projects in Vanuatu, Papua New Guinea and Tonga. The Australian foreign minister, Julie Bishop, told the ABC on Tuesday morning she remained 'confident that Australia is Vanuatu's strategic partner of choice'… 'I think there's no question that **Australia needs to redouble its efforts to persuade Vanuatu and other Pacific island nations that Australia is and should remain their preferred security partner** and development partner. Perhaps **it's time for New Zealand to get more worried about the implications of Chinese power in the South Pacific as well**.' On Tuesday morning the New Zealand prime minister, Jacinda Ardern, said 'New Zealand is opposed to militarisation of the Pacific'. Her **foreign minister, Winston Peters, said: 'This is hypothetical** as Vanuatu have stated that they are not aware of a military base being built. More generally the militarisation of the Pacific is something we've been seriously concerned about as there are certain things that are not good for the long term peace and security of the Pacific, or for democracy itself.'… [**Head of the national security college** at the Australian National University Rory Medcalf]: '**[Vanuatu] would be useful for China if it got itself in a strategic confrontation with the US** … to be able to outflank the US and the Japanese. It would allow them to have some forces positioned behind the US base in Guam and would allow China to monitor and patrol the South Pacific Ocean.' Medcalf said China was increasingly seeking to exert influence in the South Pacific. He said establishing a military presence could be a sort of payoff for development aid. **Chinese activities in the Pacific have been increasingly viewed through a military lens since the US 'pivot' to the region in 2009**. The US has a series of bases and training locations – running from Busan in Korea to Darwin in the Northern Territory – that many analysts believe is designed to demonstrate an ability to isolate China and block shipping supply routes. **Analyst Charles Edel, a senior fellow at the University of Sydney's US studies centre**, is concerned about the potential that China has been engaging in 'debt-trap diplomacy'. **'We've seen variations on this in other parts of the world,' said Edel, who was an adviser to the former US secretary of state** John Kerry. 'China does not import [energy] from the South Pacific, which begs the question why are they there. There are a number of other reasons, but **one of them is clearly a strategic play, given the US bases in the Pacific. It increases the risks and challenges to the US.'…** Prof Sam **Bateman**, a professional research fellow at the University of Wollongong's Australian National Centre for Ocean Resources and Security and **a former Australian navy commodore,** said Vanuatu would offer 'some strategic advantages' for China, but that a military buildup in the country remained unlikely. He said China's economic interest in the South Pacific was 'really only fish'. Bateman said **Chinese involvement in the South Pacific could upend the status quo**, where Australia and New Zealand take a lead role in the Pacific Islands Forum. **'It would be interesting to see what would happen, for example, if China was to play a role**

in those institutions,' he said."[168] ; ***The Guardian*** **"Opinion: Australia must prepare for a Chinese military base in the Pacific":** "**Only their strategic significance has attracted us**: the islands scattered widely across the north of our continent [Australia] are critical to our protection from armed attack. Our closest neighbours are crucial to the defence of our continent simply because of their proximity… 'We would view with great concern the establishment of any foreign military bases in those Pacific Island countries and neighbours of ours.' That was then prime minister Malcolm **Turnbull in April 2018, responding to press reports last April that China was seeking to build a naval base in Vanuatu**. **The story was swiftly and categorically denied by both Beijing and Port Vila**, and Julie Bishop, then minister for foreign affairs, poured cold water on it. **While it may prove a false alarm**, it seems Canberra has received credible indications that China is indeed actively seeking a military base somewhere in the South Pacific. **It would be hard to overstate the significance of such a development, were it to occur.** This would be the **first time since** Japan was pushed out of the islands at the end of **the Pacific War** that any major power, other than one of our allies, has sought a military base so close to Australia… **it would send an unambiguous message to us here in Australia**, signalling Beijing's rejection of our claims to our own sphere of influence in the South Pacific, and **sending a stark warning of China's reach and its capacity to punish us if we side too vociferously with the US or Japan against it**. Abandoning the sphere of influence. What can Australia do, then? One option is a radical recasting of our relations and role in the South Pacific, to draw our neighbour much more closely under our wing. But the better option would be to step back, abandoning our traditional ideas about keeping intruders out of the South Pacific. In fact, there may be no alternative. China poses an unprecedented challenge to the strategic assumptions that have framed our [Australian] policies since European settlement. We have never encountered an Asian country as powerful as China is now, let alone as powerful as it will likely become in the decades ahead. The costs to us of trying to keep China out of the region might simply prove impossible to bear. Building forces that could counter Chinese bases in our neighbourhood would mean that we could feel less anxious about the establishment of such bases, and relax the imperative to preserve the sphere of influence we have for so long assumed we must maintain. This would not mean abandoning all interest in our nearest neighbours and succumbing to the indifference that has historically weakened our relationships with them. On the contrary, we should make great efforts to maximise our role and presence – not in the form of an exclusive sphere of influence, but as one of the region's major partners. It is possible to imagine Australia actively engaged in the South Pacific not to exclude China (or any other power), but to work with it where possible, and to work against it where necessary, to protect our interests and the interests we share with our small neighbours as best we can. We should start to treat our smaller close neighbours as independent at last. The uncomfortable reality is that preserving an exclusive sphere of influence in the South Pacific is not going to be possible against a regional power that is far stronger than any we have ever confronted, or even contemplated. It might turn out that the more we try and fail to exclude China from the South Pacific, the less influence we will have there. If Scott Morrison [Australian Prime Minister] is as serious about the South Pacific as he claims, he should start, paradoxically perhaps, by

[168] https://www.theguardian.com/world/2018/apr/10/concerns-china-in-talks-with-vanuatu-about-south-pacific-military-base

abandoning the idea of an exclusive sphere of influence…" In this case, China's strategic role is actually being played by the US.

In this section on irregular wargames and wars, …

Former National Security Council and State Department analyst Laura Rosenberger and researcher Lindsay Gorman are of the belief that "construing information as a weapon or engaging in information warfare involving non-military targets risks undermining the very space democracies seek to protect."[169]

"Unlawful Deceptions: Certain deception techniques may amount to "perfidious acts" due to their treacherous nature. Perfidious acts are prohibited under the **law of armed conflict** (LOAC) because they undermine the effectiveness of the law of war and thereby **jeopardize the safety of civilians and noncombatants** and/or the immunity of protected structures and activities."[170]

Glen, Russell W., Jamison Jo Medby and Scott Gerwehr. "To Be Ready, Not Reacting: Adapting For Future Urban Operations": Critical points of Urban warfare include "key media concentrations". (p. 29) ; "Gaining the cooperation of PVOs and NGOs can relieve units of noncombatant support tasks that detract from combat operations. Further, **NGO and PVO activities that cause the temporary departure of noncombatants from given urban areas can reduce the density of civilians in areas where chances of injury or death are high. Their departure also decreases the likelihood they will interfere with friendly force operations.** More active pre-operation coordination with these organizations, **such as inviting them to participate in training exercises and simulations**, would better prepare both military and civilian agencies for operational contingencies." [171]
In other words, refugeism is encouraged urban warfare policy by DoD analysists. The US military is encouraged by policy to partner with local NGOs in order to displace populations in preparation for further military action. The analysts' rhetoric phrases their refugeism policy as if it were done benevolently to make military occupation safer for the persons being displaced, instead of being a common result of military occupation. It is also wrongly assumes that displaced persons avoid injury or death by becoming wartime refugees.

Under "Urban Intelligence Preparation of the Battlefield": "Step 3 (Threat Evaluation): usually assumes that a threat must exist. This assumption, to an extent a vestige of IPB's Cold War roots, unnecessarily contains application of the process during the many urban operations (or components of urban combat operations) in which no threat exists."[172]

The argument here is that intelligence-led threat detection processes should be conducted even when no threat actually exists. It is stated that this has been the standard US military-

---

[169] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, P. 76.
[170] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-10
[171] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 29-32.
[172] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 34-

intelligence condition since the end of the Cold War, suggesting that US action has been taken consistently without provocation or threat since 1991.
+ADD Joint Forces "MILDEC planning can be deliberate planning (used normally during peacetime to develop operation plans and operation plans in concept format)… Successful deception operations are those that do more than make the target "believe" or "think" that the deception is true. MILDEC must end in an action, or inaction, that supports the JFC operational plan… **Deception planning is** an iterative process that requires continual reexamination of its **objectives, target, stories, and means throughout the planning and execution phases**. A key factor that must be considered during MILDEC planning is risk. The overriding consideration in risk analysis is the comparison between the risk taken and the possible benefits of the deception. The MILDEC planning process consists of six steps**: deception mission analysis, deception planning guidance; staff deception estimate; commander's deception estimate; Chairman of the Joint Chiefs of Staff estimate review; deception plan development; and deception plan review and approval**."[173]

[TOPIC – International wargaming trend in societies]

"In 2012, a senior **Russian** general published a paper articulating what became known as the Gerasimov Doctrine, calling for 'the use of special-operations forces and internal opposition to create a permanently operating front,' including engagement in 'long-distance, contactless actions against the enemy' via 'informational actions, devices, and means.'[174]

[TOPIC - nuclear security wargaming in scientific community]

The Relativistic Heavy Ion Collider in Brookhaven National Laboratory, NY & CERN, Switzerland. "Franceso Calogero, **Italian** physicist and former secretary general of Pugwash, an organization that pursues ways to reduce threats to global security, championed an alternative way to deciding how risky an experiment might be. In a paper entitled, 'Might a laboratory experiment destroy planet Earth?', he backed for a more adversarial approach to risk analysis. Instead of one panel of experts, there should be two. The first**, the blue team**, makes the case for the experiment's safety, while **the red team** does its best to emphasise the dangers. The two then come together and decide whose arguments are the most robust. 'It is not perfect, but I think it is the best strategy,' says Calogero. 'It overcomes any perceived vested interest and gives people a chance to point out arguments that are not watertight and what might go wrong.'"[175]

In other words, a debate is held for the purpose of discussion and decisionmaking. The jargon of wargaming – red team and blue team - , as well as the doomsday title "Might a laboratory experiment destroy planet Earth?" are telltale signs of influence from the US wargaming industry on the international nuclear scientific community.

"In conventional warfare, the enemy is clearly defined and the goal is to defeat the enemy through any means possible. However, COIN [counterinsurgency] operations are more delicate. **Actions are 'constantly directed towards a political goal,'** and the primacy of political over

[173] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. xi-xii
[174] Click here to kill everybody, p. 71.
[175] Berlatsky, Noah, ed. *Doomsday Scenarios*. Greenhaven Press. 2011, p. 116.

military power is key. More boots must be on the ground, working with the local populations, as opposed to remaining at a distance and striking from afar. In COIN, the focus is on 'highly mobile and lightly armed infantry,' instead of rumbling tanks and explosive bombs. **The importance of intelligence and information technology is paramount to success in irregular campaigns**."[176] [Emphasize terrorism of irregular warfare 'directed towards a political goal']

[Subsection? TOPIC – Wargame conduction can constitute actual war/state of war]

"The US Navy destroyer USS John S. McCain sailed through the Taiwan Strait Thursday, marking the first such transit since President Joe Biden took office. **The US Navy's Theodore Roosevelt carrier strike group entered the contested waterway at the same time, and the Chinese aircraft conducted a simulated attack run, using the American aircraft carrier as a mock target.** US Indo-Pacific Command said in a statement that "the Theodore Roosevelt Carrier Strike Group closely monitored all People's Liberation Army Navy (PLAN) and Air Force (PLAAF) activity, and at no time did they pose a threat to US Navy ships, aircraft, or Sailors." **The US military criticized China's actions as "aggressive and destabilizing"** as the State Department called out Beijing for its efforts to militarily, economically, and diplomatically pressure Taiwan."[177]

Weeks later after this story was published, it was revealed that the Chinese intrusion into Taiwan airspace took place in response to a US wargame conducted in September 2020: "Last fall, the U.S. Air Force simulated a conflict set more than a decade in the future that began with a Chinese biological-weapon attack that swept through U.S. bases and warships in the Indo-Pacific region. Then a major Chinese military exercise was used as cover for the deployment of a massive invasion force. The simulation culminated with Chinese missile strikes raining down on U.S. bases and warships in the region, and a lightning air and amphibious assault on the island of Taiwan. The highly classified war game, which has not been previously made public, took place less than a year after the coronavirus, reportedly originating in a Chinese market, spread to the crew of the USS Theodore Roosevelt aircraft carrier, taking one of the U.S. Navy's most significant assets out of commission. Then in September in the midst of the war game, actual Chinese combat aircraft intentionally flew over the rarely crossed median line in the Taiwan Strait in the direction of Taipei an unprecedented 40 times and conducted simulated attacks on the island that Taiwan's premier called 'disturbing.' Amid those provocations, China's air force released a video showing a bomber capable of carrying nuclear weapons carrying out a simulated attack on Andersen Air Force Base on the U.S. Pacific island of Guam. The title of the Hollywood-like propaganda video was 'The god of war H-6K [bomber] goes on the attack!'… In Senate testimony on Tuesday, the head of U.S. Indo-Pacific Command, Adm. Phil Davidson, warned that he believes China might try and annex Taiwan 'in this decade, in fact within the next six years.'… In the early 2000s, China experts and military analysts at the RAND Corporation were given a trove of classified U.S. intelligence on Beijing's military plans and weapons programs, and were asked to war-game a confrontation 10 years into the future… China's answer was a well-funded strategy that the Pentagon refers to as 'anti-access, area denial' (A2/AD), meaning it would prevent an adversary like the U.S. from being able to carry out the sort of significant military buildup it carried during the two Iraq wars. The PLA's military plans rely on space-based and airborne surveillance and reconnaissance

[176] Parisi, Jessica, "Game Changers in US Defense Strategy: An Examination of the Causes Behind the Increased Emphasis on Irregular Warfare Since 9/11". *CUREJ: College Undergraduate Research Electronic Journal, University of Pennsylvania.* 08 April 2011, p. 4.
[177] https://www.msn.com/en-us/news/world/a-us-navy-warship-sailed-through-the-taiwan-strait-for-the-first-time-since-biden-became-commander-in-chief/ar-BB1dopBg

platforms; massive precision-guided missile arsenals; submarines; militarized man-made islands in the South China Sea; and a host of conventional air and naval forces to hold U.S. and allied bases, ports and warships in the region at risk. Because it lies only 90 miles from Taiwan, China needs only to hold U.S. forces at bay for a matter of weeks to achieve its strategic objective of capturing Taiwan. 'Whenever we war-gamed a Taiwan scenario over the years, our Blue Team routinely got its ass handed to it, because in that scenario time is a precious commodity and it plays to China's strength in terms of proximity and capabilities,' said David Ochmanek, a senior RAND Corporation analyst and former deputy assistant secretary of defense for force development. 'That kind of lopsided defeat is a visceral experience for U.S. officers on the Blue Team, and as such the war games have been a great consciousness-raising device.'… Hinote [Air Force Lt. Gen. S. Clinton Hinote, deputy chief of staff for strategy, integration and requirements] pointed out that the Blue Team force posture tested in the **recent war game is still not the one reflected in current Defense Department spending plans**. 'We're beginning to understand what kind of U.S. military force it's going to take to achieve the National Defense Strategy's goals,' he said. 'But that's not the force we're planning and building today.'"[178]

+ADD from Wargaming chapter of *Future War* book (Navy War College) on wargaming and budgets

"AMPHIBIOUS DEMONSTRATION—OPERATION DESERT STORM During the early days of DESERT SHIELD, a powerful **18,000-man amphibious task force steamed into the North Arabian Sea to add an important element to the allied arsenal**. Within less than a month after the Iraqi invasion of Kuwait, more than 20 amphibious ships from ports in Virginia and California completed the roughly 10,000-mile trip to the Gulf of Oman, where nearly 8,000 Marines and 10,000 Sailors commenced full-scale preparations to "hit the beach" to eject Iraq's army from Kuwait. The task force, with Marines from the 4th Marine Expeditionary Brigade (MEB) and 13th Marine Expeditionary Unit embarked, included air, land, and sea assets tailor-made for coastal assault— Harrier attack jets and assault support helicopters to provide air cover for infantry, and armor that would hit the beach aboard high-speed landing craft, aircushion vehicles. The Task Force, quickly forged from several amphibious ready groups, represented the largest amphibious assault force assembled in more than 30 years. **They also completed demanding shipboard drills and amphibious assault training on coalition beaches. That training grew more intense as the amphibious forces performed high-visibility exercises off the coast of Saudi Arabia to heighten the enemy wariness of an invasion from the sea.** The amphibious presence grew larger following President Bush's 8 November decision to nearly double US forces in theater. The 13 ships of Amphibious Group Three arrived from three west coast ports with nearly 15,000 Marines of the 5th MEB embarked to join the amphibious task force. As the ground war commenced, nearly 17,000 Marines stood ready aboard the largest combined amphibious assault force since the Inchon landing in Korea**. Only then did the Sailors and Marines of the amphibious force learn that their warfighting skills would not be immediately required as they had expected. But their preparation had not been in vain. It was at the core of the deceptive tactics which played a major role in the quick allied victory. Amphibious operations focused enemy attention on the threat from seaward and**

[178] https://news.yahoo.com/were-going-to-lose-fast-us-air-force-held-a-war-game-that-started-with-a-chinese-biological-attack-170003936.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANby48bfCSdj3vupdXvgd_DQIq_wWXsut75OOlxSageVw24niJW1wvyZ1R0g2txWhN90wlzHEAIC8q5zc0zsLSopufvZtk76bnqScy3F1M_1rAm1M8uQXjrPsWaFSnMxC1oXGdmn9hlIgVLAC5kGWPYCFKKhCr4j0Rnb49EtcNZ8

tied down at least seven Iraqi divisions, even after the coalition ground campaign was well under way. SOURCE: Department of the Navy, Naval Historical Center"[179]

"FEMALE SPEAKER #1: What?
FEMALE SPEAKER #2: Whoa!
FEMALE SPEAKER #1: What was that?
FEMALE SPEAKER #3: Is that real-world?
FEMALE SPEAKER #2: Real-world hijack.
FEMALE SPEAKER #1: Cool!
…
SPEAKER 1: Is this explosion part of that that we're looking at now on TV?
SPEAKER 2: Yes.
SPEAKER 1: Jesus …
SPEAKER 2: And there's a possible second hijack also—a United Airlines …
SPEAKER 1: Two planes?…
SPEAKER 2: Get the fuck out …
SPEAKER 1: I think this is a damn input, to be honest.
…
BACKGROUND MALE SPEAKER: Langley's on battle stations.
FEMALE SPEAKER: Fuck.
FEMALE SPEAKER 2: What?
BACKGROUND MALE SPEAKER: Battle stations.
FEMALE SPEAKER: Langley.
FEMALE SPEAKER: LFI.
FEMALE SPEAKER: I know. I hope they cancel the exercise**,** because this is ridiculous.
…
SGT. ZUBON: You guys watching the news?
NEADS TECHNICIAN: Yeah, they've got it on in the battlecab right now.
ZUBON: Oh, do they?
NEADS: Yeah.
ZUBON: Yeah, I've been watching it for about ten minutes, and I said "I wonder if they're--did they suspend the exercise?"
NEADS: Not at this time, no**.**
ZUBON: Not yet?
NEADS: But I think they're going to. I don't know. (Laughing).
ZUBON: Yeah, I would imagine.
NEADS: Things look pretty horrific out there.
…
MALE SPEAKER 1: You know, let's get rid of this goddamn sim, turn the sim switches off, let's get rid of that crap."[180]

Herman Kahn writes in *On Thermonuclear War*:

---

[179] file:///E:/joint%20forces%20college%20military%20deception%20MILDEC.pdf p. I-10
[180] 9/11 NEADS TAPE TRANSCRIPTION DRMl DAT2 Ch.2 MCC Upside Transcribed by Jackie Herter from the audio tapes provided to Alderson Reporting. <NYC_Box3_NEADS-CONR-NORAD-TranscriptNEADSChannel02.pdf>.

> I mentioned **in discussing World War III** (1951) that much of our international difficulties stemmed from the fact that the Soviets had become an important European and Asiatic power as a result of World War II. Their becoming a World Power is likely to have even more far-reaching effects. It could mean, for example, **the penetration by peaceful and subversive means of Africa and the Western Hemisphere**. Sometimes people misunderstand the impact of such terms as 'parity' and 'World Power.' **They seem to think of them as a score in some interesting but irrelevant game.** It is not at all like that. Soviet successes and achievements – the growth of the Soviet 'presence' – **could well mean that the West has to move into a smaller house – that our children will not be as well fed**. (I am speaking halfway between literally and figuratively.)[181]

In *George W. Bush, War Criminal?* Michael Hass chronicles 269 war crimes which the George W. Bush Administration has been accused of, among which are:

> Homicides from beatings… Packing a detainee naked, bound with duct tape, in a shipping container… 'Accidental' eyebrow shaving… Caging… "Bitch in a box" (confining prisoner to car trunk on hot day)… Placing scorpions on body… Chocking and gagging… Breaking limbs and ribs… Standing on the prisoner's body, including neck… Whipping, Chaining (to a harness, the floor, the ceiling)… Spreadeagling (inc. while handcuffed), Straightjacketing of arms and legs… Tied to the top of a vehicle as if a slain deer… Burning pain: Chemical (pouring phosphoric liquid on bodies), Electric burns, Thermal (strapping bound prisoners to hoods of vehicles, causing severe burns), Electric shocks to genitals… Forced administration of drugs, Forced administration of enemas… Biting by dogs and humans, Cutting into flesh, Displaying a nude person who has been strapped to a board… Forced to find objects in excrement, Forced to wear vomit-covered jumpsuit… Wiping hair and clothes in feces and urine…False flag (pretending that the interrogator is from another country)… Forced to bark like a dog and do dog tricks… Forced masturbation, including simulated fallatio"[182]

https://www.jpost.com/Middle-East/Islamic-State-selling-crucifying-burying-children-alive-in-Iraq-389994

+ADD https://academic.oup.com/ejil/article/18/2/253/361968

John Bolton's plan to let the ICC "die on its own" is one of the war crimes he and others are wanted for: "punishment for disobeying an order resulting in death". (p. 268) [MOVE?]

+ADD DoD defended use of war crimes

"Basically, while US troop presence seemingly deters the incidence of international war, it actually contributes to 'a greater likelihood of low-intensity militarized behavior', which is just a euphemism for Hybrid War. The author described what this entails in his book on the general topic and subsequent multi-volume series detailing over 45 country studies related it whose scenarios could be advanced in order to disrupt, control, or influence China's Silk Road projects through the exploitation of preexisting identity conflict variables in the targeted states. As it relates to the RAND study, there's a clear relationship between US troops in 'Lead From Behind' proxy states and an outbreak of Hybrid War in the theater, though the organization of course portrays this as not being related in any way do the US' own policies but instead as a reaction to the so-called 'potential US adversary' that was being targeted all along. Either way

---

[181] Kahn, p. 464.

[182] Hass, Michael. *George W. Bush, War Criminal?: The Bush Administration's Liability for 269 War Crimes*. Praeger: CT. 2009, p. 368-270

and regardless of who initiates it (or as is probably case, if the targeted state proactively defends itself after being provoked, possibly through a false flag 'rebel/terrorist raid into its borders), more often than not the end result of a nearby US troop presence is nevertheless a category of conflict that is best described according to the author's Hybrid War model… Despite recognizing this possibility, it shouldn't be discounted that the penultimate finding of 'U.S. Troop Presence [Being] Associated with Less Intrastate Conflict During the Cold War and More in the Post–Cold War Period' might not entirely be because of where the Pentagon chooses to deploy, which could be in reaction to an outbreak of terrorism in any given country but one that was prepared to occur beforehand by the CIA and other intelligence agencies whose activities aren't included in **the RAND Corporation's analysis. Accordingly, the criteria that they use for defining 'intrastate conflicts' should be examined as well, as they define this in the context of their study as being 'anti-regime campaigns in which domestic opposition groups initiate a coordinated and sustained campaign aimed at achieving maximalist goals against the incumbent regime, have a clear organizational structure, and include at least 1,000 participants or 'full-scale civil wars'. While they importantly clarify that their definition does indeed include 'campaigns [that] employ…non-violent tactics…since even nonviolent movements can radicalize or escalate their tactics',** which is a clear allusion to Color Revolutions and their predisposition to morph into Unconventional Wars in accordance with the author's Hybrid War theory, this still prevents the study from incorporating some levels of modern-day terrorism that fall below their stipulated threshold of being an 'intrastate conflict'."[183]

Paxson, another RAND wargame theorist, took part in game theory scenarios called "murder board briefings"[184] - classified games referred to by Specht as level-"BBRSC" or "Burn Before Reading and Shoot the Courier".[185]

Describing game theory as applied to wargames, Herman Kahn said in a presentation to Air Force officers,

> You see, ideally, what we would like to do is to get the models of your bombers, send them over Russia, see how many get shot down, how many get through, let them run over their bombing runs, then come back. But you can't get cooperation in doing this.[186]

This is not a scenario Kahn proposes but a description of an actual war operation with casualties and international relations risked. Understanding wargames in their functions to both prepare and deceive those who will be most involved in the actual events, or "to mask a surprise attack" as Kahn wrote,[187] is strongly supported by the political military strategic history of the Middle East as grounds for The Great Game.

On Pentagon's acknowledgement that wargaming lends itself to committing real warfare: "In the meantime, the 852 Saudi military students at U.S. military installations will not receive any operational training and will be limited to classroom instruction as part of a security and safety stand-down by the U.S. military services. Esper said that the Pentagon is working closely with

---

[183] Korybko, Andrew. "RAND Corporation Proves Link Between US Military And Hybrid War". *Oriental Review.* 27 February 2018.
[184] Abella, p. 57
[185] Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957.
[186] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, p. 99.
[187] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 237.

the Saudi government in its response to Friday's deadly shooting incident that was carried out by a young Saudi air force officer."[188]

ADD+ "Active measures are semi-covert or covert intelligence operations to shape an adversary's political decisions. Almost always active measures conceal or falsify the source—intelligence operators try to hide behind anonymity, or behind false flags. Active measures may also spread forged, or partly forged, content. The most concise description of disinformation as an intelligence discipline comes from one of its uncontested grandmasters, Colonel Rolf Wagenbreth, head of the East German Stasi's Active Measures Department X for over two decades: 'A powerful adversary can only be defeated through […] a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies […] and within their elites.'"[189] The prevalence of the use of anonymity in 'active measures' or irregular warfare, and the East German Stasi state's influence on the United States' foreign and domestic policy is addressed further in the Conclusions section of this essay. The use of forged content and false flag attacks by US intel-security is discussed in the section The Spectacular Security State.

+ADD US technologist CEOs were accused by the Department of Justice in June of 2020 of employing Stasi-style counter-intelligence tactics against rival website owners. Ebay CEOs … https://www.washingtonpost.com/technology/2020/06/15/ebay-former-employees-cyberstalking/

In wargaming, the sociopolitical conditions are portrayed through obviously engineered media reports that are intended to create something close to the emotional-intellectual state one would feel if the scenario were occurring in the real world. Specific examples of this are discussed at length in the section The VNN Effect.

Wargaming itself is a form of psychological warfare, especially when it is publicized in the media, ostensibly in the interest of public disclosure. According to the Multinational Battle Group, simulated chemical warfare used in an aerial/rugged terrain wargame called "Operation Bowie Strike" enacted in January 2018 in Kosovo functioned both as part of a NATO peace support mission and as a dramatic, "realistic as possible" spectacle of strategic deterrence. Forward Command Post of Multinational Battle Group explained that the NATO peace mission exercise was necessary to demonstrate to Kosovars what the US and "multinational partners" are capable of with regard to Kosovo Forces and territories, with the added benefit that the chemical warfare wargame "indirectly serves as a deterrent factor for those sources of instability or actors that may try to undermine the institutions of Kosovo."[190] Presumably, the lessons learned from Operation Bowie Strike are for those with extremely limited memory recall.

The Associated Press published an article in 2020 titled "Russia's top military officer airs concern about NATO drills" in which it is stated that:

> NATO exercises near the border with Russia reflect the alliance's preparations for a large-scale military conflict, Russia's chief military officer said in remarks published Wednesday. The chief of the General Staff of the Russian armed forces, Gen. Valery Gerasimov, said at Tuesday's meeting with foreign military attaches that NATO's activities have heightened

[188] Martinez, Luis. "DOD suspends operational training for all Saudi students in wake of Pensacola shooting". *ABC News.* 10 December 2019.

[189] Rid, Thomas, p. 1-2 https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

[190]

> tensions and reduced security along the Russian border. He added, however, that Western pressure on Russia could trigger 'crisis situations' that may spin out of control and provoke a military conflict. Gerasimov charged that the scenarios of the alliance's drills in eastern Europe 'point at NATO's deliberate preparation for its troops' involvement in a large-scale military conflict.[191]

In March of 2020 domestic and international defense organizations cancelled the majority of their scheduled wargames, including the massive international wargame DEFENDER Europe, following the World Health Organization's declaration of the COVID-19 pandemic.

[TOPIC - on implications and uses of wargames]

"**U.S. Troop Presence Can Deter Potential Adversaries:** U.S. forward presence may enhance deterrence by improving U.S. and partner capacity to fight and by demonstrating U.S. resolve and alliance cohesion… U.S. Troop Presence Can Embolden Potential Adversaries: U.S. troop presence could actually diminish the overall military resources available to deter potential adversaries and make an adversary more likely to initiate conflict… **U.S. Troop Presence Can Threaten Potential Adversaries:** First, the adversary may worry that **the larger presence indicates that the United States has plans to use force in the region** or that it may be more likely to do so in the future. Second, **U.S. troop presence close to an adversary increases the risk that the two militaries, operating in close proximity to one another, may have accidents or misperceive each other's intentions, resulting in an increased risk of escalation and conflict.** Finally**, incentives to protect U.S. forces near a highly capable potential adversary can lead the United States to adopt military concepts and pursue technologies that could potentially increase both sides' incentives to strike first.** Such pressures for preemption **could make an adversary feel that fullscale war against its homeland is more likely**. An adversary's security concerns can in turn affect the likelihood of conflict. **An insecure adversary may, for example, take long-term steps, such as increasing its defense spending**, to regain security. The United States and its partners may respond with defense spending of their own, **leading to arms races** and a heightened security competition **that could make any of the parties involved—the potential adversary, the United States, or U.S. partners—more likely to initiate conflict**. Insecure adversaries may also take immediate militarized steps either to strengthen their defenses or to signal their own resolve to defend their homeland or sphere of influence. These steps could include making threats, **putting military forces on a higher level of alert, initiating a limited use of force**, or pursuing aggressive territorial expansion to preemptively secure militarily important areas."[192]

"Admitting all of the above, it must be conceded that in 1956 we are living dangerously – more dangerously than necessary, because **nobody has tried very hard to distinguish between a façade and an objective capability.** While deterrence is a psychological phenomenon, it is not true that one has it for all practical purposes, just because the enemy and others believe that he does. **Psychological nonobjective capabilities are extremely unstable**. They are subject to erosion by time and, equally important, to subtle tactics of the enemy or our own panic. **The enemy can investigate and teach himself what capabilities we really have. He can also, by means of crises and other tactics, teach others what he has learned about our objective capabilities**. One of the serious problems in **psychological deterrence** is that the learning is

---

[191] https://apnews.com/c1d775ab65a794f8a2a7ef1ec9aaa0bd

[192] O'Mahony, Angela, et al. *U.S. Presence and the Incidence of Conflict*. The RAND Corporation. 2018, p. 23; 25-26.

likely to be too convincing. These things are like a pendulum. If one has been successfully exaggerating his capabilities, removal of this façade is likely the result in disillusionment and a tremendous underestimation. This could be most serious. **It may lead to quick diplomatic victories by the other side or it may lead to a disastrous situation arising because of overconfidence and miscalculation**… This means that bargaining, even at courteous and ordinary **diplomatic levels** where these is no threat or even hint of violence, **will be affected by consideration of** what would happen if the bargaining broke down and violence or threats of violence came into the picture. It is important to realize that **one does not have to be putting SAC on alert and evacuating cities to have the capability for initiating war** or retaliating effectively after attack **to affect innocuous-looking negotiations.** Military power casts a very long shadow before it."[193]

[TOPIC – US military wargame preparations for domestic warfare]
"Marines raid water park in urban-assault training held in Hawaii for first time" **https://www.stripes.com/news/pacific/marines-raid-water-park-in-urban-assault-training-held-in-hawaii-for-first-time-1.566682 ; "**Air Force will bring urban training to Boise — and some residents are fighting back" **https://www.idahostatesman.com/news/local/military/article228882944.html ; "**Idaho residents file suit to stop Mountain Home from using their cities for close-air support training" **https://www.airforcetimes.com/news/your-air-force/2019/04/06/idaho-residents-file-suit-to-stop-mountain-home-from-using-their-cities-for-close-air-support-training/ ; "**To prepare for urban warfare, soldiers train for chemical attack, mass disaster response in Detroit" **https://www.armytimes.com/news/your-army/2018/08/29/to-prepare-for-urban-warfare-soldiers-train-for-chemical-attack-mass-disaster-response-in-detroit/**
"Target 'Yodaville': The town in the middle of the Arizona desert built by the U.S. Air Force to practise its bombing raids" https://www.dailymail.co.uk/news/article-2170984/Target-Yodaville-The-town-middle-Arizona-desert-built-U-S-Air-Force-practice-bombing-raids.html

From RAND's *Ready for Armageddon* "Urban Intelligence Preparation of the Battlefield":
"Population analysis should come to the analytic foreground when dealing with urban areas. It should include such components as demographic analysis, cultural intelligence, and media and international actor analysis."[194]
"[Pentagon training video released in 2014] 'Megacities' posits that despite the lessons learned from the ur-urban battle at Aachen, Germany, in 1944, and the city-busting in Hue, South Vietnam, in 1968, the U.S. military is fundamentally ill-equipped for future battles in Lagos or Dhaka. 'Even our counterinsurgency doctrine, honed in the cities of Iraq and the mountains of Afghanistan, is inadequate to address the sheer scale of population in the future urban reality,' the film notes, as if the results of two futile forever wars might possibly hold the keys to future success. 'We are facing environments that the masters of war never foresaw,' warns the narrator.

[193] Kahn, p. 446-447.
[194] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 34.

'We are facing a threat that requires us to redefine doctrine and the force in radically new and different ways.'"[195]

[TOPIC - description of US-led urban operations in Mosul in 2016]

Leon Trotsky wrote: "One must never forget that the barricade, though a material element in any insurrectionary situation, plays above all a moral role. Instead of functioning as fortresses do in a time of war – as physical obstacles – **barricades have served in every revolution simply as a way of halting the movement of troops, thus placing them in contact with the people**."[196]

[Re: barricades, insurgents, and police function as inroad to urban warfare, warfare against populations. +ADD more on barricades from chapter 7]

"Satellite images of Mosul have revealed how fighters from so-called Islamic State have constructed multiple barricades across key routes into the northern Iraqi city.

The imagery, released by US geopolitical intelligence company Stratfor and taken on 31 October, shows a defensive line built across the city's southern edge. The jihadists have also destroyed a number of buildings south of their positions around Mosul airport to enable them to observe advancing government forces, Stratfor says. The barricades constructed across key routes into the city have been made out of concrete blocks and other rubble, Stratfor's analysis says, possibly from the concrete walls of destroyed buildings. In other areas, the militants have stockpiled materials ready to block roads as the battle nears… In the southern district of Wadi Hajar, a number of roads have been blocked while earthen defences have also been constructed. Just north of the airport, a large number of obstacles have been placed in multiple roads. Nearly all of the buildings in the airport complex and the former military base to its west have been destroyed, Stratfor says... The jihadists' defensive measures will pose a "substantial tactical challenge to the converging forces", according to Stratfor's analysis. Iraqi troops will either have to adjust their course to avoid running into IS positions head-on, or accept the risks of crossing open terrain to reach the dug-in IS fighters, it says."[197]

"Progress was initially swift, with pro-government forces advancing from the north, south and east, seizing outlying towns and villages despite strong resistance. Iraqi special forces first entered Mosul on 1 November 2016. **But progress slowed as troops encountered fierce resistance from IS, including snipers, suicide bombers and shellfire**… But the west of the city presented a more difficult challenge. The densely-packed housing and narrow alleyways enabled a relatively **small number of militants to target advancing troops with snipers and suicide bombs**… Satellite images show extensive damage to Mosul's infrastructure, buildings and archaeological sites - **in particular to the airport and bridges**. Imagery released by US geopolitical intelligence company Stratfor in October 2016, showed how IS fighters **sabotaged much of the city's airport, with wide trenches carved into it and rubble placed along their lengths. The barriers were made out of concrete blocks and other rubble,** Stratfor's analysis said, possibly from the walls of destroyed buildings. Imagery also revealed how the jihadists constructed **multiple barricades across key routes into the city, including north of the airport. <u>Meanwhile,</u> coalition air strikes destroyed all bridges linking the east and west of the city across the Tigris river**, with the aim of limiting the jihadists' ability to resupply or

---

[195] https://theintercept.com/2016/10/13/pentagon-video-warns-of-unavoidable-dystopian-future-for-worlds-biggest-cities/

[196] Traugott, Mark. *The Insurgent Barricade*. The Regents of the University California. 2010, p. 178.

[197] Mosul satellite images reveal IS barricades 4 November 2016 https://www.bbc.com/news/world-middle-east-37870455

reinforce their positions in the east. In the centre of the city, **four of the five main bridges were put out of action in October and November by coalition air strikes**, with the aim of limiting the jihadists' ability to resupply or reinforce their positions in the east. The Old Bridge - **the only remaining route open to vehicles in the centre of the city - was then disabled in a US-led coalition air strike** at the end of December 2016… **A US air strike damaged the al-Hurriya Bridge at the eastern end in October 2016, but IS then set up a barrier on the western side**, shown below. In November 2016, **a US air strike damaged the Fourth Bridge**, but was later rendered impassable by further damage, shown below. Iraqi military engineers installed a floating bridge across the Tigris river in May, after recapturing eastern Mosul, reconnecting the two halves of the city to facilitate troop deployments ahead of the final assault to dislodge IS… the UN estimates rebuilding the city's basic infrastructure will cost more than $1bn. **Reinstating water, sewage and electricity services, as well as reopening schools and hospitals, would cost more** than twice initial estimates, the organisation said. In June 2017, the ancient Great Mosque of al-Nuri, where IS leader Abu Bakr al-Baghdadi demanded allegiance after declaring a "caliphate", was blown up by IS, according to Iraqi forces. IS claims the mosque was destroyed in a US air raid… Following the recapture of eastern Mosul in January, there was deep concern for thousands of people remaining in the west of the city, **with food supplies reported to be very low and clean drinking water in short supply**. The UN said in late January that **almost half of all the casualties in Mosul were civilians**. At least 2,463 have been killed and 1,661 injured across Nineveh province since October. UN human rights officials said in June that they had received credible **reports of hundreds of civilians being shot dead by IS militants as they attempted to flee** the fighting in western Mosul, with **reports of others being used as 'human shields'**. Dozens more have reportedly **died in Iraqi and US-led coalition air strikes**."[198]

; "The mission is now regarded as the single **largest urban battle since World War II**… Taking into account damage to multiple floors of buildings, **not seen via satellites**, the UN now estimates the real number of damaged buildings to be more than three times greater - about 32,000. Lise Grande, the **UN's humanitarian coordinator for Iraq**, says it will take years for affected areas to return to normal. **Reconstructing** the city and returning civilians to their homes will be "extremely challenging", she has warned, costing **an estimated $1bn** (£760m)… After almost nine months 9,519 buildings damaged (85% homes). In the final weeks of battle, more than 5,000 sites were destroyed. About **98% of these were residential buildings** - largely in the Old City. The iconic **Great Mosque of al-Nuri was also destroyed**. The UN's initial satellite analysis suggests **housing has been the most heavily hit**, with at least 8,500 residential buildings **severely damaged or completely destroyed, most of them in the Old City**… About 130km of roads have also been damaged overall… **Coalition air strikes also destroyed all bridges** linking the east and west of the city across the Tigris river, with the aim of limiting the jihadists' ability to resupply or reinforce their positions in the east. **The city's airport, railway station and hospital buildings are also in ruins.** Iraqi officials estimate that nearly 80% of Mosul's main **medical hub has been destroyed**… Satellite imagery suggests that more than 5,500 of the 16,000 residential buildings in the Old City - about one in three - have been severely damaged or completely destroyed. An estimated 490 homes were destroyed in the final weeks of the offensive. **The real figures, again, are likely to be higher**… [Al-Hadba Minaret two photographs June 20, 22, 2017 show minaret collapsed, telecom transmission tower next to minaret left standing]… Amnesty International has said **5,805 have been killed by air strikes**

[198] https://www.bbc.com/news/world-middle-east-37702442

alone… one million civilians have left the city - about half the pre-war population - since the beginning of the Mosul offensive last October, according to UN estimates… **It has been the largest managed evacuation in modern history**… More than 440,000 people are living in camps… Among those to make this move was Jumana Najim Abdullah, a 35-year-old **hairdresser**, who fled the fighting in the west to stay with family in the east. Jumana, a divorced mother, **was banned from practicing her trade under IS rule**, but managed to earn some money by cutting the hair of known and trusted clients within the safety of their homes. Now, with the militants gone, she has moved into a rented apartment and **started her own business**, Jumana Salon. '**I was the first person to open'**, she says. 'I felt very proud. **People warned me it could be dangerous and said I might face consequences**, but luckily I had no problems.' And, she says, **with her daughter now back in school, she intends to stay put** in the east of the city. **'Even though this is not my original home, I will stay here now**,' she says."[199]
"Overall, around **one-in-five U.S. adults (22%) say they either changed their residence due to the pandemic or know someone who did**, according to a new Pew Research Center survey… Among U.S. adults **who moved due to the pandemic, 28%** say the most important reason was **to reduce their risk of contracting the virus**, which has infected more than 2.8 million Americans of all ages. Another **23%** say it was because their **college campus closed**, and **20%** say they wanted to be **with family**. An additional 18% say the most important reason was financial – either **job loss (8%) or another money-related reason (10%).** Survey respondents who did not select one of these reasons gave a variety of other reasons for moving. One said, 'I am **traveling and am now blocked from returning home.'** Another wrote: 'Needed more space **to work from home**.' And a third said, '**Recalled to active duty for military's COVID response.**'"[200]

[TOPIC – transition to next section]

National Intelligence Council fake presidential diary entry from projected-2020 in the section titled "October Surprise": "We talk a lot about these problems at the G-14 summits and in fact have started to engage in joint scenario exercises, but doing anything about an impending storm cloud is still beyond us."[201]

When reading the major points of focus in the following JLASS-SP wargame scenarios based in the US, contextualize the scenarios within academic cybersecurity literature's understanding of the nature of governments and their respective cyberthreats. The literature states that within "**Cyber revolutions**:… Two of Kello's disruptive features of cyberspace lie at the heart of this reasoning on the part of **authoritarian states**: '**the expansion of nonphysical threats to national security, the growing ability of non-state actors to instigate diplomatic and military crises**.'"[202] [REWORD]

---

[199] https://www.bbc.co.uk/news/resources/idt-9d41ef6c-97c9-4953-ba43-284cc62ffdd0
[200] https://www.pewresearch.org/fact-tank/2020/07/06/about-a-fifth-of-u-s-adults-moved-due-to-covid-19-or-know-someone-who-did/#:~:text=About%20a%20fifth%20of%20U.S.,or%20know%20someone%20who%20did&text=Overall%2C%20around%20one%2Din%2D,new%20Pew%20Research%20Center%20survey.
[201] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 59.
[202] Steed, p. 38. / Lucas Kello *The Virtual Weapon and International Order, p. 4. (2017)*

+ADD review list of articles on website https://www.armyupress.army.mil/Online-Publications/New-Extended-Battlefield/

Hold in mind the significance of these points while approaching the following accounts of real wargames conducted by the US military Joint Special Program, after which follows an account of news reports which show that the precise events of the wargames have transpired despite wargaming preparations. [EXPAND scope]

Horseshoes and Hand Grenades

I do remember - and I do know, because I felt the same way on our side – that it is sometimes quite difficult to tell the difference between an exercise and the beginning – the raising of indicators that we watch all the time every day, every hour… They were moving a hell of a lot of stuff in position and everybody knew it was just a maneuver and it was an annual exercise, but I got quite alarmed, because I kept saying, 'What if it isn't? We've lost about five days of time.' So the difference between a realistic exercise or maneuver and what could be preparations for an attack, that line is sometimes quite blurred.
Former Secretary of Defense Caspar Weinberger, *Able Archer 83*

[TOPIC – Real world events are exact recreations of wargames scenarioed years earlier. This section details a prolific list of recent examples.]

"**The cornerstone of any deception operation is the deception story. The deception story is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception.** It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe to be the true situation, then decide and act on that basis. In other words, the deception story parallels what the deception would want the opponent's intelligence estimate to say about your own commander's intentions and your own unit's actions. The deception story identifies those friendly actions, both real and simulated, that when observed by the deception target will lead it to develop the desired perception. Deception story development is both an analytic and creative process that involves a variety of information on enemy data acquisition and processing. An exact understanding of the perceptions and observables required for the deception provides a concrete basis for crafting the deception story. The deception story weaves these elements together into a coherent depiction of the situation the target will reconstruct from the information provided. Ideally, the deception planner wants the deception story to be the exact mental picture of the target forms as the deception unfolds. **The deception story should read like the adversary's own intelligence estimate**. The deception story is, in effect, the equivalent of a completed puzzle. As such**, it serves as a means of checking the logic and consistency of the internal elements of the deception. This allows the deception planner to identify desired perceptions, observables, and executions that may need refinement, and to add supporting observables as needed to strengthen certain elements of the deception story or diminish the impact of troublesome competing observables.**"[203] [REPEATED from Spectacular Security State]

[203] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-5

"These fears are reflected in the hyperbolic "Megacities" video [released by Pentagon in 2014]. As the film unfolds, we're bombarded with an apocalyptic list of ills endemic to this new urban environment: "criminal networks," "substandard infrastructure," "religious and ethnic tensions," "impoverishment, slums," "open landfills, over-burdened sewers," and a "growing mass of unemployed." The list, as long as it is grim, accompanies photos of garbage-choked streets, masked rock throwers, and riot cops battling protesters in the developing world. "Growth will magnify the increasing separation between rich and poor," the narrator warns as the scene shifts to New York City. Looking down from a high vantage point on Third Avenue… "Megacities" posits that despite the lessons learned from the ur-urban battle at Aachen, Germany, in 1944, and the city-busting in Hue, South Vietnam, in 1968, the U.S. military is fundamentally ill-equipped for future battles"[204]

Global Trends: Paradox of Progress: "Imagining a surprise news headline in 2018 . . . 'Robin Hoodhacker' Paralyzes Online Commerce, Upends Markets Nov. 19, 2018 – New York Online commerce ground to a halt a week before the Christmas shopping season started in the United States, Canada, and Europe after numerous attacks by the persona 'Robin Hoodhacker.' The attacks created chaos by altering online payment accounts by as much as $100,000 in credit or debts—sparking a frenzy of online shopping that has forced retailers to shut down all digital transactions. The disruption sent global financial markets into a free fall before trading was suspended in most exchanges due to uncertainty about how long and widely the hacking would persist."[205] **Robinhood Reportedly Hit By SEC Fraud Probe 9/2/2020** [high-frequency "millennial" machine/app trading] "According to a Forbes investigation earlier this month, despite its proclamations about democratizing finance, Robinhood's entire business has been built since its inception on selling its customers' orders—known as "payment for order flow"—to Wall Street's most notorious sharks"[206]

Documents obtained by The Intercept via the Freedom of Information Act reveal that a Pentagon war game, called the 2018 Joint Land, Air and Sea Strategic Special Program, or JLASS, offered **a scenario in which members of Generation Z, driven by malaise and discontent, launch a "Zbellion" in America in the mid-2020s**. The Zbellion plot was a small part of JLASS 2018, which also featured scenarios involving Islamist militants in Africa, anti-capitalist extremists, and ISIS successors. The war game was conducted by students and faculty from the U.S. military's war colleges, the training grounds for prospective generals and admirals. While it is explicitly not a national intelligence estimate, the war game, which covers the future through early 2028, is 'intended to reflect a plausible depiction of major trends and influences in the world regions,' according to the more than 200 pages of documents. : "Both the September 11 terrorist attacks and the Great Recession greatly influenced the attitudes of this generation in the United states, and resulted in a feeling of unsettlement and insecurity among Gen Z. Although Millennials experienced these events during their coming of age, Gen Z lived through them as part of their childhood, affecting their realism and world view … many found themselves stuck with excessive college debt when they discovered employment options did not meet their

[204] https://theintercept.com/2016/10/13/pentagon-video-warns-of-unavoidable-dystopian-future-for-worlds-biggest-cities/
[205] Global Trends: Paradox of Progress. P. 12
[206] https://www.forbes.com/sites/sergeiklebnikov/2020/09/02/robinhood-reportedly-hit-by-sec-fraud-probe-possible-fine-of-over-10-million/#3e6bcb53619e

expectations. Gen Z are often described as seeking independence and opportunity but are also among the least likely to believe there is such a thing as the 'American Dream,' and that the 'system is rigged' against them. Frequently seeing themselves as agents for social change, they crave fulfillment and excitement in their job to help 'move the world forward.' Despite the technological proficiency they possess, Gen Z actually prefer person-to-person contact as opposed to online interaction. They describe themselves as being involved in their virtual and physical communities, and as having rejected excessive consumerism. In early 2025, a cadre of these disaffected Zoomers launch a protest movement. Beginning in 'parks, rallies, protests, and coffee shops' — first in Seattle; then New York City; Washington, D.C.; Los Angeles; Las Vegas; and Austin — a group known as Zbellion begins a 'global cyber campaign to expose injustice and corruption and to support causes it deem[s] beneficial.' During face-to-face recruitment, would-be members of Zbellion are given instructions for going to sites on the dark web that allow them to access sophisticated malware to siphon funds from corporations, financial institutions, and nonprofits that support 'the establishment.' The gains are then converted to Bitcoin and distributed to 'worthy recipients' including fellow Zbellion members who claim financial need. Zbellion leadership, says the scenario, assures its members that their Robin Hood-esque wealth redistribution is not only untraceable by law enforcement but 'ultimately justifiable,' as targets are selected based on 'secure polling' of 'network delegates.' Although its origins are American, by the latter 2020s, Zbellion activities are also occurring across Europe and cities throughout Africa, Asia, and the Middle East, including Nairobi, Kenya; Hanoi, Vietnam; and Amman, Jordan. In the world of JLASS 2018, Gen Z's most militant members have essentially taken to privately taxing large corporations and other institutions to combat income inequality or, as the war gamers put it, using the 'cyber world to spread a call for anarchy.'"[207]

[REMOVE text not used from below paragraph – keep in other document]

2020s "a collection of U.S. military documents from 2016 obtained by *TomDispatch* via the Freedom of Information Act. Those files detail a plethora of shocking acts of terrorism across the United States including mass poisonings, the use of improvised explosive devices (IEDs), and that "People's Armed Liberation (PAL) attack on U.S. Central Command (USCENTCOM) headquarters in Tampa, Florida, [by] a drone-launched missile." That's right! A drone-launched missile attack! On CENTCOM's Florida headquarters! By a terrorist group known as PAL! Wondering how you missed the resulting 24/7 media bonanza, the screaming front page headlines in the *New York Times*, the hysterics on *Fox & Friends*, the president's hurricane of tweets? Well, there's a simple explanation. That attack doesn't actually happen until May 2020. Or so says the summary of the 33rd annual Joint Land, Air, and Sea Strategic Special Program (JLASS-SP), an elaborate war game carried out in 2016 by students and faculty from the U.S. military's war colleges, the training grounds for its future generals and admirals. **PALing Around with Terrorists** The 2016 edition of JLASS-SP was played out remotely for weeks before culminating in a five-day on-site exercise at the Air Force Wargaming Institute at Maxwell Air Force Base in Alabama. It involved 148 students from the Air Force's Air War College, the Army War College, the Marine Corps War College, the Naval War College, the Eisenhower School for National Security and Resource Strategy, the National War College, and the National Defense University's Information Resources Management College. Those up-and-coming officers -- some of whom will likely play significant roles in running America's actual

[207] https://theintercept.com/2020/06/05/pentagon-war-game-gen-z/

wars in the 2020s -- confronted a future in which, as the script for the war game put it, “lingering jealousy and distrust of American power and national interests have made it politically and culturally difficult for the United States to act unilaterally.” Here’s the scene as set in JLASS-SP: while the U.S. is still economically and militarily powerful into the next decade, anxieties abound about increasing constraints on the country’s ability to control, dictate, and dominate world affairs. “Even in the military realm... advances by others in science and technology, expanded adoption of irregular warfare tactics by both state and non-state actors, proliferation of nuclear weapons and long-range precision weapons, and growing use of cyber warfare attacks have increasingly constricted U.S. freedom of action,” reads the war game’s summary.”While the materials used are “not intended to be an actual prediction of events,” they are explicitly meant “to reflect a plausible depiction of major trends and influences in the world regions.” Indeed, what’s striking about the exercise is how -- though scripted before the election of Donald Trump -- it anticipated many of the fears articulated in the president’s December 2017 National Security Strategy. That document, for instance, bemoans the potential dangers not only of regional powers like Russia, China, Iran, and North Korea, but also of “transnational threats from jihadist terrorists and transnational criminal organizations,” undocumented immigrants, “drug traffickers, and criminal cartels [which] exploit porous borders and threaten U.S. security and public safety.” “The JLASS-SP scenario also prefigured themes from that 2018 DOJ/DHS report supporting the travel ban in the way it stoked fears of, above all, a major “foreign-born” -- especially Muslim -- terror threat in the United States. A 2017 Government Accountability Office report would, however, conclude that, of “the 85 violent extremist incidents that resulted in death since September 12, 2001, far right-wing violent extremist groups were responsible for 62 (73 percent) while radical Islamist violent extremists were responsible for 23 (27 percent). Two years after the war game was conducted, in a time of almost metronomic domestic mass killings, President Trump continues to spotlight the supposedly singular danger posed by “inadequately vetted people” in the U.S.,”...”An examination of the threats from international and domestic terror groups, as imagined in JLASS-SP, offers unique clues to the Pentagon’s fears for the future. “Increasingly,” reads the war game’s summary, “transnational organizations, businesses, non-governmental organizations, and violent extremist organizations challenge the traditional notions of boundaries and sovereignty.” “That drone-launching terror group, PAL, for instance, is neither Islamist nor a right-wing terror group, but an organization supposedly formed in 2017 in hopes of defeating “globalism and capitalism throughout the world by rallying the proletariat to orchestrate the overthrow of capitalist governments and global conglomerates.” Its ideology, an amalgam of increasingly stale leftist social movements, belies its progressive ranks, a rainbow coalition consisting of “most of the globe’s ethnicities and cultures,” all of whom seem to be cyber-sophisticates skilled in fundraising, recruiting, as well as marketing their particular brand of radicalism. As of 2020, the audacious drone strike on CENTCOM’s headquarters was PAL’s only terror attack in the tangible world. “Increasingly,” reads the war game’s summary, “transnational organizations, businesses, non-governmental organizations, and violent extremist organizations challenge the traditional notions of boundaries and sovereignty.” “That drone-launching terror group, PAL, for instance, is neither Islamist nor a right-wing terror group, but an organization supposedly formed in 2017 in hopes of defeating “globalism and capitalism throughout the world by rallying the proletariat to orchestrate the overthrow of capitalist governments and global conglomerates.” Its ideology, an amalgam of increasingly stale leftist social movements, belies its progressive ranks, a rainbow coalition consisting of “most of the globe’s ethnicities and cultures,” all of whom seem to be cyber-sophisticates skilled in

fundraising, recruiting, as well as marketing their particular brand of radicalism. As of 2020, the audacious drone strike on CENTCOM's headquarters was PAL's only terror attack in the tangible world. The rest of its actions have taken place in the digital realm, where the group is known for launching cyber-assaults and siphoning off "funds from large global corporations, banks, and capitalist governments around the world."..."include the fictional versions of the real Irish National Liberation Army and the Revolutionary Armed Forces of Colombia (FARC). There's also the Environmentalists Against Capitalists Organization, or EACO, "a lethal environmental anti-capitalist terrorist group with global connections." Formed in 2010 (though not in our actual world), EACO, according to the war gamers, evolved into an increasingly violent organization in the 2020s, carrying out not just cyberattacks on corporations but also a full-scale bombing campaign "targeting executive board meetings of large corporations, particularly in industries such as oil, coal, natural gas, and logging." The group even took to planting IEDs on logging roads and employing tainted food as a weapon. By 2025, EACO was implicated in more than 400 criminal acts in the U.S. resulting in 126 deaths and $862 million in damages. Then there's Anonymous. In the Pentagon's fictional war-game, this real-world hacktivist group is characterized as a "loose organization of malicious black-hat hackers" that employs its digital prowess to "distribute bomb-making instructions, and conduct targeting for options other than planes, trains, and automobiles." In the past created by the military's imagineers, Anonymous was declared a terrorist organization after it conducted an August 2015 digital attack on Louisiana's power grid with something akin to the Stuxnet worm that damaged nuclear centrifuges in Iran. That cyber-assault was meant to protest the state's restrictions on online gambling -- an affront, according to the fictional Anonymous, to Internet freedom. (In the real world, Louisiana lawmakers actually just deep-sixed online gambling without an apparent terrorist response.) Taking down that power grid "resulted in the death of 15 elderly patients trapped in a facility denied air conditioning as a result of the power outage." Also included among domestic terror groups is Mara Salvatrucha 13 or MS-13, the Los Angeles street gang, born of the American-fueled Central American civil wars of the 1980s, that was transplanted to El Salvador and has since returned to the United States." "… in the Pentagon's future fantasy there is "substantial evidence... that terrorists from the Middle East and North Africa transit the Mexican-U.S. border." Worse yet, radical Islamists even "camouflage themselves as Hispanics" to cross the border. The military's fantasists point to "a flood of name changes from Arabic to Hispanic and the reported linking of drug cartels along the Texas border with Middle East and North Africa terrorism." … ""Popular opinion in the United States is beginning to believe the 'Narco-corruption' is affecting the 'rule of law' north of the border," according to their scenario, with the cartels spending $20 billion in 2022 alone to buy off U.S. officials or get candidates of their choice elected. That same year, allegations of election tampering in mayoral races across the American South come to light and the number of corruption convictions of U.S. Border Patrol agents and law enforcement officials skyrockets."..."reports of the defeat of the Islamic State in Iraq and Syria, like the much-hyped defeat of its predecessor, al-Qaeda in Iraq, turn out to be premature. In the 2020s, the re-re-branded group, now known as the Global Islamic Caliphate, or GIC, draws "support from Sunni-majority regions in Syria and Iraq; refugee camps in Lebanon, Jordan, and Turkey; and internally displaced persons in Syria and Iraq," while continuing to launch attacks in the region. Meanwhile, al-Qaeda in the Islamic Maghreb (AQIM) has grown in reach, size, and might. By 2021, the group has 38,000 members spread across Algeria, Mali, Mauritania, and Niger with bases reportedly located in Western Sahara. On May 23, 2023, AQIM carries out the most lethal terror attack in the U.S. since 9/11, detonating

massive truck-bombs at both the New York and New Jersey ends of the Lincoln Tunnel, killing 435 people and injuring another 618. The bombing prompts President McGraw -- you remember him, Karl Maxwell McGraw, the independent Arizona senator who rode his populist "America on the Move" campaign to victory in the 2020 election -- to invade Mauritania and become mired in yet another American forever war that shows every indication of grinding on into the 2030s, if not beyond."..."“States are the principal actors on the global stage, but non-state actors also threaten the security environment with increasingly sophisticated capabilities," reads an unclassified synopsis of the Pentagon's 2018 National Defense Strategy. "Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption. In the fictional future of the Pentagon's JLASS-SP 2016, this menace only expands to include various hybrid threats and new homegrown groups with increasing capabilities for death and destruction."..."While it may be "the policy of the United States to protect its citizens from terrorist attacks," as President Trump's 2017 executive order declares, the Pentagon envisions a future in which such policies are increasingly ineffective. In their dystopian war-game future, more than two decades of fighting "them over there so we do not have to face them in the United States of America" (as former President George W. Bush put it in 2007) proves unequivocally futile. In this sense, the Pentagon's fantasies bear an eerie resemblance to the actual present. In the dystopian scenario used by the Pentagon to train its future leaders, today's forever wars have proven ineffective and future threats are to be met with new, similarly ineffective, forever wars.

2023 fire season: "as fires raged in the western United States, UPAIGO [PAL's other organization devoted to even more rapidly eroding 'confidence in governmental and institutional bodies by staging events that demonstrate the 'impotency' of the establishment.' That splinter group, United Patriots Against International Government (UPAIGO)] established relief efforts designed to compete with the U.S. government's response, in order to 'undermine confidence in government agencies.'"[208]

'PAL' terrorist organization & CENTCOMM attacks, possible real-world explanation: "Some [**nuclear command and control** improvements], like **permissive action links, PALs**, which are **coded locks that block detonation of a weapon without inserting the PIN code**, and were pressed by far-seeing congressional advocates, these improvements may have helped forestall disaster. This brings me to my second major point. We must be willing to invest the requisite funds to keep our technology up to date. But in the nuclear command and control business, hardware is trumped by software, and software is trumped by wetware. Hardware refers to the technologies like the PALs I just mentioned. Software refers to the rules and procedures that govern how the hardware is used; for instance, the code management system that determines **who has the PAL codes and who is authorized to release them. Wetware refers to the human element**, the reliability of people involved in enforcing the rules, and the civil-military relations that form the political context in which the software and hardware operate."[209]

drone-launching terror group, PAL, for instance, is neither Islamist nor a right-wing terror group, but an organization supposedly formed in 2017 in hopes of defeating "globalism and capitalism

[208] Turse, Nick. "Tomgram: Nick Turse, Tomorrow's Terror Today". *Tom Dispatch.* 29 May 2018.
[209] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 9.

throughout the world by rallying the proletariat to orchestrate the overthrow of capitalist governments and global conglomeratesdrone strike on CENTCOM's headquarters was PAL's only terror attack in the tangible world. https://en.wikipedia.org/wiki/Lloyd_Austin 2021 Sec. of Defense nominee former commander of CENTCOM, board member of Raytheon, commander of Airborne division at Fort Bragg (Special Forces headquarters), graduate of Army War College, former top commander in Middle East (in 2015). On Austin's ISIS war record: "A **$500m effort to train Syrian forces against the Islamic State has resulted in only a handful of fighters** actively battling the jihadi army, the top military commander overseeing the war has testified. **'We're talking four or five,' General Lloyd Austin, commander of US Central Command**, told a dissatisfied Senate armed services committee on Wednesday. The training initiative is Barack Obama's linchpin for retaking Syrian territory from Isis. The Pentagon anticipated in late 2014 that it would have trained 5,000 anti-Isis Syrian rebels by now. 'The program is much smaller than we hoped,' conceded the Pentagon's policy chief, Christine Wormuth, saying there were between 100 and 120 fighters currently being trained. **Wormuth said they were 'getting terrific training'**. Both Wormuth and **Austin defended US strategy against Isis** in the face of bipartisan skepticism from the senators. Senator Claire McCaskill, a Democrat from Missouri, mocked the Syrian training program, expressing incredulity **that the Defense Department would seek another $600m to fund fighters she said the US was counting 'on our fingers and toes'**… Former intelligence officials have told the Guardian the command climate inside Central Command is 'toxic'. They have expressed bewilderment that Austin has not addressed it forcefully."[210]

Guard units defending Capitol warned of IED threat: report https://thehill.com/policy/national-security/534193-guard-units-defending-capitol-warned-if-ied-threat-report

Re: News stories about ISIS in North Africa https://nypost.com/2014/10/13/isis-cancer-spreading-to-north-africa/ & increasing media push for electric energy that would require minerals from West Africa. Abandonment of OPEC relations https://www.msn.com/en-us/money/markets/irans-oil-minister-warns-that-opec-collapse-is-likely/ar-AAAQAmu?ocid=spartanntp

Re: Reports Trump does not listen to intelligence officials; Open letter plea to Biden from former CIA officers https://www.latimes.com/nation/la-na-pol-trump-intelligence-chiefs-20190203-story.html ; "A Letter to President-elect Biden on Restoring Relations with the Intelligence Community" https://www.justsecurity.org/73287/a-letter-to-president-elect-biden-on-restoring-relations-with-the-intelligence-community/

Re: Not due to hacking yet - California PG&E shut down due to wildfires and nursing home stories in news [3 articles printed highlighted]

- Re: Turkey bombing Kurds and resurgence of ISIS [printed?] https://www.msn.com/en-us/news/world/isis-eyes-breakout-opportunity-as-turkish-forces-batter-kurds/ar-AAIX2AA?ocid=spartanntp ; https://www.msn.com/en-us/news/world/defense-dept-

[210] Ackerman, Spencer. "US has trained only 'four or five' Syrian fighters against Isis, top general testifies". *The Guardian*. 16 September 2015.

watchdog-says-turkish-incursion-and-us-drawdown-helped-isis/ar-BBX12Jq?ocid=spartanntp

Re: IRA Irish Liberation violence 10/10/2019 John Bruton https://www.pbs.org/wnet/amanpour-and-company/video/nancy-mceldowney-on-complete-chaos-in-northern-syria-2/

Re: Border agent corruption and convictions 1 https://www.msn.com/en-us/news/us/asylum-officers-rebel-against-trump-policies-they-say-are-immoral-and-illegal/ar-BBWTW3i?ocid=spartanntp ; 2 https://www.msn.com/en-us/news/us/migrant-kids-in-arizona-report-sex-assault-retaliation-from-us-border-agents/ar-AAE5VK9?ocid=spartanntp ; 3 https://www.msn.com/en-us/news/politics/aoc-to-dhs-chief-border-agents-shared-images-of-my-violent-rape-in-secret-facebook-group/ar-AAEwI4o?ocid=spartanntp ; https://www.msn.com/en-us/news/us/lawsuit-us-border-officers-questioned-journalists-at-length/ar-BBX3SL7?ocid=spartanntp ; https://www.msn.com/en-us/news/us/memo-reveals-improper-medical-care-by-ice-led-to-deaths-surgery-for-childs-partial-forehead-removal/ar-AAK4Uww?ocid=spartanntp ; ACLU sues Customs and Border Protection Tactical Terrorism Response Teams https://www.nbcnewyork.com/news/national-international/aclu-sues-cbp-teams-detaining-travelers/2244861/ ; https://www.theatlantic.com/family/archive/2019/12/sick-migrant-children-are-at-the-whims-of-us-border-guards/603901/ ; https://www.usatoday.com/in-depth/news/nation/2019/12/19/ice-asylum-under-trump-exclusive-look-us-immigration-detention/4381404002/

Re: MS 13 in Maryland and HLN/CNN story of "Joanna" threatened by MS13 https://www.snopes.com/news/2018/02/11/what-is-ms-13/ ; https://www.cnn.com/videos/tv/2018/09/21/lead-lisa-ling-live-preview-this-is-life-jake-tapper.cnn ; https://www.fresnobee.com/news/local/crime/article219451335.html

Re: Cyber attacks into electric grids – not yet attributed to Anonymous,

Anonymous, AntiFA declared terrorist organization "As of 2019, the FBI has designated QAnon as a "domestic terror threat" because of its potential to incite extremist violence… What started out as a primarily U.S. based conspiracy theory, has expanded to gain international recognition. Currently, QAnon followers seem to be propagating misinformation pertaining to both COVID-19 (coronavirus disease 2019) and the George Floyd protests, all while membership across various digital platforms, such as Facebook, seem to be on the rise."[211] ; "Department of Homeland Security intelligence officials are targeting activists it considers antifa and attempting to tie them to a foreign power…'They targeted Americans like they're Al Qaeda,' a former senior DHS intelligence officer with knowledge of the operations told *The Nation*." [212]

[211] Vanderzielfultz, Victoria. "Conspiracy Theory Trends: Qanon". *On the Homefront: The HSDL Blog*. Homeland Security Digital Library. 4 August 2020.
[212] https://www.thenation.com/article/society/dhs-antifa-syria/

US Military bases with tainted water likely to rise https://www.msn.com/en-us/news/us/pentagon-warns-that-number-of-military-bases-with-contaminated-water-likely-to-rise/ar-BBX4J45?ocid=spartanntp

'Caravan' from Central America / Islamists disguised as Hispanics [printed article Turkish political refugees crossing on Mexico border] ; https://www.msn.com/en-us/news/us/lawsuit-us-border-officers-questioned-journalists-at-length/ar-BBX3SL7?ocid=spartanntp

FROM NIC Global Trends 2025:

[repeated from essay] The National Intelligence Council predicted in 2009 that the world would make a "rapid" transition away from fossil fuels between 2020 to 2025 due to negative effects on the climate. This will remain unsolved despite the abandonment of fossil fuels. The report illustrates that this change would devastate oil producing nations, and could reduce economic growth for low-efficiency nations like China. It also claims climate change "could lead to increasingly heated interstate recriminations and possibly to low-level armed conflicts."[213] "'We are on the verge of a massive collapse': Ex-Energy Secretary Perry says COVID-19 will ravage oil industry" by William Cummings *USA Today* 1 April 2020.https://www.usatoday.com/story/news/politics/2020/04/01/rick-perry-coronavirus-oil-industry-near-collapse/5102155002/

Failed states of "Latins" Bolivian President Morales resigns after street protests (plus blackouts in Bolivia) https://www.sfgate.com/world/article/Power-void-in-Bolivia-after-president-resigns-14826659.php

Irregular warfare and traditional violence https://www.msn.com/en-us/news/us/fbi-no-link-found-between-cyberattack-and-navy-base-attack/ar-BBXZXvI?ocid=spartanntp FBI: No link found between cyberattack and Navy base attack, AP, 12/10/19

NIC *Global Trends: Paradox of Progress*: "Imagining a surprise news headline in 2018 . . . "Robin Hoodhacker" Paralyzes Online Commerce, Upends Markets Nov. 19, 2018 – New York Online commerce ground to a halt a week before the Christmas shopping season started in the United States, Canada, and Europe after numerous attacks by the persona "Robin Hoodhacker." The attacks created chaos by altering online payment accounts by as much as $100,000 in credit or debts—sparking a frenzy of online shopping that has forced retailers to shut down all digital transactions. The disruption sent global financial markets into a free fall before trading was suspended in most exchanges due to uncertainty about how long and widely the hacking would persist."[214]

NIC *Global Trends: Paradox of Progress*: "Imagining a surprise news headline in 2019 . . . China Buys Uninhabited Fijian Island To Build Military Base February 3, 2019 – Beijing A

[213] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 66
[214] https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf p. 12

Chinese development firm—with links to the Chinese Government and People's Liberation Army— today announced that it recently purchased the uninhabited Cobia Island from the Government of Fiji for $850 million. Western security analysts assess that China plans to use the island to build a permanent military base in the South Pacific, 3,150 miles southwest of Hawaii."[215]

NIC *Global Trends: Paradox of Progress*: "Imagining a surprise news headline in 2019 . . . Mexico Outlaws Private Drones After Latest Assassination Attempt May 13, 2019 – Mexico City The Mexican Government today announced it was a crime for private citizens to own drones after the fifth "drone-bomb" assassination attempt by drug cartels against senior government officials in less than three months, the latest targeting the new Minister of Interior."[216]

Table of scenarios and corresponding real-world news reports

Scenario	**Org. & Date**	**Outlet & Date**	**News Report**
The water treatment facility led to contamination of the base's water supply causing infection among nearly half the base's population. The US CAOC was non-mission capable for 96 hours at the end of the attack. The United States has not been able to attribute these actions and no organization has claimed responsibility	JLASS-SP 2018	*Military.com* 11/21/2019	Pentagon Warns that Number of Military Bases with Contaminated Water Likely to Rise
EACO terrorist group uses cyberattacks and tainted food as a weapon	JLASS-SP 2016	*BBC* 2/9/2021	Hacker tries to poison water supply of Florida city
EACO terrorist group conducts full-scale bombing of executive board meetings and even took to planting IEDs on logging roads	JLASS-SP 2016	*NBC* 1/7/2021 ; *Associated Press* 1/11/2021 ; *FOX 7 Austin* 2/23/2021 ; Wisc News 3/1/2021 *ABC* 3/15/2021 ; *WMI Central* 3/26/2021	Improvised explosive device found at Capitol ; Discovery of pipe bombs in DC obscured by riot at Capitol; Multiple IEDs discovered during arrest of Williamson County man ; Beaver Dam man placed on $50,000 cash bond for possession of pipe bomb, police confirmed that it was an IED or improvised explosive device;

[215] https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf p. 36
[216] https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf p. 43

			FBI report finds Nashville bomber wanted to kill himself, not motivated by terrorism, bomber authorities say set off an IED ; Explosive devices found in trailer in Vernon, deputies allegedly found more than one improvised explosive device (IED)
Al-Qaeda in the Islamic Maghreb (AQIM) has grown in reach, size, and might. By 2021, the group has 38,000 members spread across Algeria, Mali, Mauritania, and Niger with bases reportedly located in Western Sahara. On May 23, 2023, AQIM carries out the most lethal terror attack in the U.S. since 9/11	JLASS-SP 2016	*Jerusalem Center for Public Affairs* 3/1/2021 ; *Newsweek* 3/17/2021 ; *Middle East North Africa Financial Network* 3/18/2021 *Nigerian Tribune* 3/21/2021 ; *The New York Times* 3/22/2021 ; *Middle East Media Research Institute* 3/24/2021	Africa Is a Jihadist Playground for the Resurgent Islamic State and al-Qaeda ; When will the World Respond to Jihadi Violence in Africa? ; Stunning Classified Memo Details How U.S. Commandos Are Getting Beaten By Terrorists in Africa ; ISIS, Al-Qaeda Planning To Penetrate Southern Nigeria, US Warns ; 137 People Killed in Niger in Series of Attacks on Villages Along Mali Border ; Following Lull, Islamic State West Africa Province (ISWAP) Claims Second 2021 Attack In Chad
Anonymous was declared a terrorist organization in August 2015	JLASS-SP 2016	*The Hill* 8/1/2019	FBI memo warns QAnon poses potential terror threat: report
In 2023, as fires raged in the western United States, UPAIGO [PAL's other organization] devoted to even more rapidly eroding 'confidence in governmental and institutional bodies by staging events that demonstrate the 'impotency' of the establishment	JLASS-SP 2016	*Axios.com* 12/26/2020	More than 57,000 U.S. wildfires scorched 10.3 million acres in 2020
The number of corruption convictions of U.S. Border Patrol agents and law enforcement officials skyrockets	JLASS-SP 2016	*NBC* 12/18/2019 ; *The Washington Post* 7/10/2019	ACLU Sues CBP Over 'Highly Secretive' Teams Detaining Travelers ; Teen migrant claims Border Patrol agent sexually assaulted her, sparking federal investigation

Reports of the defeat of the Islamic State in Iraq and Syria, like the much-hyped defeat of its predecessor, al-Qaeda in Iraq, turn out to be premature. In the 2020s, the re-re-branded group, draws from refugee camps in Lebanon, Jordan, and Turkey and internally displaced persons in Syria and Iraq, while continuing to launch attacks in the region	JLASS-SP 2016	*USA Today* 8/28/2020 ; *Terrorism Research Initiative* 8/2020	ISIS did not simply disappear and now with instability in the Middle East from the coronavirus, the Islamic State is poised for a threatening rise ; ISIS Resurgence in Al Hawl Camp and Human Smuggling Enterprises in Syria: Crime and Terror Convergence?
Drug trafficking organizations, sustained in part by increased local drug consumption, transnational criminal cartels, and local crime rings and gangs, will continue to undermine public security. These factors, and persistent weaknesses in the rule of law, will mean that **a few small countries, especially in Central America and the Caribbean, will verge on becoming failed states.**	NIC 2008	*SF Gate* 11/11/2019 ; *The Washington Post* 3/18/2021 ; *NPR* 3/18/2021 *Associated Press* 3/22/2021 *Associated Press* 3/24/2021 ; *Al-Jazeera* 3/24/2021 ; *Al-Jazeera* 3/25/2021	Power void in Bolivia after president resigns, heads to Mexico ; The Bolivian government is on a lawless course. Its democracy must be preserved ; With Honduras' Narco Allegations, Pressure Rises To Sanction Its Leader ; Mexico worried by killings of politicians ; Haiti court orders release of those accused in alleged coup ; ICRC found that violence, killings and disappearances are on the rise in Colombia in a worrying trend ; Annulment of former President Lula’s corruption convictions threw Brazil into unprecedented political chaos.
The world would make a “rapid” transition away from fossil fuels between 2020 to 2025	NIC 2008	*USA Today* 4/1/2020 ; *CNN* 1/28/2021 ; *Republicworld.com* 1/4/2021 ; *CNN* 2/3/2021	‘We are on the verge of a massive collapse’: Ex-Energy Secretary Perry says COVID-19 will ravage oil industry ; GM plans to sell only emission-free vehicles by 2035 ; Massachusetts Joins California In Making Electric Cars Mandatory By 2035 ; Big oil companies are facing the moment of truth. The stakes couldn't be higher
Failure to create a vaccine against a pandemic disease in which “tens to hundreds of millions of Americans within	NIC 2008	*Voice of America* 1/3/2021 ; *Kaiser Family Foundation*	US Passes 350,000 COVID-19 Deaths ; Biden Terms Vaccine Rollout ‘A Dismal Failure’ as He

the US Homeland would become ill and deaths would mount into the tens of millions.		1/15/2021	Unveils Pandemic Response Plan
(con't) Outside the US, critical infrastructure degradation and economic loss on a global scale would result as approximately a third of the worldwide population became ill and hundreds of millions died	NIC 2008	*Associated Press* 1/15/2021 ; *United Nations* 5/13/2020 ; *The Wall Street Journal* 1/5/2021	'This is not a game': Global virus death toll hits 2 million ; COVID-19 to slash global economic output by $8.5 trillion over next two years ; Covid-19 Aftermath Could Spell a 'Lost Decade' for Global Economy, World Bank Says
Terrorists from the Middle East and North Africa transit the Mexican-U.S. border. Radical Islamists even "camouflage themselves as Hispanics" to cross the border. A flood of name changes from Arabic to Hispanic and the reported linking of drug cartels along the Texas border with Middle East and North Africa terrorism	JLASS-SP 2016	*Vox* 11/2/2018	The caravan "invasion" and America's epistemic crisis: the far right's xenophobic fantasies now involve the actual US military
Imagining a surprise news headline in 2018 . . . 'Robin Hoodhacker' Paralyzes Online Commerce, Upends Markets Nov. 19, 2018 – New York Online commerce ground to a halt a week before the Christmas shopping season started in the United States, Canada, and Europe after numerous attacks by the persona 'Robin Hoodhacker.' The attacks created chaos by altering online payment accounts by as much as $100,000 in credit or debts—sparking a frenzy of online shopping that has forced retailers to shut down all digital transactions. The disruption sent global financial markets into a free fall before trading was suspended in most exchanges	NIC 2017	*Forbes* 9/2/2020 ; *Bloomberg Wealth* 10/30/2020 *The Wall Street Journal* 1/29/2021 ; *The Wall Street Journal* 1/29/2021	Robinhood Reportedly Hit By SEC Fraud Probe, Possible Fine Of Over $10 Million: high-frequency "millennial" machine/app trading ; Dark Web Hackers Say They Hold Keys to 10,000 Robinhood Accounts ; GameStop, AMC Close Week With Surge as Broader Market Falls, Popular online brokerage Robinhood Markets said it would reinstate some trading ; Starbucks Added to List of Restricted Stocks on Robinhood
That drone-launching terror group, PAL… As of 2020, the audacious drone strike on	JLASS-SP 2016	*Joint Forces Staff College* 1/14/2021 ;	USCENTCOM Commander visits JFSC ;

CENTCOM's headquarters was PAL's only terror attack in the tangible world. [note: PAL is military acronym for *permissive action link* to security codes to nuclear weapons – news articles chosen due to "PAL" used in conjunction with CENTCOM]		*Stars and Stripes* 12/8/2020 ; *CNN* 1/8/2021	Biden officially announces he's picked retired CENTCOM Gen. Lloyd Austin for defense secretary ; Pelosi's letter on speaking with the chairman of the Joint Chiefs about Trump and the nuclear codes
In 2021 Al-Qaeda in Islamic Maghreb (AQIM) kills Canadian ambassador and staff during attack on Canadian Embassy in Mauritanian capital	JLASS-SP 2016	*CNN* 2/22/2021	DR Congo: Italian ambassador killed in attack on UN convoy
June 2024: an attack, in coordination with members of the Irish National Liberation Army (INLA), on a U.S. flagged air carrier transporting U.S. military personnel at Shannon Airport in Ireland. Militants fired two surface-to-air missiles at the aircraft, which was damaged but managed to land successfully. Fictional People's Armed Liberation (PAL) terrorist group includes the Irish National Liberation Army	JLASS-SP 2016	*The Irish Times* 1/19/2021 ; *The Economist* 2/6/2021 ; *The Spectator* 1/13/2021 ; *The Economist* 4/8/2021	Continuity IRA may have fired at civilian helicopter in belief it was PSNI aircraft ; A messy Brexit deal threatens to reignite violence in Northern Ireland ; Northern Ireland is still plagued by terrorism ; Brexit is the catalyst for rioting in Northern Ireland
Imagining a surprise news headline in 2019 . . . Mexico Outlaws Private Drones After Latest Assassination Attempt May 13, 2019 – Mexico City The Mexican Government today announced it was a crime for private citizens to own drones after the fifth "drone-bomb" assassination attempt by drug cartels against senior government officials in less than three months, the latest targeting the new Minister of Interior.	NIC 2017	*Liteye.com* 7/11/2018 ; *The Drive/The War Zone* 8/28/2020 ; *Forbes* 8/24/2020	Mexican Cartel Crashes Drone IED into Home of Border State Security Chief ; Drug Cartel Now Assassinates Its Enemies With Bomb-Toting Drones ; Mexican Drug Cartel Carries Out 'Drone Strikes' In Gang War
Imagining a surprise news headline in 2019 . . . China Buys Uninhabited Fijian Island To Build Military Base February 3, 2019 – Beijing A Chinese development firm—with links to the Chinese	NIC 2017	*The Guardian* 4/10/2018 *Sunshine Coast Daily* 9/25/2018 ; *The Interpreter* 10/4/2018 ;	'Impossible': China denies planning military base in Vanuatu, New Zealand Foreign Minister Winston Peters: 'This is hypothetical as Vanuatu have stated that they are not

Government and People's Liberation Army— today announced that it recently purchased the uninhabited Cobia Island from the Government of Fiji for $850 million. Western security analysts assess that China plans to use the island to build a permanent military base in the South Pacific, 3,150 miles southwest of Hawaii.		*The Guardian* 7/14/2019	aware of a military base being built' ; ISLAND GRABBING: China almost has Australia surrounded ; Australia outbids China to fund Fiji military base ; Australia must prepare for a Chinese military base in the Pacific
Generation Z, driven by malaise and discontent, launch a "Zbellion" in America in the mid-2020s. In early 2025, a cadre of these disaffected Zoomers launch a protest movement. Members of Zbellion are given instructions for going to sites on the dark web that allow them to access sophisticated malware to siphon funds from corporations and turn into Bitcoin. Zbellion leadership assures its members that their wealth redistribution is untraceable by law enforcement and 'justifiable,' as targets are selected based on 'secure polling' of 'network delegates.' Gen Z's most militant members have essentially taken to privately taxing large corporations	JLASS 2018	*Financial Times* 6/12/2020 ; *The Washington Post* 4/8/2020 ; *France 24* 1/26/2021	Pandemic helps 'Generation Z' ignite a movement ; Gen Z was fed up with the status quo. Coronavirus could affirm their beliefs. ; 'Sick of Zoom': Teachers and students rally in France for more virus support
When there's some super bug out there floating around**. But when you shut down schools, you don't just shut down schools, you shut down parents, right? You shut down businesses. You start shutting down all sorts of things**. Huge decision! So, **you use a game to start playing out the consequences, and the interactions of all those consequences**. **We did a game for our board of Institute of Civil Justice where they wanted to focus very**	The RAND Corporation "The Serious Role of Gaming at RAND" 3/23/2017	*The Associated Press* 2/4/2021	Lawmakers fast track COVID-19 liability protection bill

narrowly on questions of legal liability. Let's say a genetically engineered pathogen escapes containment and causes one of these outbreaks. Who is responsible? Who actually has legal liability for the consequences? **Is it the lab? Is it the government funder for the research that produced it?** We spent an entire day playing a game letting them look at different scenarios about how that might play out.			

'A Live Exercise'

Held in October 2019, *Event 201* scenarioed the outbreak of a global pandemic in a roundtable exercise that preceded the COVID-19 pandemic by five months. Viewed by a panel of leading experts and bureaucrats, a hypothetical news segment used in *Event 201* reports on disinformation surrounding the hypothetical CAPS pandemic: "**This is a huge problem that's going to keep us from ending the pandemic and might even lead to the fall of governments as we saw in the Arab Spring**."[217]

The connection made within a scenario between the Arab Spring and the COVID-19 pandemic is threefold. The precursory comparison of a hypothetical pandemic to the Arab Spring should indicate that the COVID-19 pandemic was a premeditated tragedy. It should also indicate that the Arab Spring was similarly premeditated. Ultimately, the connection I make suggests that irregular warfare, especially electronic warfare, was used to effect both the Arab Spring and the COVID-19 pandemic.

[TOPIC – pandemic as intentional nuclear-biological-chemical (NBC) warfare that was wargamed]

In a later section The Satellite Empire, I describe the modern world of electronic warfare. In this discussion, it will suffice to introduce electronic weaponry as it was conceived. Popularly credited as the inventor of the first electronic weapon, Nikola Tesla (1856-1943) referred to his directed energy weapon prototype as **a weapon to make war obsolete.** Newspapers referred to his electrifying prototype as a "death beam".[218] Reality has proven both conceptions accurate. Electronic warfare precludes war but not war-scale fatalities, in the manner I describe in this section.

The strategic consequence of war-precluding electronic warfare continues to evolve precipitously. This is occurring in the changing state of national security threats from the 'leaderless terrorism' or 'leaderless revolution' model to 'actorless threats'. All are effected through electronic warfare, with actorless threats being the most resistant to negotiation.

---

[217] https://youtu.be/LBuP40H4Tko "Segment 4 - Communications Discussion and Epilogue Video" @2:30
[218] https://daily.jstor.org/nikola-tesla-death-ray-craze/

+ADD https://www.justsecurity.org/72939/an-age-of-actorless-threats-re-thinking-national-security-in-light-of-covid-and-climate/ ; https://www.justsecurity.org/70001/the-perils-of-hyping-pandemic-response-as-a-national-security-issue/

+ADD In actuality being led by cartels, meaning corporate monopolies (*cartel: a group of similar independent companies who join together to control prices and limit competition.)*[219]

Air Force (Maj.?) Zachary Martin writes on the actorless threat of chemical addiction in the Drug War in *The Hydra: The Strategic Paradox of Human Security in Mexico*:

> The nature of the human security threat and the enemy's behavior it drives represent a **fundamental departure from Clausewitz's paradigm of war for two reasons**, the first being that **cartels do not seek to defeat the state**; they rely on the services and infrastructure ensured by the government's survival. Cartel members still require access to food, running water, sanitation, residential property, roads, railways, and cell towers that the continued operation of the state provides. **The threat of violence and the actual violence employed against the state do not target its downfall but rather its acquiescence**. Clausewitz notes two objectives in war: 'to overthrow the enemy—to render him politically helpless or militarily impotent, thus forcing him to sign whatever peace we please; or merely to occupy some of his frontier-districts so that we can annex them or use them for bargaining at the peace negotiation.' Cartels do not pursue these objectives because they do not seek to bargain toward an end state of peace. Instead, they seek to operate in parallel with the state to pursue their illicit business. **Additionally, <u>the lack of a political, economic, or social grievance to motivate the narcotics supply-demand dynamic means that the state lacks a coherent entity to negotiate with toward its own objectives</u>**. Likewise, because individual cartels do not hold authority over this dynamic, **the state cannot bargain with them to end it. To do so would be akin to attempting negotiations with a force of nature**.[220]

The National Intelligence Council's 2025 policy scenarios predicts failure to create a vaccine against a pandemic disease in which "tens to hundreds of millions of Americans within the US Homeland would become ill and deaths would mount into the tens of millions. Outside the US, critical infrastructure degradation and economic loss on a global scale would result as **approximately a third of the worldwide population became ill and hundreds of millions died**… Under such a scenario, **inadequate health-monitoring capability within the nation of origin probably would prevent early identification of the disease**. Slow public health response would delay the realization that a highly transmissible pathogen has emerged. **Weeks might pass before definitive laboratory results could be obtained** confirming the existence of a disease with pandemic potential. In the interim, **clusters of the disease would begin to appear in towns and cities within Southeast Asia**. Despite **limits imposed on international travel**, travelers with mild symptoms or who were asymptomatic could carry the disease to other continents. **Waves of new cases would occur every few months**. The **absence of an effective vaccine** and near universal lack of immunity would render populations vulnerable to

---

[219] https://dictionary.cambridge.org/us/dictionary/english/cartel

[220] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 4.

infection."[221] ; "2025—What Kind of Future? The above trends suggest major discontinuities, shocks, and surprises, which we highlight throughout the text. **Examples include nuclear weapons use or a pandemic.** In some cases, the surprise element is only a matter of timing"[222]

Mike Pompeo: "There's been some discussion about China – **what they knew and when they knew it.** We need to know immediately. The world is entitled to know. The Chinese government was the first to know. And that puts a special obligation, that that data gets to our scientists, our professionals. This is not about retribution. This matter's going forward. **We're in a live exercise here**… to get this right." [223]

In the March 2017 RAND Corporation's podcast *The Serious Role of Wargaming at RAND*, David A. Shlapak, Senior International Research Analyst and Codirector of the RAND Center for Gaming, speculates on a pandemic scenario, saying:

> [On] decisionmaking and planning. So, **it would be great if we could plan how to respond to the outbreak of an antibiotic resistant pathogen without actually having to have an outbreak of an antibiotic resistant pathogen.** Because that would be, as I understand it from my friends in the healthcare community, a really, really bad thing. [audience laughter] **So, we use a game.** We design games to help us work through, how would you respond? What are the interactions between the public health community and the political community? **How do political decisionmakers manage the risks associated with, say, shutting down the airports?** Right, with the economic consequences of shutting down the airports? Right. **Closing schools – that's the first thing we do when there's an epidemic threat on the horizon, because kids are little biological weapons, laboratories,** on the best days, let alone when there's some super bug out there floating around**. But when you shut down schools, you don't just shut down schools, you shut down parents, right? You shut down businesses. You start shutting down all sorts of things**. Huge decision! So, **you use a game to start playing out the consequences, and the interactions of all those consequences**. **We did a game for our board of Institute of Civil Justice where they wanted to focus very narrowly on questions of legal liability**. Let's say a genetically engineered pathogen escapes containment and causes one of these outbreaks. Who is responsible? Who actually has legal liability for the consequences? **Is it the lab? Is it the government funder for the research that produced it?** We spent an entire day playing a game letting them look at different scenarios about how that might play out.[224]

Biden Administration Intel Chief appointee Avril Haines, current Deputy Director of the CIA, was the Intelligence "player" in *Event 201* roundtable. Haines is concurrently a Senior Fellow at

---

[221] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 75.
[222] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. xii.
[223] Pompeo, Mike (Secretary of State)."User Clip: Mike Pompeo We're in a live exercise here." President Trump with Coronavirus Task Force Briefing. 20 March 2020. https://www.c-span.org/video/?c4875167/user-clip-mike-pompeo-live-exercise&fbclid=IwAR00kpFAOvV0AxCpUEEIkETSW3kuW_z3FYBp-royKtZ6MPT8h9vVa7hH4nk
[224] https://www.rand.org/multimedia/audio/2017/03/23/the-serious-role-of-gaming-at-RAND.html @9:00-11:10

the Johns Hopkins University Applied Physics Laboratory and is on the board of the Nuclear Threat Initiative's Bio Advisory Group, the Board of Trustees for the Vodafone Foundation, and the Refugees International Advisory Council.[225] Haines is also known for her role in the Obama Administration's target killing drone program and her refusal to take disciplinary action against her own agency when it was revealed that the CIA had hacked the computers of Senate Intelligence Committee staff during the Committee's 2009-2014 investigation into the CIA's detention and torture program, the committee which rendered the 6,000 page *Report on Torture*.[226]

[October 2019 *Event 201* pandemic tabletop exercise videos]
Segment 1[227]: @24:20 "GNN" news channel reports medical supplies hoarding (3M featured) ; @19:00 pandemic model likened to Spanish Flu of 1918 ; @48:00 lack of surveillance in underdeveloped nations mean they don't know who is infected ; @35:40 pandemic-related predatory loans to Third World, IMF/World Banks ; @45:00 school closures as transmission loci ; @46:40 discrepancies in fatality rates ; @55:40 conspiracy theories released that governments and companies released the virus.
Segment 2[228]: @3:45 "it's also leaders themselves…spreading misinformation", 'GNN' states "good public health info accurate and truthful" ; @19:40 NIC representative Haines "flood telecoms with trusted sources"…(@20:30) "identifying foreign disinformation campaigns" ; @35:20 "disinformation censorship on healthcare became a political persecution tool…"
Segment 3[229]: @1:40 GNN report: Response to the CAPS pandemic is now the world's most expensive international emergency ever
@2:00 GNN report - **Fake expert economist Dave Gamble, PhD**: "What exactly are the risks and benefits of slowing air travel, of staying home from work, closing schools, disrupting supply chains, interfering with our reliable channels of communication and news? Sure, some of these steps can help slow CAPS, but often only marginally and with serious costs. When this is all over some families, some cities will have suffered more from our interventions than from CAPS." / **Fake Reporter**: "No question, there is a lot of suffering."
@5:10 Dr. Eric Toner from panel: "Losses are greater in the wealthier countries despite having fewer cases… [Global per capita GDP] There could be an 11% decline in GDP at the one year mark into the pandemic, and a 25% fall at the two year mark, when after the full effects of the pandemic are felt." … @6:45 "The World Bank and IMF would not have enough money to get us out of this crisis."

Minority deaths disproportionate
Segment 4[230]: @2:30 "We know **social media companies** are working around the clock to combat these disinformation campaigns, but the task of identifying every bad actor is immense. Experts agree that new **disinformation campaigns** are being generated everyday. **This is a huge problem that's going to keep us from ending the pandemic, and <u>might even lead to the fall</u>**

[225] Center for Health Security. *Event 201 Players: Avril Haines*. Center for Health Security webpage. Accessed 20 January 2021.
[226] Katkov, Mark. "Biden Pick For Intel Chief: 'Biggest Challenge Is Building Trust And Confidence'". *NPR*. 19 January 2021.
[227] https://youtu.be/Vm1-DnxRiPM "Segment 1 - Intro and Medical Countermeasures (MCM) Discussion"
[228] https://youtu.be/QkGNvWflCNM "Segment 2 - Trade & Travel Discussion"
[229] https://youtu.be/rWRmlumcN_s "Segment 3 - Finance Discussion"
[230] https://youtu.be/LBuP40H4Tko "Segment 4 - Communications Discussion and Epilogue Video"

of governments as we saw in the Arab Spring. If the solution means controlling and reducing access to information, I think it's the right choice." ; Epilogue: @33:00 **65 million dead ;** @34:00 **"The global economy was in free fall. The GDP down 11%. Stock markets around the world plummeted between 20 and 40%... While nearly all businesses were affected, certain sectors were especially hard hit: travel, finance, service, manufacturing, healthcare, and insurance among them, with some major companies going bankrupt."** ; @34:40 "The world saw **large scale protests and, in some places, riots**. People were angry about the loss of access to healthcare and medicine, as well as government's inability to protect them from the disease. This led to **violent crackdowns in some countries and even marshal law**. Political upheaval became the rule across the globe **as the public lost trust** in their respective administrations. **Several governments fell** while others were desperately striving to hold on to power. **This spurred further crackdowns. Attempts to control media messaging – originally only aimed at health-related misinformation - became used increasingly to quash political dissent.** Economists say the economic turmoil caused by such a pandemic will last for years, **perhaps a decade**. **The societal impacts – the loss of faith in government, the distrust of news, and the break down of social cohesion – could last even longer.** We have to ask: Did this need to be so bad? Are there things we could have done in the five to ten years leading up to the pandemic that would have lessened the catastrophic consequences? We believe the answer is yes."
"Segment 5 - Hotwash and Conclusion" +ADD "wash-up" wargame term for post-game analysis (photocopies *Future of War* navy book, pg. ~60)

Science fiction story published the Marines: "The Montgomery Crisis," display and small arms technology advances, but the U.S. Navy has to make do with then-ancient vessels and planes, like Zumwalt-class destroyers, Ford-class carriers, and F-35B Lighting II Joint Strike Fighters. The military threats are still anti-access, area-denial, powerful ship-killing foreign-designed missiles in the hands of radical religious extremists with near-peer backing. **But it's the impetus behind those attacks, the plague and the grain shortage, that provides the most direct shift: an America made hungry, through careful sabotage at the hands of just a few well-placed malcontents. The story ends with victory, but a temporary one**: the plague vector remains, and is beyond the problem-solving abilities of the Marines. Instead, grain shipments and free global trade provide the immediate salvation…"[231]

+ADD Wargame roundtable notes from videos Clade X, Event 201

Colonel Guo Ji-wei, The People's Liberation Army, China, is Director, Department of Medical Affairs and **Yang Xue-sen,** is a biotechnology lecturer. "Ultramicro, Nonlethal, and Reversible Looking Ahead to Military Biotechnology" in 2005: "Directed-energy-induced mutation. High-intensity ultraviolet rays and electromagnetic waves can induce genetic-locus cell mutation.9 If we determine the relationship between the specific frequency, wavelength, or power of the ray or wave and the specific gene or locus, we can cause injury by remote, radiation-induced, genetic function changes. Direct integration. University of Wisconsin scientists have made exogenous, naked DNA and injected it into veins for easy access into muscle cells for gene therapy. By combining this knowledge and particle-gun technology, we could create a microbullet out of a 1-μm tungsten or gold ion, on whose surface plasmid DNA or naked DNA could be precipitated,

[231] https://news.usni.org/2017/10/17/marines-solicit-science-fiction-stories-imagine-future-conflicts

and deliver the bullet via a gunpowder explosion, electron transmission, or high-pressured gas to penetrate the body surface. We could then release DNA molecules to integrate with the host's cells through blood circulation and cause disease or injury by controlling genes. Biological tag-tracing, electromagnetic targeting, and nanometer biological technologies can help build highly military-oriented biotechniques. While it is perhaps too early to decide what form modern biotechnological weapons might take, one thing is sure: all such weapons require a military that focuses on information more than on mechanization… such weapons might finally change the methods of "physical annihilation" or "destruction within the killing range" which have characterized war since the invention of gunpowder… Specificity of wounding. Precision injury is an embodiment of specificity. HGP and proteomics have greatly enriched bioinformation. If we acquire a target's genome and proteome information, including those of ethnic groups or individuals, we could design a vulnerating agent that attacks only key enemies without doing any harm to ordinary people. We could also confine the attack to a more precise level. Injuries might be limited to a specific gene sequence or a specific protein structure. Through gene manipulation, we can attack or injure one or more key human physiological functions (the ability to learn, memorize, keep one's balance, or perform fine motor activities and even act aggresively) without a threat to life. Ultramicro damage. When attacking an enemy with biotechnological military weapons, we could choose targets from a nucleotide sequence or protein structure. We could cause physiological dysfunction by producing an ultramicro damaging effect to a gene's or a protein's structure and functioning. Precision injury and ultramicro damage are two vulnerating methods based on genomics and proteomics. Because they target the primary structure of the gene or protein, they are completely different from traditional weapons of war that directly damage tissues and organs. Crypticity. Although applications of military biotechnology are complicated, the finished products are convenient to carry, easy to use, and do not require large support systems. Detecting and predicting their use is difficult. Only after obvious wounding occurs will enemies realize they are under attack. In this sense, using military biotechnology weapons is a good tactic. Controllability and recoverability. Unlike weapons that use ammunition whose damaging effects can only be ascertained after shooting, we can test in a laboratory the degree of damage biotechnological weapons produce. We can control the degree of injuries and damage produced and even provide an antidote or a cure (a vaccine, a countervulnerating agent, or a piece of bioinformation). Providing such an anodyne to our enemies would represent real "mercy."… Traditional biological weapons aim to produce mass destruction. They reduce the enemy's fighting power by damaging a large number of human beings, livestock, crops, and even the ecological system. Biological weapons of mass destruction originated from the idea that the more they kill and the fiercer the disasters they produce, the better they are. Technologically, traditional biological weapons depend on microbiology, especially bacteriology, which uses destructive bacteria, viruses, and toxic living bodies obtained directly from the natural world. These weapons are subject to nature, are difficult to control, and have irreversible effects. The use of such weapons is opposed by most countries in the world…. current military biotechnology possesses a quality of "mercy," and its action, purpose of study, and specifications are totally different from traditional biological weapons. Modern biotechnology will help rid the world of primitive forms of microorganisms, biological agents and toxins; offer an alternative to biological warfare; and, ultimately, help eliminate traditional biological weapons."[232] (76-78 pg)

[232] Ji-wei, Colonel Guo and Xue-sen Yang. "Ultramicro, Nonlethal, and Reversible Looking Ahead to Military Biotechnology". *Military Review*. July-August 2005.

The COVID-19 pandemic, as has been noted, has epidemiologically spread unlike most airborne infectious diseases, defying many experts' model-based predictions. Symptomatically, it is consistent with high level exposure to electromagnetism.
"Influential COVID-19 model uses flawed methods and shouldn't guide U.S. policies, critics say"[233]

"Surgisphere: governments and WHO changed Covid-19 policy based on suspect data from tiny US company"[234]

"Study estimates US Covid-19 infections may be 4 times higher than reported"[235] based on "Estimation of US SARS-CoV-2 Infections, Symptomatic Infections, Hospitalizations, and Deaths Using Seroprevalence Surveys": "**Findings:** In this cross-sectional study using data from public health surveillance of reported coronavirus disease 2019 cases and seroprevalence surveys, an estimated 46 910 006 SARS-CoV-2 infections, 28 122 752 symptomatic infections, 956 174 hospitalizations, and 304 915 deaths occurred in the US through November 15, 2020. **Meaning**: Findings of this study suggest that although more than 14% of the US population was infected with SARS-CoV-2 by mid-November, a substantial gap remains before herd immunity can be reached… Conclusions: In this cross-sectional study, estimates of underreporting multipliers were derived and combined with surveillance data to adjust reported surveillance data for underreporting. Results suggest that although more than 14% of the US population may have been infected with SARS-CoV-2 as of mid-November 2020, there remains a substantial gap between the estimated proportion of the population infected and the proportion infected that is required for herd immunity. Additional seroprevalence surveys are warranted to monitor the pandemic, including after the development of safe and efficacious vaccines."[236]

For lack of a coherent epidemiological model fitting the spread of COVID-19, researchers in mathematics and chemical engineering at the Rochester Institute of Technology published an article in *Physica D: Nonlinear Phenomena*, a physics journal, titled "Accurate closed-form solution of the SIR epidemic model".[237] The researchers created a model for the spread of COVID-19 based on demonstrated solutions to problems in published research on quantum gravity, including Fourier solutions for localized oscillatory forcing/signaling problems of radar imaging, and mechanical engineering, including thermodynamics of boundary density fluid flow and equilibrium.

This is to say, interpreting prolonged microwave signals over territories and their visualizations as images on radar has proven predictive of the spread of the COVID-19 'virus'. As well, measuring the engineered flow of particles in fluid dispersed and how that fluid

---

[233] Begley, Sharon. "Influential COVID-19 model uses flawed methods and shouldn't guide U.S. policies, critics say". *STAT*. 17 April 2020.
[234] Davey, Melissa, Stephanie Kirchgaessner and Sarah Boseley. "Surgisphere: governments and WHO changed Covid-19 policy based on suspect data from tiny US company". *The Guardian*. 3 June 2020.
[235] https://www.cnn.com/world/live-news/coronavirus-pandemic-vaccine-updates-01-05-21/h_833be27384fd892bf390e72fe3f34b1e
[236] https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2774584?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=010521
[237] Barlow, Nathaniel S. and Steven J. Weinstein. "Accurate Closed-Form Solution of the Sir Epidemic Model". *Physica D: Nonlinear Phenomena*. Vol. 408. 2020.

distributes over areas with structures has also proven more predictive of the spread of COVID-19. The caveat in this model lies in people's movement traced as though they were dispersing particles. The model does not actually address particle dispersal, like might be expected with airborne disease.

regular epidemiological models which focus on viruses which spread via human-to-human contact transmission. In other words, COVID-19 is more likely contracted via long-term microwave radar imaging. Additionally, populations are better imagined as settling of fluids released into the open air over vast urban regions, rather than through human-to-human infection. The success of this model calls into question the validity of so-called 'contact tracing' surveillance being implemented to reduce COVID-19 transmission.

The COVID researchers claim that their "method was based on solutions they previously developed to very different problems in thermodynamics, fluid mechanics and predicting the trajectories of light around black holes… Although the authors haven't previously worked in the field of epidemiology, their previous work translated seamlessly to this new field."[238]

The model, for reasons unclear, treats 'susceptible populations' as a variable undefined from total population, and treats 'susceptible populations', 'recovered populations' and 'infected populations' analogically as flowing fluids of varying densities which obey the laws of thermodynamics, i.e. heat transfer, in their interactions. While one might expect a thermodynamic model of virology to treat the flow of infectious fluids emitted between populations, this is not the stated case. At face value, this model suggests a near-medieval understanding of fever contraction which could be caused by certain heat transfer rather than by a host of factors that would determine contraction of bacteria or viruses.

The relation of all of this to black holes and gravitational physics, other than the variable *t*=time, remains remarkably undefined. One possible interpretation agrees with COVID-19 being the effect of radiation. Irradiation causes the breaking apart of molecules at the atomic level, specifically electrons. Atoms react similarly around black holes, phenomena in outer space which are believed to tear apart all matter and light at the atomic level.

While there may be problems with the model, its successful prediction of COVID-19 spread through applying laws of thermodynamics and radar physics indicates that the 'virus' is spread via mechanisms outside of human-to-human contact transmission, as Chinese government officials have alleged.

Along with this more successful thermodynamic or astrophysics model for virus spread, environmental indicators have arisen which are associated with unusually high levels of tapping into the geomagnetic belts used for directed energy weaponization. In April 7, 2020, an atmospheric "record-size hole" above the Arctic formed two weeks after the so-called pandemic was declared. The previous occurrence of atmospheric holes forming above the Artic was in the spring of 2011, coinciding with the Arab Spring movement.[239] Further argument for the causal relation between so-called leaderless revolution, war and mass poisonings is made in the section Radio-logical Warfare.

It should also be noted that contact tracing surveillance involving counterintelligence training is the same "peace deal" the Taliban - not the Afghan National Government - received in

[238] Web Desk. "New mathematical method to help epidemiologists map spread of COVID-19". *The Week.* 4 June 2020.
[239] Harvey, Fiona. "Record-size hole opens in ozone layer above the Arctic". *The Guardian.* 7 April 2020.

February 2020, detailed in a secret accord with Washington which has been viewed only by select persons kept in an underground Capitol bunker.[240] [MOVE]

Scott Atlas, professor of neuroradiology, appointed White House adviser on pandemic: "Prior to joining the Hoover Institute at Stanford, Atlas was the chief of neuroradiology at the school's medical center from 1998 to 2012, according to his profile on Stanford's website."[241] "Dr. Atlas is also the editor of the leading textbook in the field, Magnetic Resonance Imaging of the Brain and Spine" and author of a 2012 publication in the *Journal of Radiology* on the effects of exposure to ionizing radiation.[242]

"Managing the Risk From COVID-19 During a Return to On-Site University Research"[243] by the JASON group further supports the argument that COVID-19 is the result of cyber and biological warfare, specifically the group's involvement in advising university reopening procedures. The JASONs, founded during the early Cold War to advise the government on the use of "electronic barriers" (acoustic and heat-detecting remote sensing partition technologies) in the Vietnam War, are an unlikely group to advise academic policy on influenza-style health measures. The JASONs are concerned almost exclusively with defense technologies including cyberwarfare, nuclear missiles, lasers, climate change, ELF radio transmissions, space science imaging, radiological detection, aircraft pollution, biological weapons defense, and directed energy weaponry." The group's special purpose for cyber defense planning begs the question why the JASONs would be especially fit to advise on the COVID response.[244] [245]

While the JASONs have published recently on AI health informatics, as recently as 2017 their research has specifically focused on diseases which can be caused by radiological exposure including heart conditions, retinopathy, and skin cancers. **The group's research on health informatics are now measures proposed for use with COVID**, including contactless diagnostic imaging, making networked medical records interoperable, supporting corporate data-driven healthcare enterprises, capturing mobile device information for health application, crowdsourcing data collection for health applications, virtual health monitoring, capturing data on toxin exposure, and environmental remote sensing and imaging over different geographical areas. The JASONs themselves in 2017 described this confluence of R&D as "this seemingly perfect storm".[246]

By applying the exact health informatics measures proposed for experimentation two years earlier by the JASONs to a novel virus, which also mimics the effects of radiation exposure on humans *and* the climate, further supports the claim that this pandemic has been intelligently

---

[240] https://www.newsbreak.com/news/1523045371951/a-secret-accord-with-the-taliban-when-and-how-the-us-would-leave-afghanistan

[241] Collman, Ashley. "Meet Trump's new coronavirus adviser Dr. Scott Atlas, a Stanford physician who frequently criticized lockdown measures and believes in the full reopening of schools". *Business Insider*. 13 August 2020.

[242] Profiles. "Scott W. Atlas: Senior Fellow at the Hoover Institute". *Stanford University webpage*. Accessed 13 August 2020.

[243] JASON. *Managing the Risk From COVID-19 During a Return to On-Site University Research*. JASON The MITRE Corporation. 10 July 2020.

[244] https://en.wikipedia.org/wiki/JASON_(advisory_group)

[245] http://large.stanford.edu/courses/2013/ph241/kallman2/

[246] JASON. *Artificial Intelligence for Health and Health Care*. JASON The MITRE Corporation. December 2017, p. 9.

plotted for return benefit to R&D industries, and has been steered publicly (and surreptitiously) via the VNN effect.

The nature of the JASONs as an elite group of fulltime academics active in research and development, along with the focus of their 2020 publication stating that "JASON charged itself to assess risks and best practices for restarting university research programs," further supports arguments made in this essay's section Recent Developments and Research and Development: that research and development industries fund themselves through a cycle of violence that begins with R&D followed by shocking developments publicized, resulting in more demand for R&D, all part of a mechanism to maintain relevancy and funding. [FIND OTHER CITE]

The Army posture on its pandemic response is expressed on its website:

> **As part of the COVID-19 response**, **the U.S. Army Rapid Equipping Force**, Program Executive Office Soldier and the C5ISR Center of U.S. Army Combat Capabilities Development Command **led the initiative to use thermal-imaging devices to screen for potentially elevated body temperatures** of personnel entering military facilities… 'This is a different adversary we are combating and, as always, it is **our number-one priority to protect the force** and community to ensure our safety, resilience and readiness,' Wilson said. 'We are looking to the **thermal-imaging sensors as one of many methods to prevent the spread** and exposure of COVID-19.'[247]

This exemplifies the US military's neglect of military duties to protect the nation, situations in which a greater emphasis is placed on self-defense of the military industrial complex while endangering civilian populations in order to provide greater (maybe unnecessary) protection for military personnel.

Specifically, the military neglects full-scale conflict risks inherent in militarizing civilian areas "such as Metro entry points" as the article mentions, positioning troops in civilian centers, and the proliferation of militarized technologies to civilian populations. The actions taken by the US military during COVID-19 to protect military interests and personnel increases the incident of conflict through increased troop presence and accelerated technologies scaling. The argument that potential human adversaries may be deterred by US troop presence and technology scaling cannot apply to a virus as adversary.

Government responses have consistently framed the pandemic as a "war".
from Channel 4 News "Coronavirus '**worse than a bomb'** on Italy, says doctor coordinating" and "Coronavirus expert: '**War is an appropriate analogy/Virus expert: This is war**". ; "'I know what I am asking of you is unprecedented, but circumstances demand it. **We are at war,' Macron** said… All travel between European countries will be suspended."[248]
+ADD On the website of the Department of Defense Non-Lethal Weapons Program's Joint Intermediate Force Capabilities Office, a Captain George Galdorosi (Ret.) published an article on April 1, 2019 entitled "Unleash Directed-Energy Weapons" which calls for the increased use of electronic weaponry[249] [ADD quotes printed article] ;
Russia's vaccine called Sputnik V, after the first orbiting satellite *Sputnik*, purported to be the first vaccine to the Coronavirus-19.[250]

---

[247] https://www.army.mil/article/235191/army_ref_deploys_thermal_imaging_sensors
[248] http://www.ecns.cn/news/politics/2020-03-17/detail-ifzunmih1236773.shtml
[249] https://jnlwp.defense.gov/Press-Room/In-The-News/Article/1809399/unleash-directed-energy-weapons/
[250] https://sputnikvaccine.com

+ADD **"This is Iran's Chrenobyl"**[251]

Years earlier in the spring of 2009, Center for Disease Control Director Tom Frieden briefed former President Obama on the so-called Swine Flu epidemic in similar war lexicon:

> He [Obama] asked a series of questions about H1N1, which was just kind of emerging and it was kind of like **a fog of war reality** and he said, 'This isn't going to kill a million people, is it doctor?' And I answered, 'No, Mr. President.'[252] [**Clausewitz 'fog of war' reference]**

+ADD RAND Corporation accuses the nation state for "vaccine nationalism", spread of "virus", games the global effects of vaccine absence or vaccine misdistribution:
"In this study [*COVID-19 and the Cost of Vaccine Nationalism* (2020)], we examine some of the negative consequences that vaccine nationalism could have in terms of how well we manage the pandemic in the future once a vaccine has been developed. **Another objective is to understand the potential economic implications that could arise if countries follow a nationalistic behaviour with regard to the development, manufacturing and distribution of future COVID-19 vaccines**. To this end, we use a macroeconomic model where all countries in the world are interlinked with each other through trade in goods and services as well as investment. **The model allows us to put the world economy into a laboratory and run different 'what-if' experiments, in order to examine what would happen to global economic output if no vaccine was developed or if only a few countries or regions managed to immunise their own populations**.[253]

"Why a **vaccine** for coronavirus will take longer to develop than you might think" *USA TODAY* [254] ; https://www.youtube.com/watch?v=ek3T8xiu1Fw "The Race To Develop A Coronavirus Vaccine" *CNBC News* 14 March 2020 [relate to **R&D** – 'chaos', **'financial markets'**, 'freezing supply chains', 'competition for developing vaccines'] [255]
+ADD Michael Brendan Dougherty (*The Week* correspondent) on Twitter via MSNBC News 2/28/2020: "I can't emphasize enough that he [Trump] **can't stop the sell off without a competent public health response."** And "The more they treat this as a market and re-election problem, the worse the market and re-election problems can become."
+ADD "**No final conclusion on the natural host of the COVID-19 virus has been made yet so far**, which is key to epidemic prevention as **an unclear origin** means there is a potential risk of animal-to-human infection, a top Wuhan pathogen biologist told the Global Times in an exclusive interview… The poor conditions at the seafood market made it an ideal place for the virus to reproduce and spread. But currently, we can only say that 'Huanan seafood market is likely to be one of the places of the origin of the epidemic,' Yang said. Regarding the 'biochemical war' conspiracy theory circulated online, Yang explained that **Wuhan held the Military World Games in October last year [2019]** and the US delegation stayed in a hotel not far from the seafood market. **Wuhan discovered cases of coronavirus infection later in**

---

[251] https://www.cnn.com/2020/03/18/politics/state-department-coronavirus-iran-outreach/index.html
[252] NBC Nightly News Broadcast (Full) - March 13th, 2020 | NBC Nightly News https://www.youtube.com/watch?v=WuyFniRMrxY
[253] Hafner, Marco, Erez Yerushalmi, Clement Fays, Eliane Dufresne, and Christian Van Stolk, *COVID-19 and the cost of vaccine nationalism*. The RAND Corporation. 2020, p. iii.
[254] https://www.youtube.com/watch?v=hO-UiPoi3iI "Why a vaccine for coronavirus will take longer to develop than you might think" *USA TODAY* 12 March 2020
[255] https://www.youtube.com/watch?v=ek3T8xiu1Fw "The Race To Develop A Coronavirus Vaccine" *CNBC News* 14 March 2020

December. 'This is why some people have speculated that **the outbreak is a biochemical war** conspiracy launched by the US against China,' Yang said."[256] ; "Chinese foreign ministry spokesman Zhao Lijian took to Twitter on Friday to double down on an unproven claim that the US military brought the new coronavirus to the central city of Wuhan, where the outbreak began… **The allegation was apparently linked to the US Army's participation in the international Military World Games held in Wuhan in October**, which drew competitors from more than 100 countries… It comes as senior US officials including President Donald Trump have sought to describe it as a 'foreign virus', with US Secretary of State Mike Pompeo and Republican leaders going further to label it the "Wuhan virus" or "Chinese coronavirus","[257] and also "a live exercise" about which China withheld information from the US.

Final argument that COVID-19 is radiological warfare rather than biochemical attack or viral phenomenon: "'The Psychology of Biological Warfare'… the primary **reason for the decline of biological warfare** is that is has become too easy to start and too difficult to stop. **Germs and viruses are not as disciplined as soldiers** and will attack any vulnerable victim they can reach."[258]

The responses to the 2020 COVID-19 pandemic have been draconian, to say the least. Associate Supreme Court Justice Samuel Alito spoke on what the American Bar Association, in relation to Homeland Security provisional governance, has described as "something more than the exercise of executive power":

> The pandemic has resulted in previously unimaginable restrictions on individual liberty. I'm not saying anything about the legality of COVID restrictions. Nor am I saying anything about whether any of these restrictions represent good public policy. I'm a judge, not a policymaker… I think it is an indisputable statement of fact, **we have never before seen restrictions as severe, extensive and prolonged as those experienced**, for most of 2020. Think of all the live events that would **otherwise be protected by the right to freedom of speech**, live speeches, conferences, lectures, **meetings**, think of worship services, churches closed on Easter Sunday, synagogues closed for Passover on Yom Kippur War. Think about access to the courts, or the constitutional right to a speedy trial. **Trials in federal courts have virtually disappeared** in many places. One of these is **the dominance of lawmaking by executive Fiat rather than legislation**. The vision of early 20th century progressives and the new dealers of the 1930s was the **policymaking would shift from narrow minded elected legislators, to an elite group of appointed experts in a word, the policymaking would become more scientific. That dream has been realized to a large extent…** And what have we seen in the pandemic **sweeping restrictions imposed for the most part, under statutes that confer enormous executive discretion**… Under that law**, if the governor finds that there is, quote, a natural, technological, or manmade emergency, or disaster of major proportions, the governor can perform and exercise such functions**, powers and duties as are necessary to promote and secure the safety and protection of the civilian population. To say that this provision confers broad discretion would be an understatement… laws giving an official so much discretion can of course, be abused. And

[256] GT Staff Reporters. "Wuhan pathogen biologist addresses six conundrums about deadly novel coronavirus". *Global Times*. 16 February 2020.
[257] Zheng, Sarah. "Chinese foreign ministry spokesman tweets claim US military brought coronavirus to Wuhan". *South China Morning Post*. 13 March 2020.
[258] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 254.

> whatever one may think about the COVID restrictions, we surely don't want them to become a recurring feature after the pandemic has passed. **All sorts of things can be called an emergency or disaster of major proportions**. Simply slapping on **that label cannot provide the ground for abrogating** our most fundamental rights… it does not mean that whenever there is an emergency, executive officials have unlimited unreviewable discretion.[259] [+ADD MORE…]

In *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments*, Ernest B. Abbott, Otto J. Hetzel, and the American Bar Association describe:
+ADD "The Homeland Security Act of 2002 (HAS) includes 'emergency medical and related personnel, agencies, and authorities' in its definition of 'emergency response provider.' On February 28, 2003, President Bush released **Homeland Security Presidential Directive 5** (HSPD 5)… The NPR [National Response Plan] was adopted in November 2004. The NRP includes in its first responder definition 'public health, clinical care, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations… **Initial actions by responders may include surveillance, testing processes, immunizations, prophylaxis, and isolation or quarantine for biological threats**… NIMS [National Incident Management System] outlines the NIC's [NIMS Integration Center] in very approximate terms. A variety of entities, including local, state, tribal, federal, private sector, and professional organizations may suggest changes in NIMS standards and other corrective actions. The **secretary of DHS** [Department of Homeland Security], however, **retains ultimate authority** for alteration of NIMS standards. In other words, **other affected entities** may put forward modifications, but their **input is advisory only**. "[260]
+ADD "NFPA 1600 [National Fire Protection Association's Standard on Disaster/Emergency Management and Business Continuity Programs, proposed by the National Commission on Terrorist Attacks Upon the United States (a.k.a. 9/11 Commission)] recommends that financial institutions and insurers consider compliance when evaluating creditworthiness and insurability. For those enterprises, **compliance will result in better protection of their own assets**. Therefore, they will likely adopt the proposal. The result would be that businesses of individuals not in compliance could find themselves facing significant increases in the costs of borrowing and insurance. For the health care industry, the cost and availability of insurance is already creating national concern. **Similarly, this capital-intensive business cannot function without the availability of credit. In this manner, the federal government has created a system that relies on business to encourage obedience with the standard**. "[261]
"MSEHPA comes down strongly on the side of public health regulation, granting broad powers to states. **State adopting MSEHPA provisions have given their governors broad powers to declare and enforce public health emergencies**. MSEHPA also would allow adopting states to **seize medical supplies and drugs, regardless of ownership**, during a declared public health

---

[259] Alito, Associate Supreme Court Justice Samuel, ed. Josh Blackman. "Video and Transcript of Justice Alito's Keynote Address to the Federalist Society". *Reason.* 12 November 2020.
[260] Abbott, Ernest B. and Otto J. Hetzel, eds. *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments.* American Bar Association. 2005, p. 60-61.
[261] Abbott, Ernest B. and Otto J. Hetzel, eds. *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments.* American Bar Association. 2005, p. 62.

emergency. Authorities also could **take possession of, utilize, and if needed, destroy property**."[262]

"In the United States**,** it has **never been quite true that** the measures needed to meet **emergencies are outside the strictures of the law; it is more accurate to say that, in the past,** the law and its **normal processes have been too slow to keep up with the pace of emergencies**. This is probably even more accurate given the potential of new threats of terrorist acts and other situations that have not been encountered previously. The ability of lawyers to function in such pressure situations is changing **with the development of ever-faster microprocessors.** This **evolution of information and its processing**, in less than a generation, has vastly improved the lawyer's ability to function in emergencies… as in many states, the power of the state to act in emergencies is vested in **the governor as its chief executive authority**. The governor is the 'commander-in-chief of all military forces of the state not in active service of the United States…[and] the chief administrative officer of the state responsible for the planning and budgeting for the state.' The state constitution further provides that the governor **'shall have power to call out the militia to preserve the public peace, execute the laws of the state, suppress insurrection, or repel invasion**.'… The sweeping delegation of authority from the governor to the state coordinating officer relates to this in several ways. First, the delegation **concentrates formidable powers into the hands of the state coordinating officer.** Second, these powers are **not the exercise of executive powers only**. While countenanced by authorizing legislation or based on constitutional powers relating to emergencies, the exercise of such authority **may be used to countermand**, at least for a time, other **laws** adopted by the legislature. **Exercising that emergency authority intrudes upon the legislative function.** This is something more than the exercise of executive power. Third, as a practical matter, the state coordinating officer is often too preoccupied with operation duties to select *ad interim* statewide policies from the wide array of options available, for better or worse. This may include such quasi-legislative determinations as choosing which features of the statue or rule should be suspended, for how many days, and for which cities or counties. Often, these decisions are left to counsel. Therefore, **counsel must take on the added role of policymaker**… In such circumstances, lawyers should understand that they are assuming a multiple role that may compromise their independent professional judgment, or pose yet other ethical issues… On the one hand, counsel must frame the orders to ensure that agencies or other parties are relieved of literal compliance with a statue or rule whose requirements can no longer be met, or circumstances arise where adherence to those requirements cannot be justified in the face of an emergency. On the other hand, an important role and obligation of counsel is to limit the scope and duration of the order, so that it is no broader than necessary to achieve the intended purpose. **By declaring a state of emergency, the governor has not only called up formidable powers of that office to countermand what the legislature has done, but has in turn delegated that power to the state coordinating officer, who has not been elected by anyone**. It therefore falls to counsel to be aware of the need to strike the appropriate balance between what is needed to meet the disaster and the public interest in restoring the law to its *status quo ante* once the need has passed. This is not the only variable in the equation. The interest of **various political constituencies do not go into hibernation when disaster strikes. Indeed, some of them see the disaster as a window of opportunity to achieve ends the law denies them in ordinary times.** Lawyers preparing for a role in emergency management must be prepared to assume their

---

[262] Abbott, Ernest B. and Otto J. Hetzel, eds. *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments.* American Bar Association. 2005, p. 64.

roles before an emergency exists, and they need to be familiar with the statutory and regulatory maze applicable to situations where they will be asked to make adjustments to existing policies when the emergency arises. **Undertaking this role effectively would not have been possible a generation ago, but the current texts of relevant statues, rules, and cases are now only keystrokes away.**"[263]

From *Preparing for a Pandemic Influenza: A Primer for Governors and Senior State Officials* (2006) by National Governors Association Center for Best Practices: "Pandemic preparedness involves more than **stockpiling pharmaceuticals** and planning for **surges of patients at hospitals**. A severe pandemic will affect all sectors of society: **high rates of worker absenteeism** could **affect the operations of water treatment facilities and power plants**; efforts to slow or stop the spread of the disease could **limit the availability of food**, **cause schools to be closed** for significant periods of time, and **create economic hardships for state and local governments**, **business** owners, and **individuals**; and government efforts to manage **the public's response could be complicated by the myriad sources of information—including the Internet**—on which people rely for guidance."(p. ii) … "Once a pandemic happens, we will divide forever the progress of our nation as pre-pandemic and post-pandemic." When a pandemic occurs, the impact of the disease will join the lexicon of nation-changing incidents on the scale of 9-11 and the 2005 Hurricane Season. In every state, governors and senior officials will be at the forefront… An episode of pandemic influenza is the viral equivalent of a perfect storm. Three essential conditions must be met for an outbreak to begin: **A new flu virus must emerge from the animal reservoirs** that have produced and harbored such viruses—**one that has never infected human beings and therefore one for which no person has developed antibodies**. **• The virus has to make humans sick (most do not).**; **It must be able to spread efficiently, through coughing, sneezing, or a handshake**." (p. iv)[264] [+ADD more]

http://www.centerforhealthsecurity.org/event201/about *Event 201* held NY,NY October 18, 2019 by Gates Foundation, World Economic Forum and Johns Hopkins;
http://www.centerforhealthsecurity.org/event201/scenario.html: "Event 201 simulates an outbreak of a novel zoonotic coronavirus transmitted from bats to pigs to people that eventually becomes efficiently transmissible from person to person, leading to a severe pandemic. The pathogen and the disease it causes are modeled largely on SARS, but it is more transmissible in the community setting by people with mild symptoms.The disease starts in pig farms in Brazil, quietly and slowly at first, but then it starts to spread more rapidly in healthcare settings. When it starts to spread efficiently from person to person in the low-income, densely packed neighborhoods of some of the megacities in South America, the epidemic explodes. It is first exported by air travel to Portugal, the United States, and China and then to many other countries. Although at first some countries are able to control it, it continues to spread and be reintroduced, and eventually no country can maintain control. There is no possibility of a vaccine being available in the first year. There is a fictional antiviral drug that can help the sick but not significantly limit spread of the disease. Since the whole human population is susceptible, during the initial months of the pandemic, the cumulative number of cases increases exponentially, doubling every week. And as the cases and deaths accumulate, the economic and societal consequences become increasingly severe. The scenario

[263] Abbott, Ernest B. and Otto J. Hetzel, eds. *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments.* American Bar Association. 2005, p. 139, 140, 145-146.
[264] https://www.nga.org/wp-content/uploads/2020/02/Pandemic-Influenza-Primer.pdf

ends at the 18-month point, with 65 million deaths. The pandemic is beginning to slow due to the decreasing number of susceptible people. The pandemic will continue at some rate until there is an effective vaccine or until 80-90% of the global population has been exposed. From that point on, it is likely to be an endemic childhood disease."[265] ; Big tech involvement "Steve Wozniak [Apple Co-founder] Checking out Janet's bad cough. Started Jan. 4. We had just returned from China and may have both been patient zero in U.S. (@ West Coast Sports Institute in Santa Clara, CA)"[266]
https://www.centerforhealthsecurity.org/our-work/events-archive/2005_atlantic_storm/index.html virus wargamed as bioterrorist attack in Atlantic Storm 2005 & https://www.centerforhealthsecurity.org/our-work/events-archive/2001_dark-winter/index.html Dark Winter wargamed as covert bioattack in 2001, both *Dark Winter* and *Atlantic Storm* and *Clade X* (2018) listed on *Event 201* (Oct. 2019) website

"[CDC Director] Dr. Anthony **Fauci said in June 2019 that his nightmare public-health scenario** was a **'respiratory illness that easily spreads and has a high degree of morbidity** and some degree of mortality.'… **'I'm so sorry that I was so prescient** when we had our last interview, Steve. I really am very sorry about that,' Fauci said during this year's edition of The Hill's healthcare summit on Thursday. 'When we had our conversation last year, I said this is what I would be most worried about. I'm so sorry that it occurred, and occurred so quickly after that interview… Fauci is not the only one who's been raising this kind of alarm. **Bill Gates** has similarly said that the world needs to **prepare for pandemic** disease outbreaks in the same serious way **as armies prepare for war'**… 'Even as we're getting through this, **and there'll be many, many lessons learned**, we've got to for the future, **make sure that we don't lose this corporate memory** of what we're going through because we need, obviously, to be better prepared… You don't want to frighten society and say, **'At any given moment, something is going to come in and destroy society'** Because when you hear that over and over again ... people get inured to that, and they say, 'Well, you're just trying to frighten us,' **Fauci said last year [2019].** 'The way you prepare for an outbreak is to preemptively put in place the scientific and public-health capabilities to respond. Don't try to guess what the next outbreak is because you're **almost always gonna guess wrong**. Try to put a fundamental system in place of **surveillance**.'"[267]

Lessons Learned

When the negative results of wargames recreated are in the real world, they are portrayed to the public conciliatorily as unprecipitated events which can still provide "lessons learned". The specific rhetoric "lessons learned" is indicative of a deliberate process used in the intel-security industry to create trillion-dollar research and development funding opportunities out of disasters planned and executed by the same industry.

---

[265] "The Event 201 scenario". http://www.centerforhealthsecurity.org/event201/scenario.html
[266] https://twitter.com/stevewoz/status/1234575727678435328
[267] Brueck, Hilary. "Dr. Fauci said he's 'so sorry' the worst-nightmare pandemic scenario he outlined a year ago has become reality". *Business Insider*. 9 July 2020.

[TOPIC- The negative results replicated from wargames. This topic is also addressed in the section Research and Arrested Development]

+ADD "In effect, the small nation is using its own and neighboring countries' cities and population as hostages to deter the Soviet reluctance to destroy these nonmilitary targets. While the policy may be effective, it still has a superficial absurdity and callousness about it which may reflect an inherent weakness that will show up in a crisis."[268]

+ADD "Even if the U.S. did not retaliate instantly against the Soviets as a result of a major Soviet provocation in Europe, the Soviets would still have to envision the Americans evacuating their cities (even against the will of the American government), putting their strategic forces on extreme alert, and probably taking various kinds of limited measures which could easily escalate."[269]

+ADD purpose of American intervention in Europe for arms race: "There are also dangers in **having 'independent' European deterrents**, one of which is that they would encourage the growth of a Finite Deterrent philosophy in the United States, **making the American SAC much harder to trigger.** They many also **discourage the NATO countries from procuring adequate conventional forces.** Another possible weakness is the creating of opportunities for the Soviet to **act as agents provocateurs**. Another problem – **particularly if the independent deterrents are national rather than NATO – is the subsequent pressure toward the diffusion of nuclear weapons systems everywhere and the corresponding Nth-country problems**. The most exciting **developments of World War VI will have occurred in the new missiles and satellites first seen in World War V**. In addition to the military program, missiles and satellites will be widely used in **scientific research**."[270]

"Project Lincolnia Assessment" by Mike Hammon, Research Fellow at Potomac Institute for Policy Studies: "Project Lincolnia I was the first of a series of war games that had the object of testing: The Department of Defense's (DoD) capability to manage urban combat operations, The interoperability of the DoD with other executive branch agencies; Advanced technologies that might be applicable to the urban warfare venue." … "The Lincolnia I scenario centered on the collapse of a failed Persian Gulf island archipelago nation-state named Nicholesia. Nicholesia's government; weak, plagued by warring factions, unable to support its own citizen's welfare, and corrupted by a powerful drug cartel; requested UN assistance. That international body in turn asked for a U.S.-led multinational force (MNF) to stabilize the situation and proved security for international relief agencies already present and providing services. This scenario was designed to facilitate joint, multinational, and interagency planning at all three levels of war: the strategic, operational, and tactical."[271] Whether it be codenamed *Nicholesia*, N-th Country, or something more conspicuous like *Nahrain*, the exercise obviously refers to Bahrain as it is the only island archipelago nation in the Persian Gulf.

+ADD In March 2011 the GCC intervened in the Bahrain crisis that resulted from the Arab Spring. https://www.nytimes.com/2011/03/15/world/middleeast/15bahrain.html?_r=1&hp ; https://www.washingtoninstitute.org/policy-analysis/view/bahrains-crisis-saudi-forces-intervene ; https://www.bbc.com/news/world-middle-east-12729786

---

[268] Kahn, P 477

[269] Kahn, p. 478.

[270] Kahn, p. 478.

[271] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 22.

The *Lincolnia I* wargame is described as a "political-military strategy game" and a "tactical game with on-the-ground advanced technology experiments," including "reconnaissance, surveillance and target acquisition (RSTA) cloud" and "non-lethal directed energy weapons". The exercise included "notional forces" of narcotics traffickers and paramilitary ethnic militias "designed to replicate the Tamil Tigers, Sierra Leone's Revolutionary United Front, and the Hezbollah." One of the training grounds for the *Lincolnia I* exercise is named "Yodaville," a reference to a telekinetic supernatural character from the movies *Star Wars*. Star Wars is also the popular name given to the US nuclear weapons Strategic Defense Initiative (SDI).[272]

Playing all roles in the scenario, US forces allegedly learned to counter **but also practice, as the Red Team, producing "difficult civil issues such as children being killed by terrorists, religious leaders protesting government policies, and breakdowns in the humanitarian aid delivery process.** The JTF commander had to operate within the terms of the political-military plan and the agreement negotiated in the strategy-policy game."[273]

In the wargame scenario that would take place later on September 11, 2001, decision-makers would also be restricted by wargame terms and agreements while an actual attack took place which killed thousands, destroyed a major urban area of the US, and initiated a twenty year-long war in Afghanistan. Those playing the wargame during the 9/11 terrorist attack would be called to testify before Congress and an extensive investigation would take place known now as the 9/11 Commission Report. Self-feeding by the DoD through the "political-military strategy game" is detailed further in the section Recent Developments and Research and Development. ."

" 'One major issue is the lack of publicly available data to measure progress, as well as a system that has led government agencies and other organizations to fudge statistics to make themselves look better… "**First they classified the data, then they stopped reporting it**," he said. "**You as members of Congress have no public metrics to rate the billions of dollars we are spending in Afghanistan'**… 'Despite the U.S. Air Force doing 'a wonderful job' working with their Afghan counterparts, the Afghan military and police have been a 'hopeless nightmare and a disaster'… **'As much as you hate the Taliban, and I do, to the average Afghan it's better than the justice provided by the national unity government.**'," **John Sopko, Special Inspector General for Afghanistan Reconstruction said before the House Foreign Affairs Committee hearing held January 16, 2020**.[274]

Because the US created and armed the Taliban as the *mujahidin*, it is a suggestion that the Cold War US-created militia is preferable to the current US-sponsored Afghan government. This is a fine example of wargaming logic in real situations – the US plays against the multiple versions of itself it has trained. It is an endorsement for the US Air Force deployment of aerial weaponry and its proliferation among forces of a highly unstable nation.

It is also a call for more research and development – part of the $133 billion dollars lamented already spent on the Afghan War. Inevitably, this recent 'embarrassing' development before the House and public will result in more demand for research and development to respond

---

[272] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 23.

[273] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 24.

[274] Blitzer, Ronn. "" https://www.foxnews.com/politics/afghanistan-watchdog-testimony

to the embarrassing testimony. This exemplifies one part of the entropic mechanism at work detailed in the final section Research and Arrested Development.

Pointed out in *Lincolnia I* wargame results analysis that "Strategy-policy participants established Humanitarian and Security Committees."[275] … *Lincolnia I*'s result analysis includes recommendations that prepare the wargame industry for *MC'02* by recommending, "There is a need to incorporate weapons of mass destruction (WMD) considerations in future Project Lincolnia exercises." (p 26). One year after the publication of this presentation, the US invaded Iraq on the premise of Saddam Hussein concealing WMDs.

While the *Lincolnia I* wargame report found that, "NGOs were a vital link in determining militia group motivations and behaviors. Increased contact and better management of military-NGO interactions is highly recommended,"[276] the US government and NGOs repeatedly deny fomenting revolt through deliberate coordination. These are the exact court claims made by the Egyptian government before and still concerning the Arab Spring. The same accusations against US NGOs is being made now by the government of Hong Kong concerning protests there as well. This is despite drilling for NGO-US military coordination in situations of revolt and recommending increased coordination in published policy.

"In the tactical game/experiment, Project Lincolnia I sought to gather data on applications for, the potential value of, and the strategic implications involved in applying new technologies during urban stability missions. In particular, air and ground robotic, directed energy non-lethal, and thermobaric capabilities were either tested, of simulated at Quantico and George AFB [Air Force Base]."[277] [move to hacker's arsenal] "Information and direction were passed between the two locations by phone and computer, simulating the radio communications to be found during an actual operation."[278]

"Factions and narcotics cartel unexpectedly formed alliances. On the other hand, friendly force internal cooperation was found wanting… Drug cartel and paramilitary forces remained active, as did humanitarian aid organizations."[279] [cite about Intro]

The 9/11 Commission Report: "To be dangerous, an enemy had to muster large armies. Threats emerged slowly, often visibly, as weapons were forged, armies conscripted, and units trained and moved into place. Because large states were more powerful, they also had more to lose. They could be deterred… Now threats can emerge quickly. An organization like al Qaeda,

---

[275] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 25.

[276] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 26.

[277] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 24.

[278] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 25.

[279] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 25.

headquartered in a country on the other side of the earth, **in a region so poor that electricity or telephones were scarce, could nonetheless scheme to wield weapons of unprecedented destructive power in the largest cities of the United States**. In this sense, 9/11 has taught us that terrorism against American interests 'over there' should be regarded just as we regard terrorism against America 'over here.' In this same sense, **the American homeland is the planet**." … "Our enemy is twofold: al Qaeda, a stateless network of terrorists that struck us on 9/11; and a radical ideological movement in the Islamic world, inspired in part by al Qaeda, which has spawned terrorist groups and violence across the globe. The first enemy is weakened, but continues to pose a grave threat. **The second enemy is gathering, and will menace Americans and American interests long after Usama Bin Ladin and his cohorts are killed or captured."**[280] In this sense, the 9/11 Commission Report is a wargaming scenario… [add more here]

Buck Kernan summarized a 2002 wargame *The Millennium Challenge* as "the key to military transformation." RAND analyst Micah Zenko describes the wargame which leaked 13 years later:

> The featured activity of MC '02 would be a red team war-game simulation. The hypothetical joint experiment would feature an anti-access, area-denial scenario that was situated in the world of 2007, pitting a U.S. blue team of 350 personnel led by Army Lt. Gen. B. B. Bell against an OPFOR of 90 personnel modeling an adversary, and initially led by Van Riper. Kernan personally selected Van Riper to lead the OPFOR, believing that, since he was a 'devious sort of guy' and 'a no-nonsense solid professional warfighter,' he was the best possible candidate. The OPFOR, widely understood to represent Iraq or Iran's military, had a carefully prepared campaign plan, for which the ultimate objective was to preserve the red team's ruling regime and reduce the presence of blue forces in the region. The blue team also had a campaign plan, which included securing shipping lanes, eliminating the OPFOR's weapons of mass destruction facilities, and compelling the red ruling regime to abandon its goal of regional hegemony. To most participants, MC '02 resembled much of the 'Running Start' plan that U.S. Central Command (CENTCOM) planners were developing and refining in the summer of 2002 to disarm Saddam Hussein and remove him from power.[281]

This is what occurred one year later in the 2003 invasion of Iraq. And CENTCOM, the reader will recall from the National Intelligence Council *Global Trends* report, experiences its own scenarioed bombing by 2025 following the proliferation of limited warfare directed nuclear weaponry. New York City, the reader will recall from the JLASS-SP 2016 wargame, alos experiences a scenarioed attack by 2025 on the Lincoln Tunnel (?), that, along with a Christmas Eve bombing of a Canadian Embassy in Mauritania, provokes the US into a more publicized war in West Africa.

One year before *MC '02*, JFCOM ran another wargame on a fictitious landlocked Central Asian country. On this occasion, the wargame was called *Unified Vision 2001*. A US military commander again played the role of the enemy power. (+ADD description of *UF '01*) …When

---

[280] https://govinfo.library.unt.edu/911/report/911Report_Ch12.htm

[281] Zenko, Micah. "Millennium Challenge: the real story of a corrupted military exercise and its legacy". *War on the Rocks.* 5 November 2015.

the commander argued against (whose?) reports to Congress on the effectiveness of the exercise, that "it was simply assumed that in the future the United States would have the real-time radar and sensor capabilities to eliminate them [fictitious underground ballistics in the fictitious landlocked country], and not actually demonstrated by the exercise, "he was promised, regarding MC '02, that 'next year will be a free play and honest exercise.'" [282] [rewrite – confusing]

Following the May 2001 *UF* wargame and the September 11th 2001 attacks on New York City and the Pentagon, the US found itself provoked into a war in Afghanistan, bombing alleged subterranean ballistic and terrorist hideouts. It should be noted here that several wargames were also being conducted on September 11, 2001, which involved preprogrammed false flags in aerial radar and a handover of air traffic control from military-controlled NORAD to civilian-led FAA.[283]

+ADD Hypergame discussion here. https://www.hindawi.com/journals/gt/2015/570639/

The ROSCA economic model used by Marcus Jacob and Marcel Tyrell in "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany" expands on hypergame theory to address the effects of state surveillance and observable corruption on socioeconomics and on the merit of other so-called 'reciprocity games':

> We build our model applying a similar prior updating and transmission setup as Guiso, Sapienza, and Zingales (2008), but use the formal mechanisms underlying **Rotating Credit and Savings Associations (Roscas) to simulate social and economic interaction as a 'reciprocity game'**. This allows us to adequately **capture the disproportionally negative effect of informer activity on the level of trust and scope of cooperation within a society**. Generalized reciprocity, so Putnam (2000) reminds us, is the touchstone of social capital. Our interpretation of such reciprocity games therefore is one of a set of explicit, carefully delineated and concrete practices of mobilization and exchange of labor, of capital, and of consumption goods in every aspect of life. [Footnote: Recall, for example, that in every apartment building at least one informer served as a watchdog and reported all activities to the Stasi.] **Clearly, reciprocity games as they are laid out above require trust and cooperativeness among their members,** for there is a strong economic rationale for each receiver to default after receiving the pot. The fact that in such reciprocity games a certain share of defecting members has a disproportionately negative effect on overall economic outcomes is also an essential characteristic of an informer society. To our knowledge, **the transfer and application of formal Rosca mechanisms to the study of large scale intrusion of people's private lives and its effects on the intergenerational transmission of priors about cooperativeness and the scope of cooperation in a society** is novel in the literature.[284]

And as a RAND wargame analyst writes:

---

[282] Zenko, Micah. "Millennium Challenge: the real story of a corrupted military exercise and its legacy". *War on the Rocks.* 5 November 2015.

[283] "Fiscal Year 2006 Defense Budget". 10 March 2005. *C-SPAN*.

[284] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010, p. 8-9.

> For decisionmakers with limited wargaming experience, this can be a daunting challenge. Wargames can be deceptively simple — many do not even use complicated computer models — so it is all too easy to assume that no specialized skills are needed for success. At the same time, wargames are hugely diverse: interagency decision-making seminars that involve conflict without fighting, crisis simulations adjudicated by subject matter experts, and operational warfare in which outcomes are determined by complex computer models.[285]

The Millennium Challenge was indeed highly detailed, with Van Riper enacting the "Red" position that Hussein's Iraq would soon find itself living:

> Hostile fire against the V-22s or blue's [US] C-130 troop transport planes was forbidden. The white cell [command center] also directed the chief of staff that the red team had to position its air defense assets out in the open so the blue forces could easily destroy them. Even after some were not destroyed, the red team was forbidden to fire upon blue forces as they conducted a live airborne drop. Van Riper asked the white cell if his forces could at least deploy the chemical weapons that he possessed, but he was again denied. Van Riper was furious. Not only had the white cell's instructions compromised the integrity of the entire process, but also his own chief of staff — a retired Army colonel — was receiving conflicting orders about how his force should be deployed. When Van Riper went to Kernan [who?] to complain, he was told: 'You are playing out of character. The OPFOR would never have done what you did.'... Six days into the exercise, he stepped down as commander and served as an advisor for the remaining 17 days. During that time, the blue team achieved most of its campaign plan objectives by destroying the OPFOR air and naval forces, securing the shipping lanes, and capturing or neutralizing the red regime's WMD assets. The OPFOR was capable of partially preserving the red regime, but it was substantially weakened and its regional influence was much diminished.[286]

Van Riper's complaint on the exercise that would become the model of the 2003 Iraq War alleged that:

> the exercise could lead the Pentagon to have misplaced confidence in still-untested military war-fighting concepts... Van Riper believed that MC '02 was both scripted and carried out in a way that did not realistically reflect likely future U.S. military capabilities or the threats posed by a thinking, motivated adversary. As he recalled: 'War-gaming is not normally corrupted, but this whole thing was prostituted; it was a sham intended to prove what they wanted to prove.'

Despite his attempt to keep the failure of the wargame and his grievances confidential, "Van Riper's e-mail was immediately leaked to the *Army Times (find article?)*, which published a comprehensive account: 'Fixed war games? General says Millennium Challenge 02 was 'scripted.'" This predictably resulted in a scandal over military waste on the $250 million exercise. U.S. Joint Forces Command (JFCOM) in charge of conducting the

---

[285] https://www.rand.org/blog/2016/01/getting-the-most-out-of-your-wargame-practical-advice.html

[286] Zenko, Micah. "Millennium Challenge: the real story of a corrupted military exercise and its legacy". *War on the Rocks.* 5 November 2015.

wargames was dissolved years later, just one month before the NATO attack on Libya in 2011.[287]

Consider the behavior of Iraq's political leadership and intel-security around the time of the US invasion: (+ADD here Uday Hussein AP reference)

> From 2003 to 2006 there was a lot of American reporting claiming that Saddam Hussein had planned to continue on the fight with the U.S. after he was deposed. An early example of this was a July 2003 article in ***Newsweek*** **that claimed to have found an order from the Iraqi intelligence service, the Mukhabarat [Intelligence] to conduct looting after the invasion. It also instructed agents to attack power plants, assassinate clerics, and create general chaos.** The magazine thought this was **a proof that Saddam gave orders to create the insurgency,** although it noted the document had not been verified. The magazine wrote another piece in October 2004 that quoted some analysts who believed that **Saddam planned the insurgency before the invasion**. That same month, the final findings of the Iraq Survey Group were released, which said that Saddam decided to continue the fight after his regime fell. It used as evidence the fact that **the Iraqi army had dispersed weapons throughout the countryside from April 2002 to January 2003**. Two months later, *U.S. News & World Report* claimed that U.S. intelligence reports pointed to the same thing. It cited a fall **2002 report by <u>the Pentagon's Combined Joint Special Operations Task Force that said Saddam ordered 1,000-1,200 officers of the Mukhabarat, Directorate of Military Intelligence, and Directorate of General Security to go for irregular warfare training</u>.** On December 3, **2004, a Defense Intelligence Agency (DIA) assessment said that** Saddam planned to continue the fight after the invasion, and that was why former elements of the regime such as **the Saddam Fedayeen, the Mukhabarat, the Special Security Organization, the Special Republican Guard, and former Baath Party members were responsible for the majority of attacks in the country**. In February 2005, *Newsweek* ran another story on how **Saddam hid millions of dollars and arms throughout the country to prepare for a guerrilla war.** It claimed that on July 2002 <u>Saddam **issued a directive to his forces to drag America into irregular fighting.**</u> That was followed by a January **2003 order to sow chaos after the invasion by destroying infrastructure and looting government offices**. In September 2005, there was a story in *Time* that claimed in April 2003 **Saddam met with his Vice President** Izzat Ibrahim al-Duri, Muhammad Yunis al-Ahmed, a senior member of **the Military Bureau**, and members of **the Mukhabarat** in Baghdad, and **told them to organize their followers to resist** the Americans. U.S. intelligence then hypothesized that Saddam, through **his Military Bureau began organizing these cells to fund and supply insurgents.** It was probably no coincidence that Duri and Ahmed **became two competing leaders of the Baath Party in exile after the overthrow of Saddam, and led Iraqi militant groups from Syria."**[288] Opening borders for conflict, ISIS

+ADD new wargame 2020 here. http://infobrics.org/post/30229/

Past is Prologue

[287] Ukman, Jason. "U.S. Joint Forces Command formally dissolved". *The Washington Post.* 4 August 2011.
[288] Wing, Joel. "Did Saddam Plan The Insurgency In Iraq?" *Musings On Iraq*. 26 February 2011.

The failure of scenarios and wargaming to be applied as a preventative strategic-tactical measure against devastating developments deprives the practice of credibility. This extends to fields of research and development. Instances are discussed in which analysts accurately predict the past (termed "hypothetical past" in analysis reports), revealing a process in which foreknowledge of damaging events may be admitted *post facto* for profit. In short, this process allows analysts to recycle scenarios and wargame plots as analysis.

In October 2016, the RAND Corporation published a video titled "What Would Happen if Russia Invaded the Baltics?". The wargame scenarioed that NATO forces were swiftly destroyed by Russian ground and air forces - on RAND's tabletop boardgame, anyway.

Exactly one year later, in October 2017, HBO's *VICE News* aired a segment titled "Russia's Giant Military Exercise Wasn't a Cover For War After All", which featured an enormous wargame of 100,000 personnel staged in far western Russia and overseen onsite (and through video monitor) by Vladimir Putin himself.

Two years after RAND's ponderings over an imaginary Russian-Baltic invasion and one year after Russia staged the world's largest wargame on the border with Europe, Radio Free Europe/Radio Liberty issued a news video in October 2018 titled "NATO Stages Biggest War Games Since Cold War", featuring footage of NATO allies wargaming in Eastern Europe and over the Baltic Sea. NATO's spokespeople in the media piece speculate on what Russia's response would be to the 'biggest war game', as they had heard rumors Russia was already planning a response. Radio Free commentators ignore that NATO's 2018 wargame was likely a response to Russia's wargame a year earlier in 2017, which was likely prompted by RAND's 2016 boardgame version of the wargame of the imaginary war decisively lost already a year earlier than that. These news media pieces can all be found in the first page results of one YouTube search query "rand wargames wwiii".

In *On Thermonuclear War*, published in 1958, Herman Kahn writes "the hypothetical past" of WWIII. Despite that fact that Kahn began his professional career in 1945 at CalTech and assumed his first position at RAND in 1948, Kahn reimagines past policy he actually created in this chapter, although as one can see, it precisely describes the Cold War era. In other words, according to RAND, World War III occurred in 1951.

Defined as the "startling political change of 1951[,] the emergence of Soviet Russia as a great European and Asiatic power", the "most obvious manifestation of this is the creation of the Satellite Empire, the communization of China, and various degrees of major war, civil war, or insurrection in Korea, Indochina, Greece and Iran. A more subtle result of this expansion of Soviet interests is the creation of a bipolar world – a bipolarity which dominates all international relationships…".[289] Whether Kahn was really trying to accurately predict the past (which no doubt is an important skill for analysts), or whether he is bragging about foreknowledge he had

[289] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 417.

post facto and attempting to recycle old wargame plots as analysis for his book, we may never be sure. What we can be sure about is that the 1950s were in fact defined by the rise of Soviet Russia signaled by its achievement in launching the first ever satellite *Sputnik*, and the realignment of Asian geopolitics towards Sovietism fought out through endless proxy wars with the US and Europe. Kahn's particular use of the term 'Satellite Empire' is speculated upon in terms of cyber realism in the section The Satellite Empire. [REWORD above 2 paragraphs]

Kahn, still describing his present time as if he were speaking from the past, continues in the future tense:

> There are uncommitted nations who will be known in a few years (with some exaggeration) as the 'uncommitted billion,' but on the whole most people know in 1951 whose side they are on. This known and relatively stable line-up simplifies military planning, at least for the all-out war.

Such a simplified set up of two-sided conflict lends itself to wargaming, which involves only two (red and blue) teams. This bipolarity was also opportune because wargaming had just been adopted by RAND in the late 1940s to mid-1950s.

Kahn continues: "Despite the Soviet A-bomb and the approaching balance of terror, almost no one is thinking about the *concept* of limited war…".[290] While many would describe it as political bipolarity, 'approaching balance of terror' does gel better with our current geopolitical language, though it was not yet used outside of nuclear arms race terms in 1958 when Kahn published.

+ADD **"The current 'balance of terror' can be looked upon as an intensification of the balance-of-power system. It will be recalled that before World War I the 'balance of power' was supposed to make war unprofitable**, or at least so risky that a potential aggressor would choose compromise to risking all. The problem is increased today because over a period of time the successful working of such a system tends to create instabilities. This complex problem, which I have called the '1871-1914' problem, is summarized briefly on pages 368 to 370, where the following analogies between 1914 and 196X are discussed: 1. Pre-emption important (First Strike similar to mobilization); 2. Need for quick victory; 3. War planning both rigid and narrowly professional; 4. Tendency to excessively firm positions in a crisis; **5. Increasingly widespread ignorance of the technical side of war;** 6. Crises tend to induce excessive physical and mental strain in crucial individuals; 7. Small powers can manipulate the rivalry of large powers. The ultimate solution to the Armageddon, Camlan, and 1871-1914 problems is some form of arms control and rule of law, possibly under a world government."[291]

+ADD Hypergame discussion here.

Technological plots and withholding info even from outside experts + "The year 1951 is an especially good year to examine how the rapidity of the technological revolutions creates difficulties for both the Soviets and us in evaluating the impact and significance of the new developments. This postulated World War III is far enough past World War II to illustrate how spectacularly technology can change in five to six years. Yet enough time has passed so that one

---

[290] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 417-18.
[291] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 526-527.

can claim to have developed some understanding of its problems."[292] + "There is still much talk about the scarcity of uranium – a view which is reinforced by most of the technical people. Few people in or out of government think that the atom bomb will soon be plentiful; **nobody realizes that practical and convenient thermonuclear bombs will be available before long. But a few people with high security clearances know** that some work on a rather impractical thermonuclear device is going forward. Though there is some discussion in 1951 about 'baby atom bombs,' that is bombs about the same power as the Hiroshima and Nagasaki bombs but much smaller in both weight and size, **not even the experts have any idea of the flexibility, efficiency, and economy soon to be available in the atomic weapons arsenal…This overvaluation** of bombs as being too precious to use on most military targets affects defense planning in our Zone of the Interior. Because of the threats of Soviet attacks, the Air Defense Command and the associated Army Anti-Aircraft Command is set up in Colorado Springs in 1951, **but they think of their highest priority job as defending the large cities and nuclear facilities,** and the initial deployment of their forces (radars and fighters) almost **ignores warning and defense for SAC in the contingency of a surprise attack directed at SAC and not the cities."[293]** +ADD JLASSP 2016 wargame attack on CENTCOM
+ Mockingly, Kahn writes *post facto* on dangerous oversights that occurred during a time in which he was already in a position to cause such mistakes himself along with the complicity of colleagues like Air Force General and RAND founder LeMay: "It should be quite clear from even the above superficial discussion that any arms control system set up in 1951 might easily have been based upon some serious misunderstandings of the implications of the then current technology and even more serious misunderstandings of the future. In particular some kinds of inspection schemes might have resulted in making our vulnerabilities both crystal clear and very tempting to Stalin or some of his military advisors. **Even forcing the Soviets to go through the intellectual exercise of thinking these problems through could have been dangerous. Before** we could have safely started discussion of 'the control of surprise attack' **we would have had to fix up the gaps in our posture – that is, had a limited rearmament program."[294]** +ADD Hypergame theory is used to manipulate funding research and development cycles. This is discussed more extensively in the section Recent Developments and Research and Development. +ADD Lack of control of the surprise attack is, in Kahn's own words, due in part to nefarious wargame exercises.

[TOPIC –wording similar to scenarios, scenario recycled as analysis]

"**—and it's going to end with** lots of people losing incredible amounts of money… To see how the whole thing went down, **imagine** a kind of misshapen nesting-doll set with **four characters:** GameStop, hedge funders, Reddit traders, and zillions of retail investors. At the center is GameStop, which is not a great company. In 2019, the strip-mall fixture lost almost $500

[292] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 4-17-18.
[293] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 420.
[294] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 425.

million. **In 2020, a pandemic** forcibly shut down many of its stores and gutted its revenue… GameStop was one of the more popular targets of these **hero-villains**… **This perfect storm was created by** the collision of **a tantalizing morality play** (Reddit Degenerates versus Wall Street Suits) and an age of commission-free trades **on popular platforms** such as Robinhood, which have converted the raw material of pandemic boredom into a juggernaut of **speculation**. Given the monstrous amounts of **money at play**, several large institutional investors—rival hedge funds, private-equity firms, billionaire tourist dollars—**seem to have jumped in as well, scrambling the most simplistic David-versus-Goliath narratives**. And America's investor underdogs **might already have lost the war** as the stock price ticks down. **This populist revolt could reveal itself** to be a disastrous bubble that offers and then quickly extinguishes **the idyllic dream of democratized finance**. [FAR-REACHING SPECULATIVE POLITICAL ANALYSIS] Breaking down the **GameStop saga into these four components**—the company, the short, the Reddit **army**, and **the ensuing** FOMO [fear of missing out] **mania**—is useful because this helps us disentangle **the parts of the story that are surprisingly traditional from the parts that are actually surprising**… You can despise **the Capitol siege of January 6** (I do) **and** adore **the GameStop surge of January 26** (I'm undecided), but still **see something in common: two anti-institutional plots conceived in online message boards, amplified on broader platforms such as YouTube, and actualized, chaotically, in the real world…** Perhaps all we'll remember from the past week is that a few hedge funds' greedy doltishness accidentally helped mint some Robinhood millionaires, while a bunch of latecomers set their money on fire for **lolz.** But **something tells me that we're at the dawn of something stranger.** For a week, takes have flown wildly around the internet that **tried to capture this saga in a tweet.** The **investor and former Trump White House communications director Anthony Scaramucci compared what we're seeing now to the "French Revolution of finance," with an army** of scrappy traders engaged in **a moral uprising.** [FAR-REACHING SPECULATIVE POLITICAL ANALYSIS]"[295]

The Spectacular Security State

It is also conceivable that he never appeared, that someone decided fiction had gone dangerously far and withdrew the article.
Alfred L. Jenkins, *National Security Files: China Memos*, Vol. VI (August 11, 1966)

[find 'glued to the tv like everybody else' quote by Cheney on Hurricane Katrina]

This section discusses the role of spectacle, media, and fiction in the intel-security state. I divide these into uses of speculative fiction and media spectacle.

The subsection Media Spectacle focuses on the misappropriation of surveillance technology as a tool for media production. This includes the *spectacularization* of real-world events under surveillance for the purpose of creating policy change, along the lines of the CNN effect. It also includes the *fictionalization* of real-world events under surveillance for the purpose of deception operations and financial exploitation, in which real surveillance operations are portrayed as

[295] Thompson, Derek. "The Whole Messy, Ridiculous GameStop Saga in One Sentence". *The Atlantic*. 5 February 2021.

entertainment media. I argue that policy motives, deception operations, and financial exploitation encourage the extension of unnecessary and transgressive surveillance.

"**The cornerstone of any deception operation is the deception story. The deception story is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception.** It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe to be the true situation, then decide and act on that basis. In other words, the deception story parallels what the deception would want the opponent's intelligence estimate to say about your own commander's intentions and your own unit's actions. The deception story identifies those friendly actions, both real and simulated, that when observed by the deception target will lead it to develop the desired perception. Deception story development is both an analytic and creative process that involves a variety of information on enemy data acquisition and processing. An exact understanding of the perceptions and observables required for the deception provides a concrete basis for crafting the deception story. The deception story weaves these elements together into a coherent depiction of the situation the target will reconstruct from the information provided. Ideally, the deception planner wants the deception story to be the exact mental picture of the target forms as the deception unfolds. **The deception story should read like the adversary's own intelligence estimate.** The deception story is, in effect, the equivalent of a completed puzzle. As such, it serves as a means of checking the logic and consistency of the internal elements of the deception. This allows the deception planner to identify desired perceptions, observables, and executions that may need refinement, and to add supporting observables as needed to strengthen certain elements of the deception story or diminish the impact of troublesome competing observables. Each element of the deception story should have associated deception means that can credibly portray the data, plus identified conduits that transfer this information into the enemy's information processing system. Unavoidably, various nodes in this line of communications also become filters of the information conveyed, allowing the target to introduce their own predispositions and biases that the MILDEC planner must anticipate. As the story is developed and elaborated, the MILDEC planner continuously monitors changes in the situation and validates the deception story against other friendly plans and/or actions. b. The story should be believable, verifiable, consistent, and executable. (1) Believable. The story must correspond to the deception target's perceptions of the friendly force's mission, intentions, and capabilities. (2) Verifiable. The adversary should be able to verify the veracity of the deception story through multiple channels and conduits. The deception story, therefore, takes into account all of the adversary's intelligence sources and is made available through all or many of those sources. (3) Consistent. Deception stories should be consistent with the deception target's understanding of actual friendly doctrine, historical force employment, campaign strategy, battlefield tactics, and the current operational situation. This calls for the MILDEC planner to have as complete a picture as possible of the deception target's level of knowledge and belief in these areas. (4) Executable. As with any course of action (COA), the MILDEC option that forms the deception story should be within the capabilities of the friendly force as the deception target perceives it. The deception target must believe that the friendly force has the capability to execute the operations that are being portrayed by the deception story."[296]

[296] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-5 – I-6.

"The Kosovo conflict looked and sounded like a war: jets took off, buildings were destroyed and people died. For the civilians and soldiers killed in air strikes and the Kosovar Albanians murdered by Serbian police and paramilitaries the war was as real – and as fraught with horror – as war can be. **For the citizens of the NATO countries, on the other hand, the war was virtual. They were mobilized, not as combatants but as spectators. The war was a spectacle: it aroused emotions in the intense but shallow way that sports do.** The events in question were as remote from their essential concerns as a football game, and even though the game was in deadly earnest, the deaths were mostly hidden, and above all, they were someone else's… But war without death – to our side – is war that ceases to be fully real to us: virtual war."[297]

+ADD "There are a lot of lessons we want to learn out of this process in terms of what works. I think we are in fact on our way to getting on top of the whole Katrina exercise."
Vice-President Dick Cheney, Sept. 10, 2005

"And in all fairness to the Department of Homeland Security right now, I mean this is a brand new Department that was formed after 9/11. In many ways this is a 'learn by our mistakes and figure out what to do better' type of scenario."
CNN Reporter Kyra Phillips, Sept. 9, 2005

Dr. Timothy Melley, Director of the Humanities Center at Miami University, writes in *The Covert Sphere: Secrecy, Fiction, and the National Security State* (2012): "The Covert Sphere pursues these questions through the cultural history of the Cold War and the War on Terror. My central claim is that the development of **the National Security State, with its emphasis on secrecy and deception, helped transform the cultural status of fiction as it relates to discourses of "fact," such as journalism and history.** As **state secrecy shifted the conditions of public knowledge, certain forms of fiction became crucial in helping Americans imagine, or fantasize about, U.S. foreign policy.** This transformation had a **powerful role in fostering the forms of suspicion, skepticism, and uncertainty** that would eventually find their fullest expression in postmodernism."[298] [Relate to Hazelwood's profile on the role of fantasy in deviant criminality. The fantasy 'fictions' of state secrecy consistently relate to organized deviant crime, in the intel-security state referred to as 'state secrets', the violence and infringement which only the State holds the monopoly to exercise.] ;
"George Kennan—head of the State Department's Policy Planning Staff, former chargé d'affaires at the U.S. Embassy in Moscow, and arguably the chief architect of the Cold War—insisted that the United States embrace 'covert political warfare' and 'propaganda as a major weapon of policy.' Although Kennan claimed he was promoting 'organized public support of resistance to tyranny in foreign countries,' he secretly crafted NSC-10/2, which transformed the CIA from an intelligence gathering agency to an operational outfit with a charter to engage in 'propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-Communist elements in threatened countries of the free world.' More important,

[297] Ignatieff, Michael. *Virtual War: Kosovo and Beyond.* Metropolitan Books. 2000, p. 3-5.
[298] Melley, Timothy. *The Covert Sphere : Secrecy, Fiction, and the National Security State*. Cornell University Press. 2012, viii.

NSC-10/2 specified that such actions must be carried out so that 'if uncovered the U.S. Government can plausibly disclaim any responsibility for them.' When President Truman signed this directive on June 18, 1948, he institutionalized not simply secret warfare but also public deception as a fundamental element of U.S. policy… NSC-68 ensured that what first seemed a minor exception to democratic oversight would eventually become a major basis for U.S. foreign policy. The scale of psychological operations in the early Cold War so overwhelmed the CIA that Truman was forced to create a Psychological Strategy Board packed with public relations and advertising executives."[299]

+ADD "In India, the phrase **'fake encounter'** refers to the extrajudicial killing of a civilian followed by the official claim that the victim was a Pakistani infiltrator killed in a legitimate military encounter with police or army forces. This article explores the widespread pattern of fake encounters in Kashmir Valley in order to shed light on **the processes through which violence and terror become fictionalized and fantastic**, with Kashmiri bodies gaining a heightened visibility in a falsified form within **a cultural imaginary of national security interests** and public safety concerns. Identifying Kashmir Valley as a state of exception, I examine how the suspension of the rule of law gives rise to new agents and hierarchies of power and authority and new patterns of criminalization and paramilitarization throughout Kashmiri society. I also consider how the **informalized practices of forced disappearance, fictionalized terror, and impunity for violence** are produced and reproduced through the **strategic manufacturing of public consent for violence** against Kashmiris throughout Indian society at large."[300]

+ examples of Chalmers book review critique of RAND as hyper-numerical[301] from *Gaming the System: Nine Games to Teach American Government through Active Learning* (2020) by Cohen (Asst. Professor of Political Science at Clarkson University), Alden (public school social studies teacher), and Ring (lecturer in global security/political science at the Baker Center for Public Policy): counting slaves as half a person as scores .33 of one point with breakdown of calculation (lesson on US Constitution Chapter 3[302]), chapter titles "Hard Won Equality: A Game About Social Movements", "The Tragedy of the Lagoon: A Game About Resource Management", "The People Have Spoken: A Game About Interest Groups and Messaging", "SMO-Specific Actions: Two SMOs [social movement organizations]– Radicals and Religious Organizations – each have unique actions that only they can take. These are defined below. The other two SMOs enjoy different advantages – Students can take fifteen actions instead of ten, and Moderates have access to all three of the different scoring actions. The two SMO-specific actions are: God's Glory: Available to Religious Organizations. Religious Organizations have natural followers throughout key positions in the media, government, and other important sectors of society. For an action, Religious Organizations can increase their Prestige by .25. Violent Infiltration: Available to Radicals. Frustrated that their demands are not met, Radicals can infiltrate an event held by another SMO and initiate violent protest. As a result, leaders and the general public often

---

[299] Melley, Timothy. *The Covert Sphere : Secrecy, Fiction, and the National Security State*. Cornell University Press. 2012, p. 3-4

[300] https://www.tandfonline.com/doi/abs/10.1080/09502380903221117 [PRINTED]

[301] Johnson, Chalmers. "A Litany of Horrors: America's University of Imperialism". *Tomgram: Chalmers Johnson, Teaching Imperialism 101*. TomDispatch. 29 April 2008.

[302] *Gaming the System: Nine Games to Teach American Government through Active Learning* P 24-40

misattribute the origins of Radical-led violence and wrongly conclude that other groups may be responsible. For an action, Radicals Steal .25 Prestige from another group and appropriate it for themselves."[303] ;

Wargames are, in part, coordinated by a sector and venue referred to as "The Public Space". Cohen et al. explain usage of The Public Space in the following except from *Gaming The System*:

> While playing your game, be sure to pay attention to the Public Space. The Public Space is utilized in virtually every game as a central place to display and update information relevant to the game. The exact nature of the Public Space will be determined by your instructor: it may be a whiteboard, a projected Excel file, or even something of their creation. No matter its form, though**, the Public Space will contain vital strategic information necessary for you to succeed. Use it to make strategic decisions about your opponents, evaluate your own possible decisions, and try to predict what might happen next**.[304]

In the sections Monopoly on Infringement and The VNN Effect, it is further shown that media are regularly used, without the informed consent of the public, as The Public Space for the manipulative wargaming of real-life situations and crises. That is, what is alleged to be comprehensive coverage of current events, or mere fictional entertainment, is actually used as "a central place to display and update information relevant to the game," meaning the wargame scenarios which the public is non-consensually involved in nearly constantly.

The media are fabricated by an immense systematized industry of speculative fiction writers/producers, including the US military, and portrayed as comprehensive coverage of events in order to solicit 'authentic' responses from unaware consumers. Those decisionmakers are aware of the speculative nature of the media blithely use The Public Space (i.e., public media) to communicate "vital strategic information" to opponents or cohorts, and "to make strategic decisions about [their] opponents" – which they easily could do through direct communication, if not for their fetish for gameplay and their desire to maintain plausible deniability of conspiracy and an inflated wargaming industry.

"In Chapter 2, Signing the Social Contract, you will find yourself in a fictional state of nature and must consider the central question of whether you need a government. Your initial situation is grim and illustrates the distressing conundrums inherent to surviving in an uncertain world. You have to gather enough resources to survive both today and in the future while weighing the merits of going it alone, grouping up, or even stealing from a neighbor. As the rounds of the games progress, you will interact through structured exchanges to advance up the ladder of civilization toward government, but not all like the idea of a sovereign. The winners will be those who gather the most resources, whether under the protection of a state or through the freedom of the state of nature… In this activity, you will play as a person lost and alone in an anarchic setting (meaning there is no government to protect or oppress you). The game might take place long after an apocalypse or long before civilization ever formed. Regardless, your life is hard and lonesome. You struggle to find enough resources to survive, and you are left with hard choices about whether to scavenge, steal from others, or hide what little you have… This struggle is premised on what philosophers call social contract theory. Philosophers like Thomas Hobbes and

---

[303] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 49.

[304] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 5.

John Locke were troubled with the question of why a person should prefer to have a government instead of being without one… In this case, Hobbes and Locke both proposed what we call a 'state of nature,' a fictional setting in which people live with no government whatsoever… Sequence of Play: … 1. Round Start… 2. Actions are Entered… 3. Players Rise… 4. Thieves Select Targets: Players who wish to steal move next to their intended target. They do not have to designate who they will Steal from until this point (all that they have written in their Ledger is 'S'). a. All Thieves raise their hands to indicate that they are Stealing. Thieves may Steal from anyone, including other Thieves. Multiple Thieves may not select the same target. b. A Thief selects a target by walking to a victim and stating, 'I'm stealing from you.' The victims raises both of their hands to indicate they are targeted for Stealing… e. If a Steal action is not Defended against and the victim is not Hiding, both the Thief and the target reveal their Resources to each other… Note that when updating Resource tallies, players watch one another update their tally sheets to ensure that everyone is playing honestly. f. If a Thief targets a Thief who is in turn targeting another Thief, the last Thief to designate a target Steals first. In Figure 2.1 below, Thieves are numbered by the order in which they reached their targets: This 'Thief Chain' would be resolved in the following way…".[305] ;

"[A More Perfect Union] Your goal is to re-sculpt Madison's initial proposal for the Constitution in your favor… The game's winner is the delegation that achieves the most points through seeing your objectives represented in a final ratified document."[306] +ADD from chapter 3;
"Chapter 6 delves into lawmaking. Written by Committee is set in a heated conference committee formed to resolve disagreements between the Senate and House versions of a bill… You will be able to wheel and deal, bribe and spy, and win favor with constituents and interest groups based on what you accomplished in the committee."[307] +ADD from chapter 6;
"The gameplay of Chapter 9's The Tragedy of the Lagoon exemplifies this starkly. In it, you play as lagoon monsters trying to survive, but this premise is almost inconsequential because the struggles that the monsters face are universal and easily applicable to US politics and society."[308] +ADD from chapter 9 ;
One of the nine resources used to create introduction of *Gaming the System: Nine Games to Teach American Government through Active Learning*: "Jefferson, K. (1999). The Bosnian war crimes trial simulation: Teaching students about the fuzziness of world politics and international law. *PS: Political Science and Politics, 32,* 589-592."[309]

+ADD Hypergame – deception.

ADD from *The Spectacular State* book re: Sovietism/glasnost/cold warism?

---

[305] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 5-6; 10-11; 17.
[306] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 6.
[307] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 7.
[308] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 2.
[309] Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020, p. 8.

+ADD here and in Monopoly on Violence, Monopoly on Infringement section, discussion on descriptions/images of Bosnia/Kosovo atrocities from CNN effect in action ch 5 (<p96) "the media during the Kosovo crisis"

[TOPIC - US soldier and agent abuse with use of spectacle]

"Another infamous incident involving the forcible nudity of men is that relating to the treatment of prisoners at Abu Ghraib. The Taguba report found that the intentional abuse of detainees by military police personnel included: … Videotaping and photographing naked male and female detainees; Forcibly arranging detainees in various sexually explicit positions for photographing; Forcing detainees to remove their clothing and keeping them naked for several days at a time; Forcing naked male detainees to wear women's underwear; … Arranging naked male detainees in a pile and then jumping on them; Positioning a naked detainee on a MRE [meals ready-to-eat] Box, with a sandbag on his head, and attaching wires to his fingers, toes, and penis to simulate electric torture; Writing ' I am a Rapest ' [sic] on the leg of a detainee alleged to have forcibly raped a 15-year old fellow detainee, and then photographing him naked; Placing a dog chain or strap around a naked detainee's neck and having a female Soldier pose for a picture… The Taguba report also contains a finding that groups of male detainees were forced to masturbate themselves while being photographed and videotaped. In other conflicts such as that in Sri Lanka, there are reports of victims having been forced to masturbate their captors. The forced masturbation of the victim and the perpetrator is considered to be one of the most common forms of sexual violence experienced by men."[310]

[TOPIC - transition to topics Media Spectacle and Speculative Fiction]

"CIA Public Affairs Office of Entertainment Industry: "Entertainment Industry Liaison: As an organization that plays a key role in America's defense, the CIA is a frequent subject of books, motion pictures, documentaries, and other creative ventures. **For years, artists from across the entertainment industry — actors, authors, directors, producers, screenwriters, and others — have been in touch with the CIA to gain a better understanding of our intelligence mission**. Our goal is an accurate portrayal of the men and women of the CIA, and the skill, innovation, daring, and commitment to public service that defines them. If you are part of the entertainment industry, and are working on a project that deals with the CIA, the Agency may be able to help you. **We are in a position to give greater authenticity to scripts, stories, and other products in development. That can mean answering questions, debunking myths, or arranging visits to the CIA to meet the people who know intelligence** — its past, present, and future. In some cases, we permit filming on our headquarters compound. (Please visit our Headquarters Virtual Tour.) We can also provide stock footage of locations within and around our main building. Intelligence is challenging, exciting, and essential. To better convey that reality, the CIA is ready for a constructive dialogue with a broad range of creative talents. [311] … If you missed any of our Entertainment Industry Liaison's "Now Playing" recommendations, you can see his entire list of picks here: *The Movie Breach: A Personal Perspective. Intelligence in the Public Media*, by Brian Kelly. *Using Prediction Markets to Enhance US Intelligence Capabilities, The*

[310] "Sexual Violence Against Men in Armed Conflict" Sandesh Sivakumaran, P. 266-267
[311] https://www.cia.gov/offices-of-cia/public-affairs/entertainment-industry-liaison/

Farewell Dossier, CIA Analysis of the 1967 Arab-Israeli War, Engineering the Berlin Tunnel, Tracking Julius Rosenberg's Lesser Known Associates and The Ten Commandments of Counterintelligence, CIA Air Operations in Laos, 1955-1974, Tolkachev, A Worthy Successor to Penkovsky, The Crash of TWA Flight 800, A First Tour Like No Other and A Classic Case of Deception, A Close Call in Africa, Robert Fulton's Skyhook and Operation Cold Feet, Two CIA Prisoners in China, The Fall of Lima Site 85."[312]

[TOPIC – weaponization and strategic disuse of spectacle/speculation by CIA]

"Director Hayden: '**All interrogation sessions** in which one of these lawful procedures is authorized for use **has to be *observed by nonparticipants*** to ensure the procedures are applied appropriately and safely. *Any observer can call 'knock it off' at any time*. They are authorized to terminate an interrogation immediately should they believe anything unauthorized is occurring.'
Senator Snowe: 'So you also mentioned that **there are nonparticipants who are observing the interrogation process. Who are these non-participants**?'
Director Hayden: 'They could be other interrogators, medical personnel, chief of base, debriefers, analysts.'
Senator Snowe: 'Do they ever raise concerns during this process, during these interrogations?'
Director Hayden: **'Everybody watching has – every individuals has an absolute right to stop the procedure by saying 'stop'.**'
Senator Snowe: 'Did it happen? It's never happened?'
Director Hayden: 'No, we're not aware. I'm sorry. John [Rizzo] and [redacted] point out it's just not the ability to stop it; it is an obligation to stop it if they believe something is happening that is unauthorized.'
This testimony is incongruent with CIA records, for example: During the interrogation of Abu Zubaydah, CIA personnel at DETENTION SITE GREEN objected to the continued use of the CIA's enhanced interrogation techniques against Aub Zubaydah, stating that it was 'highly unlikely' Abu Zubaydah possessed the threat information CIA Headquarters was seeking. When the interrogation team made this assessment, they stated that the pressure being applied to Abu Zubaydah approached 'the legal limit'. **CIA Headquarters directed the interrogation team to continue to use the CIA's enhanced interrogation techniques and instructed the team to refrain from using 'speculative language as to the legality of given activities' in CIA cables**."[313]
"**Haspel drafted the cable ordering the tapes' destruction** at the request of her boss at the time, the CIA's former top operations officer, Jose Rodriguez. In her testimony on Wednesday, she said that she had 'absolutely' been an advocate for the destruction of the tapes 'if we could, within and conforming to U.S. law, **and if we could get policy concurrence,' because** their release would pose **a security risk** to the officers involved. Haspel said that CIA lawyers had repeatedly said that there was 'no legal impediment to

[312] https://www.cia.gov/offices-of-cia/public-affairs/entertainment-industry-liaison/now-playing-archive.html
[313] Senate Select Committee on Intelligence. *The Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency's Detention and Interrogation* Program. Melville House. December 2014, p. 345.

disposing of the tapes,' and said a disciplinary review by former CIA deputy director, Michael Morell, found no fault with her actions."[314]

'Total' Speculative Fiction

This subsection describes the function of implausible, exaggerated speculative fiction used in Defense planning as originating from the precept of total war, both 'creativity' and total war being concepts of modern warfare laid out by Clausewitz. In the modern US defense industries, the concepts have been combined resulting in the phenomenon in war planning I will term total speculative fiction: fictionalized Defense scenario-making, increasingly violent and nondependent on reality, promoted by the expectation of total war.

https://archive.org/details/DTIC_ADA390468 United States Army Command and General Staff College & National War College essays published by the Defense Technical Information Center. All three essays are works of creative fiction that assume the voice of Prussian military strategist Clausewitz (1780-1831) to advise on nuclear strategy and the Kosovo crisis.

In all the ***fictionalized scenarios***, we highlight challenges that could emerge as a result of the ongoing global transformation. The scenarios present new situations, dilemmas, or predicaments that would cause upheavals in the global landscape, leading to very different "worlds." ***None of these is inevitable or even necessarily likely***; but, as with many other uncertainties, they are potential gamechangers."[315]

Letter from Head of Shanghai Cooperation Organization to Secretary-General of NATO
June 15, 2015 p. 38-39, part of A World Without the West
"In this world, described in a fictional letter from a future head of the Shanghai Cooperation Organization (SCO), new powers supplant the West as the leaders on the world stage." (p 4)

Presidential Diary Entry
October 1, 2020 p. 58-59, part of October Surprise
"In this world, depicted in a diary entry of a future US President, many countries have been preoccupied with achieving economic growth at the expense of safeguarding the environment." (p 4)

Letter by current Foreign Minister to former Brazilian President
February 1, 2021 p. 77-79
"In this world, conflict breaks out between China and India over access to vital resources." (p 4)

FT.com Financial Times "Politics is Not Always Local"
September 14, 2024 [316]

[314] Taddonio, Patrice. "CIA Director Nominee Supported Destruction of Torture Tapes". *Frontline.* 9 May 2018.
[315] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 4.
[316] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 38-39; 58-59; 77-79;

"In this world, outlined in an article by a fictional ***Financial Times*** reporter, various nonstate networks—NGOs, religious groups, business leaders, and local activists—combine to set the international agenda on the environment and use their clout to elect the UN Secretary General." (p 4)

Master's thesis *Clausewitz on Kosovo* (2000) from U.S. Army Command & General Staff College. Claims of "myths" abound on Kosovo, "If the statesman and commander do not follow Clausewitz's lead as a critical historian, then they risk failure by founding future policy, strategy and operations on Kosovo myths."

Instead of contrasting facts from the previous mythical year, the thesis confidently rationalizes US action in Kosovo by imagining that NATO action received the support of the 18th century Prussian General Carl von Clausewitz. The War College graduate writes: "Clausewitz would suggest the following hypothesis: if NATO leaders applied their realistic understanding of the war to reconcile their ends, ways, and means and employ effective force to achieve their political objectives, then the use of force would be rational." [317] Used in contrast to CNN Effect in Action (applies same theorist to Kosovo)

[TOPIC – Meta-argument on Speculative Fiction]

"Clausewitz, Nuclear War and Deterrence": "For Clausewitz, war consists of a **paradoxical trinity: primordial violence, subordination to policy and 'the play of chance and probability within which the creative spirit is free to roam.**'" "Combat, although absent in a nuclear exchange or its deterrence, still exists. Political tensions and objectives of many kinds still **'discharge energy in discontinuous minor shocks'.** The politics of the cold war and the threat of mutual nuclear devastation have deterred absolute war but have not prevented limited wars."[318]

The essay "Through a Time Tunnel – Clausewitz on Nuclear Deterrence" out of the National War College in Washington, D.C. imagines Clausewitz has been transported through a "time tunnel" to deliver a speech at the National War College. Hypothetically, Clausewitz says, "I obviously knew nothing of nuclear weapons in my time… Though I did not know nuclear weapons, I knew deterrence." The author, a lieutenant colonel as of 1990, goes on to argue against a competing thesis, still pretending to be Clausewitz. He declares with great situational irony that, "I believe that his thesis is invalid in the real world. This is a critical point… His argument assumes that the great powers are willing to 'push the button' – to make what I [Clausewitz] have called an extreme effort. But as I state in my book, the extreme effort is contrary to human nature. It is a fantasy, and the human mind is unlikely to consent to being ruled by such a fantasy… although technology will continue to change many of the aspects of war, the human aspect will remain the most important. As a result, war's creative nature, emphasizing the creative, comprehensive mind, will always dominate its imitative nature." [319]

"The modern concept of total war can be traced to the writings of the 19th-century Prussian military strategist Carl von Clausewitz, who denied that wars could be fought by laws. In his major work *Vom Kriege* (*On War*), he rejected the limited objectives of 18th-

[317] https://archive.org/details/DTIC_ADA390468

[318] Barr, Alan W. "Clausewitz, Nuclear War and Deterrence". National War College; Defense Technical Information Center. 1 January 1991, p. 4; 6.

[319] Studenka, John M. "Through the Time Tunnel – Clausewitz On Nuclear Deterrence". National War College; Defense Technical Information Center. 3 October 1990, p. 3; 5-6.

century warfare, in which winning local military victories was regarded as the key to advantageous diplomatic bargaining, and **described wars as tending constantly to escalate in violence toward a theoretical absolute.** Clausewitz also stressed the importance of crushing the adversary's forces in battle. His 19th-century admirers tended to overlook his insistence that the conduct of war must be strictly controlled by attainable political objectives."[320]

"The Army cannot know nor predict its next fight but it can imagine the future of warfare. Fiction is a tool of the imaginative process. Fiction allows us to imagine the details of reality-as-it-might happen in order to understand potential consequences of decisions that we need, or might need, to make. It helps us imagine how current trends might play out or how new innovations might have an impact. As a tool, fiction is cousin to war-gaming. It creates opportunities to play out potential scenarios and prepare for them.

The Army University Press publishes the Future Warfare Writing Program (FWWP). This venture seeks to answer the question: What might warfare look like in the latter half of the 21st Century? Works of fiction and nonfiction should address the addresses multiple dilemmas as outlined in the Army Operating Concept. Submissions are open to current and former members of the DoD (active, guard, and reserve) and their dependents. … FWWP welcomes works of valid and sound speculative **fiction**; well-written essays; and any combination between the two addressing the questions above or related concerns. The intent behind this program is to give creative thinkers at all levels and positions—both within and outside the Army—the space to contribute to the conversation by generating ideas about the possible complexities of future warfare. The Army is at a critical time that requires reflection on its recent history, examination of its present reality, and exploration of its near and mid-future… Ideal works will be future-looking but grounded in a plausible reality. They will not address intergalactic conflict but very well could address the role of Army space operations in terrestrial conflict. There is much unexplored space for creative thinking in Defense Support to Civil Authorities missions before reaching the boundary of the post-apocalyptic. The works do not need to be technology-centric."[321]

Science Fiction: Visioning the Future of Warfare 2030-2050 U.S. Army TRADOC Mad Scientist Initiative[322], "mad scientist" being a term innovated to refer to a scientist of the atomic nuclear age who promotes projects of mutual assured destruction:

Mathison Hall**, senior analyst and project manager at the Johns Hopkins University Applied Physics Laboratory and US Marines reservist**, author of "Patrolling the Infosphere", winner of the **2017** Mad Scientist "Warfare in 2030-2050" Writing Contest**: The main character is a soldier stationed in a desert of Africa, working with Chinese nationals to control an epidemic caused by a "synthetic bug". The fictional soldier's duties include "mak[ing] sure the resisters aren't stealing any of the bodies before they're burned". The character works under the World Health Organization's containment plan while simultaneously being engaged in a hacker war.**

---

[320] https://www.britannica.com/topic/total-war

[321] https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/

[322] https://www.armyupress.army.mil/Portals/7/Future-Warfare-Writing-Program/Documents/Compendium.pdf

In 2017, the Johns Hopkins University physics analyst imagines a 'fictional' future for his character in which "the Russian and Brazilian cube-sats will be watching our jamming bubble and broadcasting it over SkyChat … If they hack into our transmitter like they did last week, we'll be uncovered and the cube-sats will beam live images of us around the world as we fight off any ambush. It's almost a guarantee they'll throw some poor kid, probably some helpless six- or seven-year-old girl, right into the mix where she'll be torn apart by their bullets and ours on live SkyChat in front of an audience of hundreds of millions. That's exactly what Moscow and Brasilia want, to humiliate us in the never ending battle for control of world opinion. That's why we have the Chinese with us. The New Chinese National Army runs the clinics, and the resisters can't defend against our hackers and theirs at the same time."

The fictional soldier is accompanied by a "Cyber Force hacker" whose "reach-back squad in Maryland are going to start lighting up the news feeds and social media soon." The Cyber Force hacker is a genetically engineered soldier who won an International Court of Arbitration case in order to have "a chance of medaling at the last Olympics in Lagos not all that far from here." They are on a mission with two more soldiers who, after being targeted with a "micro-electromagnetic pulse generated by the gun", are described as "probably cooking in there [their flex armor suits]". On patrol, the group is pursued by drones determined to be "likely kids playing games as always. These drones aren't autonomous…they're networked to kids or whomever all over the world."

Being deployed in a cyberwar, Marine and Johns Hopkins' applied physicist describes, is being in a conflict in which mortars are guided by Internet Protocol addresses and the dead bodies of children killed by those mortar blasts are livestreamed in real-time by global news media - "Bad news is Russia Today and Brasilia TV are showing images of dead kids in the street. I'm already seeing news feeds about Americans killing civilians including children with indiscriminate mortar fire. We've just jumped to 125 million people actively live-following our patrol, increasing by nearly one million a second." The main character predicts future wars will be caused by genetic engineering policy which will lead eugenically modified persons to exterminate the rest of humanity.[323]

SGT Oren Hammerquist is an Air Defense and Airspace Management in October 17, 2016: *"*The near eruption of World War III here is speculative only in the sequence of events; the technology presented exists. Some predict that 90% of news stories will be written by machines in fifteen years. Thousands of stories a year already are. Special effects are nothing new, and dedicated pranksters could cause mass panic on a viral scale… Afghanistan and Iraq taught us more than ever that technology will change the shape of the battlefield to include the incorporeal social media realm. That the characters in this story must fall back on civilian systems run by Google and other companies to compensate for holes in our dated information infrastructure is likely more truth than fiction."[324]

On the same Army University Press platform, a non-fiction paper by head of the Department of Human Genetics at the Institute of Genetics, University of Lund, Sweden, originally published in 1970, titled "Ethnic Weapons" is promoted as a non-fiction recommendation by the Army in 2020. The paper describes the use of chemical enzymes

---

[323] Hall, Mathison. "Patrolling in the Infosphere". Future Warfare Writing Program. The Army University Press. 2017.

[324] https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/Black-Hat-Kamchatka/

developed in the 1930s "on the Rhine" that have further been proven to have varying health effects on neurological signal transmission of different ethnicities and races. An excerpt from the non-fiction article follows:

> A series of enzyme inhibitors and chemically active substances interfering with signal transmission in the brain and spinal cord have been intensely studied since the early fifties. Many of these substances have a colorful prehistory saturated with tribal sorcery. The incapacitant known as BZ derives from a drug which before its present renaissance as lysergic acid diethylamide (LSD) caused epidemic outbursts of Saint Anthony's fire in the Dark Ages. With ditran-like compounds, BZ shares **the capacity to produce transient toxic psychosis, sometimes compared to schizophrenia.** *Search Continues:* Surrounded with clouds of secrecy, **a systematic search for new incapacitating agents is going on in many laboratories.** The general idea, as discussed in open literature, was originally that of minimal destruction. **Psychochemicals would make it possible to paralyze temporarily entire population centers** without damage to homes and other structures. In addition, with the small quantities required for full effect of modern incapacitating agents, logistics problems would be minute. The effective dose of BZ-type agents amounts to micrograms. It is quite possible to use incapacitating agents over the entire range of offensive operations, from covert activities to mass destruction. **One fairly obvious offensive preparation is protection of the country's own personnel by tolerance-building. This is where enzymatic response to psycho chemicals enters the scene. Exposure to drugs or to molecules of almost identical composition is known to produce, with varying degrees of accuracy, resistance to the toxic effect at repeated exposure.** As this is a known and thoroughly discussed procedure, concealment of large-scale preparations of this type probably would be difficult if not wholly impossible… There have been some recent tendencies to stress the wide latitude between incapacitating and the lethal action of BZ-type agents. **Friendly troops could use them to dampen belligerence. They effectively slow down physical and mental activity, make the poisoned personnel giddy, disoriented, and more or less unable or unwilling to carry out commands. Friendly forces would discriminatingly use incapacitants in entangled situations to give friend and foe a short period of enforced rest to sort them out. By gentle persuasion, aided by psychochemicals, civilians in enemy cities could be reeducated. The adversary would use incapacitants to spare those whom he could use for slaves**… During the first half of that year [1969], several laboratories reported factors engaged in passing over the genic message from DNA, the primary command post, to RNA which relays the chemical signal. The enzymatic process for RNA production has been known for some years, but now the factors have been revealed which regulate the initiation and specificity of enzyme production. Not only the factors have been found, but their inhibitors. Thus, the functions of life lie bare to attack.[325]

MARINE CORPS SECURITY ENVIRONMENT FORECAST: FUTURES 2030-2045: "If there's one constant in planning for future war, it's that no one expects it to get any easier. To figure out the rough contours of how war gets harder, the Marine Corps Warfighting Laboratory put together uniformed service members with science fiction authors to craft the 'Marine Corps

[325] Larson, Carl A. "Ethnic Weapons". *Military Review.* November 1970. Accessed at Future Warfare Writing Program. The Army University Press.

Security Environment Forecast: Science Fiction Futures,' a series of short stories approximating calamities the Corps should expect in the future. In 'Water is a Fightin' Word,' by U.S. Coast Guard Lt. Cmdr. Molly Waters, Marines in exoskeleton suits and robotic teammates conduct a humanitarian relief mission in a world gone dry. In 'Double Ten Day,' by Marines Maj. Vic Ruble and Capt. Sara Kirstein, a Marine advise-and-assist mission turns into kinetic urban combat, amidst a post-earthquake Taipei riven by both competing insurgencies and the disaster itself. In 'The Montgomery Crisis,' the eight authors detail a bioengineered food shortage that forces a withdrawn United States to cobble together legacy systems and launch an attack for free navigation of the seas against hostile forces in the Mediterranean. The stories are all grounded in cold, analytical forecasts made by the Marine Corps and influenced by sources as diverse as the United Nations and the writing of Thomas Friedman. It is a useful document, if necessarily a dry one. It's one thing to say, 'it is a world driven by social unrest and marked by instability, complex conflict, food and water shortages, and severe natural disasters.' It is another thing to walk with Marines conducting a raid on a building in Taipei in a world where an earthquake and reactor meltdown turn Taiwan into a collapsed state beset by insurgents. The forecast provides the broader map, but it's the fiction that shows what inhabiting that world might actually look like. What's important about the stories is less the specifics. Speculative fiction is an approximate art, a reckoning of what might be hard in the future, more than an exact roadmap to that future. As such, the forecast deals with modern problems extrapolated outwards. In 'The Montgomery Crisis,' display and small arms technology advances, but the U.S. Navy has to make do with then-ancient vessels and planes, like Zumwalt-class destroyers, Ford-class carriers, and F-35B Lighting II Joint Strike Fighters. **The military threats are still anti-access, area-denial, powerful ship-killing foreign-designed missiles in the hands of radical religious extremists with near-peer backing. But it's the impetus behind those attacks, the plague and the grain shortage, that provides the most direct shift: an America made hungry, through careful sabotage at the hands of just a few well-placed malcontents.** The story ends with victory, but a temporary one: the plague vector remains, and is beyond the problem-solving abilities of the Marines. Instead, grain shipments and free global trade provide the immediate salvation…"[326]

Media Spectacle

+ADD "You Don't Have To Run The Exclusive Reveal For The War Crime Game" on *Six Days in Fallujah* video game 3/24/21 https://kotaku.com/you-don-t-have-to-run-the-exclusive-reveal-for-the-war-1846543966
+ADD "Video games are the new contested space for public policy" 3/228/21 https://www.brookings.edu/techstream/video-games-are-the-new-contested-space-for-public-policy/

+ADD *The Lone Gunmen* television series: "In the pilot episode, which **aired March 4, 2001, rogue members of the U.S. government remotely hijack an airliner** departing Boston, **planning to crash it into the World Trade Center, and let anti-American terrorist groups take credit, to gain support for a new profitable war following the Cold War.** The heroes ultimately override the controls, foiling the plot. The episode aired six months prior to

[326] https://news.usni.org/2017/10/17/marines-solicit-science-fiction-stories-imagine-future-conflicts

the September 11 attacks."[327] Pilot episode for transcription: https://www.youtube.com/watch?v=FcZ6HXIOmYE

"What is more astonishing is communication's huge impact: Almost 30,000 foreign fighters joined the IS army during 2013–2015; 5,000 of them were European youngsters, second- and third-generation immigrants, European-born citizens, and many were people converted to the Muslim faith (Barrett et al., 2016). Obviously, the IS transmedia propaganda impact must be considered with other factors (e.g., social marginality, attitude to crime, etc.) as a driving force to push people to embrace the jihadist cause. Nevertheless, **IS online narratives are commonly considered as having a pivotal role** in turning a Salafist Muslim into a radicalized foreign fighter. **Is the Hollywood-style engagement** or the appeal to the global Islamist community—the Ummah—to take part in a real war **the successful feature of IS transmedia strategy? Is there a substantial difference in IS strategy between the fictional and the nonfictional political narrative?"[328]**

[***Millennium Challenge '02* wargame described** by RAND analyst Zenko in previous section as it relates this essay's alternate title *Or, How I Learned to Worry and Stop Loving the Arab Spring*, a reference to the 1964 film ***Dr. Strangelove: Or, How I Learned to Stop Worrying and Love the Bomb***.] A cult-classic film in policy circles, the film features a character Dr. Strangelove (based on RAND's Herman Kahn), a Nazi German ex-pat who works in research and development with the fictional BLAND Corporation. Several other characters from this film seem to reappear in Zenko's retelling of the *MC '02* wargame: "General Buck Turgidson" in *Dr. Strangelove* as Chair of Joint Chiefs of Staff resembles Joint Forces Command commander General William 'Buck' Kernan in *MC '02*; "Jack D. Ripper" in *Dr. Strangelove* as Air Force Brigadier General may portray Lt. General Paul Van Riper in *MC '02*. https://www.gradesaver.com/dr-strangelove/study-guide/character-list

The **plot** of the film and the wargame both revolve around military information deception operations, weapons of mass destruction, and US-Soviet Russia proxy wars. ["Through a series of military and political accidents, a pair of psychotic senior military officers -- U.S. Air Force Commander Jack D. Ripper (Sterling Hayden) and Joint Chiefs of Staff General "Buck" Turgidson (George C. Scott) -- hatch an ingenious, foolproof, and irrevocable plan to unleash a wing of B-52 bombers and their nuclear payloads on strategic targets inside Russia. And when the brains behind the scheme, Dr. Strangelove (Peter Sellers), a wheelchair-bound nuclear scientist with bizarre ideas about man's future, accidentally activates the bombing mission, the President of the United States (Peter Sellers) is unable to stop it. Although he knows the secret code to stop the mission, the Royal Air Force's Group Captain Mandrake (Peter Sellers) isn't much help since he's come under attack at a U.S. Air Force base by a group of U.S. paratroopers who've been accidentally activated, too. So, despite all efforts to recall him, Major T. J. 'King' Kong (Slim Pickens) personally sees his bombing mission to its fateful conclusion, even as the Russian Ambassador (Peter Bull) is summoned to the White House in hopes of averting a crisis and preventing the activation of the 'Doomsday' machine. But the inevitable comes to pass as the efforts of the Pentagon brass and all the politicians in Moscow and Washington cannot undo the cascading series of cataclysmic events."[329]]

---

[327] https://en.wikipedia.org/wiki/The_Lone_Gunmen_(TV_series)

[328] Monaci, p. 2857.

[329] Sony Pictures Movies & Shows

Former President Bill Clinton's 2018 novel *The President is Missing* presents a fictionalized narrative of cyberwar from the point of view of an individual of the highest rank of office in the US.

Clinton's novel imagines a scenario in which a "half-Muslim" female Bosnian assassin named Nina - throughout the plot referred to by her hacker moniker 'Bach' - works alongside a hacker named Auggie to cause a global hack codenamed "Dark Ages" that disrupts the world's electronic system. In the story, fictional President Johnathan Lincoln's daughter is contacted by text message about the attack, which spurs the action of the story. President Jonathan Lincoln Duncan's struggle to deal with the cyber-attack includes his hiring foreign hackers, homoerotically described as "a cross between a Calvin Klein model and a Eurotrash punk rocker," and his covert mission with a Secret Service agent named Davis which requires the President to be smuggled out of the White House in disguise. The story even details the fictional president's past as a former Army Ranger tortured in an Iraqi prison. The plot's recurring villains are a group called Sons of Jihad who are mistakenly believed to be Islamic militants but are revealed to really be secular Turkish nationalists.

Note that at the center of former President Clinton's novel is the 1990s-era misconception that a computer virus could cause a global blackout. The plot is reminiscent of the 1995 major motion picture *The Net*, hugely popular at its release, which also centers around cyberterrorist assassinations of government officials and a global cyber meltdown caused by a rogue cybersecurity corporation's malicious virus called "Mozart's Ghost", used to hack the entire US government.

In a 2018 interview on his novel, Clinton stated:

> The danger in this book [*The President Is Missing*] is the most dangerous cyber-attack ever launched against the United States or any nation. It was designed to cripple our military, erase all our financial records, destroy our electrical grid, transmission networks, break our water and water purification systems, disable our cell phones and more. There would be massive loss of life, damage to the health of millions, economic crash greater than the Depression, and violent anarchy in the streets… It's real. Every single one of those things could happen.[330]

The psuedo-Islamist secular Turkish cyberterrorism conspiracy codenamed "Dark Ages" in former President Clinton's book is a real-world term used by cyberterrorism contractors The Hacking Team. Leaked in the 2015 emails between The Hacking Team employees, the hacking corporation's CEO David Vincenzetti reportedly sent to the entire staff listserv the 2015 *Wall Street Journal* article "The Global War on Modernity: Islamists set the time machine to the Dark Ages. Putin dreams of czarist Russia. A common enemy: America" by Human Rights Foundation Chairman Garry Kasparov.

The term 'dark ages' is used in the 2015 article shared by The Hacking Team to mean fundamentalist Islamist attacks meant to destroy infrastructure and send the Western world back to "the Dark Ages." Repeatedly referring to US adversaries anywhere from Russia to Africa as

---

[330] Martha's Vineyard Productions. "Bill Clinton The President is Missing". *Martha's Vineyard Author Series*. 30 December 2018.

"time travelers", author and Human Rights Foundation Chairman Garry Kasparov echoes the exact words used in Clinton's cyberterrorism novel, stating that "radical Islamists, from the Taliban and al Qaeda to Boko Haram and Islamic State, set the time machine to the Dark Ages."[331]

Not only is it highly unusual for a former president of the US to pen a novel, but one advertised on the book cover as revealing "Only Details A President Would Know" cements its place in the realm of policymaking speculative fiction. The discomforting fact that many turns of the novel's plot have transpired *since* the novel's publication in 2018 suggests that Clinton's novel is another example of real-world policymaking taking place in a fiction genre. In his 2018 interview with Martha's Vineyard, Clinton even quips that "it's just a matter of time" before he losses security clearance over revelations made in his novel. As is typical of the speculative fiction genre, the braggart-style whistleblowing is so unsubstantiated as to make the work utterly useless as fact or fiction.

Although not a wargame scenario proper, former President Bill Clinton's *The President is Missing* constitutes a lesser discussed genre of fictionalized policymaking in the dramatic arts, likened to the Armed Forces speculative fiction discussed further in the section Monopoly on Infringement.

[REWORD] relevance to recent events: (Turkmen new leader of ISIS? article [printed], congressional sanctions against Turkey passed & official recognition of Armenian genocide by Young Turks. 2020 attacks on Armenia. ; "The vicious war against the Armenian Republic of Artsakh (Nagorno-Karabagh) and Armenia by Azerbaijan, Turkey, and thousands of their jihadist terrorists has passed the one month mark. The jihadis' presence, which includes ISIS, is consistent with the debauched political cultures and national ambitions of Azerbaijan and Turkey. It also tells us that the U.S./NATO/EU stance towards those countries continues to be dangerously passive. Just days ago, right in our nation's capital, Azeri demonstrators chanted "jihad, jihad, jihad" and flashed the hand signal of Turkey's homicidal, neo-fascist Grey Wolves."[332]

Balkan war criminals termed 'wolves' is another favorite reference of former President Clinton's from his book recommendation list, *The Wolf of Sarajevo* (2016), which Clinton repeatedly has recommended in interviews. *The Wolf of Sarajevo*, a work of speculative fiction predicting the resurgence of interethnic conflict in Bosnia plotted by "a shadowy mafia figure" utilizing political blackmail, is written by current Department of State Deputy Assistant Secretary in the Bureau of European and Eurasian Affairs Matthew Palmer. Palmer, author of a series of political thrillers ostensibly based on his inside knowledge of State Department Foreign Affairs, also served on the Secretary of State's Policy Planning Staff and on the National Security Council.

The State Department's fabulist-in-residence speculated in 2015 on a nuclear war stoked between India and Pakistan by misinformation in the form of a falsified phone transcript

[331] https://wikileaks.org/hackingteam/emails/emailid/51162
[332] https://countercurrents.org/2020/10/the-new-kings-of-jihadist-terrorism-azerbaijan-and-turkey/

discovered in a corporate contractor's security system (*Secrets of State*), and again in 2015 on a US mining corporation's domination of US political affairs in the Democratic Republic of the Congo (*The American Mission*). In 2017 Palmer published the story of the fictional "Kate" who is assigned by her uncle who works for the US Foreign Service in Kyrgyzstan "to infiltrate an underground democracy movement that has been sabotaging Kyrgyz security services and regime supporters" in a less than overt plan by Washington to support the movement of the Kyrgyz saboteurs and "tip the scale in 'the Great Game'" (*Enemy of the Good*).[333]

"North Korea has routinely engaged in coercive acts in the physical world. In 2014, the pending release of a satirical movie—centered around a plot to kill North Korean leader Kim Jong-Un—prompted North Korea to lodge a vehement protest via the United Nations, and later resulted in a destructive attack on and release of internal documents from Sony Pictures Entertainment."[334]

"To prove they could follow vehicles in this way, the Livermore team had flown the camera in a helicopter over an oil-storage facility in the desert south of the town Mojave. Actors in two vehicles had driven in a series of patterns between two separate areas of the facility. During the test, **Marion told the facility's security guards that he was filming a movie, which was technically true. When one of the guards asked where all the cameras were, Marion pointed to a small speck in the sky: 'Up there.**'"[335]
"One Friday evening in the winter of 1998, a researcher at the Lawrence Livermore National Laboratory, the nuclear-research facility about an hour from downtown San Francisco, went to the local theater with his wife to see *Enemy of the State*… watching the film with his wife, the Livermore researcher found something else: inspiration. (For security reasons, he requested that his name be withheld.) Whereas his fellow moviegoers saw a herald of doom, he saw an opportunity. *What if such a device could actually be created?* He thought. *Wouldn't that be amazing?*... On Monday morning, a number of the researcher's colleagues convened in an office in Livermore, and the researcher explained his idea in detail. *Imagine all the things that the government could do with a wide-area persistent video-surveillance satellite*… With that, a small subset of the group launched an in-house program to explore – theoretically, at first – how emerging digital-imaging technology could be affixed to a satellite in order to produce something like *Enemy of the State*'s Big Daddy. Film the Whole Thing All the Time: As it happened, the group wasn't alone among the Livermore community in its dreams of building a fanciful surveillance satellite. In 2001 they were approached by John Marion, a lanky, soft-spoken engineer with a round, youngish face who was working with Edward Teller, still an active presence in the lab at the age of 91… In the spring of 2001 Marion had attended a briefing presented by the digital-photography group, which included a clip from *Enemy of the State*… To replicate the steady, top-down view as seen from satellite in *Enemy of the State*, the Livermore researchers decided to go to the source. They reached out to Wescam, the company that had run the aerial filming for the movie. The crew, it turned out, had created the 'satellite' imagery by flying a helicopter at high altitude with a film camera

[333] https://www.penguinrandomhouse.com/authors/240576/matthew-palmer/
[334] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. x.
[335] Michel, Arthur Holland. *Eyes in the Sky: the Secret Rise of Gorgon Stare and How It Will Watch Us All.* Houghton Mifflin Harcourt. 2019, p. 23.

pointed directly down at the earth. Nathan Crawford, a general manager at the company, invited the engineers to meet in Los Angeles, where he was working on the set of *Terminator 3*… Crawford had already been involved in a number of classified technology projects at Wescam's defense unit, which had developed the Predator's [drone] stabilized camera-mount. Thanks to a lengthy career in camera work, he also possessed the rare ability to film a golf ball flying through the air at great speeds – a useful skill if you wanted to emulate a satellite tracking a cohort of nuclear scientists going about their daily routines from several hundred miles above the surface of the earth."[336]

"Jones [Col. William Jones, Army Exercise director] noted the exercise environment isn't limited to adaptive mission planning processes. Students also **face simulations of real-world challenges, such as media and public pressures**. To set the stage each day, **students view a "special report" by the fictional Global News Network, providing realism as the wargame progresses**. Students are also given a situation briefing and a daily press summary that stresses their ability to employ instruments of national power and a whole of government approach to deal with the crises at hand. "To prevail in today's war with extremists, as well as to successfully engage with our joint, interagency, and multinational partners, we must understand, master and strategically ramp up two powerful and frequently neglected weapons: **words and images**," said Dr. Frank Kalupa, U.S. Air Force Center for Strategic Leadership Communication director. "This is especially imperative on social media platforms, used so effectively by terrorists.' "[337]

[TOPIC - VNN as media spectacle and speculative fiction]

https://www.fema.gov/pdf/privatesector/ps_notes_ttx_power.pdf (pg 10 VNN fake news broadcast video from FEMA for disaster scenarios); https://www.govtech.com/em/emergency-blogs/disaster-zone/FREE--FEMA-Tabletop.html ; https://www.youtube.com/watch?v=FtFPUdzPz6I "VNN Disaster Scenario News Broadcast" ; https://www.fema.gov/media-library-data/20130726-1833-25045-2267/mom_ttx_video_inject_scripts_final_508.pdf ; https://www.youtube.com/watch?v=udemJGMEN54 RaffertyWeiss Media uploaded 2016 pt 3, pt 2 https://www.youtube.com/watch?v=JMCZrCkjnxs 2014 (on fictional Puerto Rico hurricane earliest upload 2014 - hurricane Maria in 2017), Part 1 https://www.youtube.com/watch?v=K-bMnQRobqw ; Fake Northeast Africa countries 'Bloomland' & 'Golva' shown on map VNN report scenario w/ Persian and Arabic speakers featured from real news reel https://www.youtube.com/watch?v=UTqbmqkYuqw

Event 201 10/18/2019 pandemic simulations in NY (World Military Games Oct. 18-27 in Wuhan) http://www.centerforhealthsecurity.org/event201/media

+ADD more on performance theory https://www.brown.edu/Departments/Joukowsky_Institute/courses/architecturebodyperformance/files/257077.htm [REMOVE? Moved to VNN effect]

---

[336] Michel, Arthur Holland. *Eyes in the Sky: the Secret Rise of Gorgon Stare and How It Will Watch Us All.* Houghton Mifflin Harcourt. 2019, p. 14-15; 16; 19.

[337] Harper, Reginald. "Strategic Joint Wargame Challenges Future Leaders Ability to Think Multidimensional". *Maxwell Air Force Base News.* 29 March 2017.

+ADD John Kerry as Secretary of State asking for video of convoy being bombed in leaked discussions of the US creating ISIS, Syrian speaker says plenty of video has been provided, refuses to give video to US justify response.[338]

[TOPIC - rape as a weapon of irregular warfare, constant result of US invasion over decades of war, explicit policy of US military, **spectacle of rape as weapon of war]**

"Perhaps part of this is due to Isis going out of its way to make a point of publicising their campaign of sexual violence against Yazidi women. Rape as a weapon of war is nothing new, and was widely utilised in the Balkan conflicts, especially in Bosnia, in the 1990s. With Isis, rape is part of their propaganda campaign in their bid to wipe out the Yazidi. And perhaps there is a method in their brutality above control, subjugation and violence for its own sake; the Yazidi culture dictates that women who form relationships with non-Yazidis automatically take on the religion of their partner. Isis is effectively raping the Yazidis out of existence, one horrific assault at a time. Dr Brown says, "The women are enslaved partly as a reward for Isis soldiers, partly as a weapon against non-Muslim groups. With Bosnia it seemed that rape was a byproduct of genocide; for Isis it is something to be publicly celebrated.""
+ sadism - irregular warfare sex slavery ending in maiming by regular warfare landmine account in article.[339]
"Sexual violence against women in conflict frequently takes place in public, in front of the victims' communities and their families. On an individual level, there is the added aspect of public humiliation and shame, an added stigma. There is also little chance that word of the rape will be kept quiet. Public sexual violence is also, then, a way of communicating to the rest of the community, of spreading fear and vulnerability throughout the area. An entire community may feel compelled to flee; indeed this may have been the very purpose of the public nature of the sexual violence in the first place. The power of the perpetrators is vindicated, on show for all to see. These factors are also at play when male sexual violence is committed in public."[340]

It should be reiterated that ISIS is a multinational organization comprised of members from across the globe. This oft-forgotten fact lends further credence to the reality that ISIS sex slave trade takes place within the preexisting global human trafficking market, described by investigators of missing and exploited children in the US since the 1970s. Not only are the buyers businessmen from the West and other wealthy nations, but many foreign members of ISIS are citizens of Western and allied nations.
+ADD Internet and global sex trade features of ISIS sex slave trade.

The Great Game
The Game is so large that one sees but a little at a time.
Rudyard Kipling, *Kim* (1901)

---

[338] https://www.youtube.com/watch?v=e4phB-_pXDM&feature=youtu.be ; https://mondoweiss.net/2017/01/watched-manage-leaked/
[339] https://www.independent.co.uk/news/world/middle-east/isis-sex-slaves-lamiya-aji-bashar-nadia-murad-sinjar-yazidi-genocide-sexual-violence-rape-sakharov-a7445151.html
[340] Sexual violence against men in conflict, P. 268

The Great Game is readily understood as the long series of political and military espionage, wars, coups, colonizations, assassinations, and policy deceptions that affected the Near East. The Great Game took place between the multiple powers of the 19th and 20th centuries, the European colonial powers, Russia, Arab tribes, Indian Mughals, China, nationless states, and nearly every entity with a global presence, including mercantilist companies. In this sense, wargames are part of an antiquated form of policy endeavor, especially obvious when taking place in the Near East. There are a great number of recent events that are echoes of not only Cold War era issues, but Great Game era rivalries.

+ADD US invades Afghanistan 10 years after Soviet collapse, South Asian continent in turmoil with nuclear weapons and interreligious conflict, China trade wars, opium flooding countries (cite again), globalist expansions of companies overtaking sovereign countries, disputes of succession in Arabia proper, Syria and Iraq borders under dispute, Turkey involved in caliphate struggles….

A.J.P. Taylor in *How Wars Begin* attributes the start of World War I to information warfare surrounding military action. He writes:
"The Austrian declaration of war on Serbia was pure theory; no action followed it. Now this gives **the essential factor in the outbreak of the first world war**. All the great powers, of whom there were five, or six counting Italy, had vast conscript armies. These armies of course were not maintained in peace time. They were brought together by **mobilisation**… The Russians then thought they ought to stake out some claim to prove that they were going to support Serbia so the tsar and his advisers contemplated mobilisation but only against Austria and this was actually ordered… They had no of a war against Germany or even against Austria. **They wanted a threat, not a real preparation for war. Mobilisation was a mere gesture…** Now with Russia mobilizing, the problem moved to Germany and here again this was entirely a matter of timetables. **It was said afterwards that mobilisation meant war**. Technically for most countries this was not true; it was merely a step towards war. Mobilisation after all took place within a country. The Royal Navy had mobilised as late as 1911. Russia mobilised in 1913. There were occasions when other powers had mobilised and because war did not take place the armies could be dispersed. With one country [Germany], however, this did not apply…
The other essential part which was equally important was that there could be no delay between mobilization and war because if there were delay then Russia would catch up and the Germans would get the two-front war after all. So the moment that the Germans decided on mobilisation, they decided for war, or rather war followed of itself… and none of it could be altered because if it did all the timetables would go wrong. Thus the decision for mobilisation which the German general staff made and which Bethmann endorsed on 29 July was a decision for a general European war. There was no deeper consideration in the background. Nothing was weighed except the technical point: if Russia mobilises we must go to war. Serbia and Austria-Hungary were forgotten. The Germans declared war on Russia simply because Russia had mobilised… The Germans then invented an allegation that Nuremberg had been bombed by French planes. This was untrue. Whether there had ever been bombing I am not clear. It may be true that a German plane had dropped the bombs, but who did what did not matter; the thing was to get the war going. Thus the war came about mainly because of railway timetables."[341]

[341] Taylor, A.J.P. *How Wars Begin.* Ebenezer Baylis & Son Ltd. 1979, p. 108, 110 112, 117, 120.

M.E. McMillan in *From the First World War to the Arab Spring* likewise attributes the beginning of World War I to factors of information warfare:
"Franz Ferdinand and his wife were in Bosnia on official business. **The archduke had come to oversee the Fifteenth and Sixteenth Army Corps on maneuvers in the border province**. Security was a pressing concern for the empire because the Balkan region was in a state of upheaval. **But exactly how much the Habsburgs knew about what was really going on beyond their borders and how prepared they were to deal with it remains an open question**. **The empire's intelligence chief, Colonel Alfred Redl, had been arrested the year before, caught red-handed passing secrets to the Russians. Partly to keep his personal life private (he was gay) and partly to fund his lavish lifestyle (he had very expensive tastes), the colonel had duped his political masters for a decade.** After being interrogated, Colonel Redl was given a gun and left alone to do the honorable thing. The scandal was hushed up but the damage was done. At a time when the Habsburg Empire's southern borders were simmering with discontent**, Vienna was relying on faulty intelligence.** The province that the archduke was visiting, **Bosnia**, was bordered by Serbia and Montenegro. Both were newly independent after centuries as provinces of the Ottoman Empire… Britain and Russia, in particular, were ruthlessly Machiavellian about **using the Balkans to score points against their imperial rival** in Istanbul… All of this presented a challenge to the Austro-Hungarian Empire. It was not just that Vienna needed to protect the empire's southern border from invasion or another Balkan war [1912, 1913]. **The real threat to the empire was ideological. The newly formed Balkan states were based on the idea of *nation*."**[342]

National Intelligence Council writes that "in the case of Central Asia, where large deposits of energy resources increase the potential for a repeat of the 19th century's 'Great Game' with outsiders contending for the exclusive right to control market access. The fact that a number of countries may experience a sharp fall in national power if alternatives for fossil fuel are developed quickly injects a potentially dangerous risk of instability."[343]

+ADD Retired US Navy Adm. William McRaven: "'I am often asked where do I think the greatest external security threat is, and I always point to Russia,' McRaven, a former Navy SEAL and special operations commander, said at a Chatham House event on Tuesday. 'A lot of people think about China, but Russia jumps to mind first.' While he acknowledged that Russia is not the superpower it once was, he stressed that **'Putin has outplayed us. He has played the great game better than anyone on the world stage,**' McRaven said of the Russian president. Pointing to Russian actions in Crimea, Ukraine, Syria, and even the US that were detrimental to American interests, he said: 'Putin is a very dangerous person.'… McRaven argued Tuesday that the US needs to not only make its position clear to Russia, but it also needs **to rebuild and leverage alliances 'to make sure that Russia understands how they need to play.'**"[344]

---

[342] McMillan, M.E. *From the First World War to the Arab Spring: what's really going on in the Middle East?* Palgrave MacMillan: NY. 2016, p. 11.
[343] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 82.
[344] https://www.msn.com/en-us/news/world/former-navy-seal-commander-says-putin-has-outplayed-the-us-and-russia-is-the-greatest-external-security-threat/ar-BB1dqsfF?ocid=Peregrine

+ADD “Hypergame analysis extends game theory by providing the larger game that is really being played whether or not both players are aware of it.”[345]

+ADD DEFENDER-Europe 20 wargame[346]

Oversimplification in US policy towards the Middle East, being late comers to Middle East expansionism, tends towards interpersonal psychoanalysis combined with unstated orientalist reductionism. This is displayed recently by President Trump on non-intervention on the northern Syria border when he stated, about conflict arising between Turkish and Kurdish military, “Sometimes you have to let them fight like two kids in a lot, you gotta let them fight, and then you pull them apart.”[347]
Previously, poor policy advisors have successfully published and pushed similar frameworks to describe their policy failures in the Israeli-Palestinian negotiations. American psychologist Kenneth Levin famously presented his orientalist paradigm of abused child syndrome called the Oslo Syndrome to explain away the Clinton Administration’s failure in the 1993 Oslo Accords. His argument relies on concepts of group “pathology” created by “marginalization”, “disparagement”, “chronic assault” and “dangers”, even felt vicariously by a diaspora.
Levin writes:
But the metaphor of Jews as the West’s miners’ canary is no less applicable to the themes of the present study. Significant numbers of Jews have repeatedly responded to the noxious fumes of chronic assault in the Diaspora and in Israel by deluding themselves into believing they could win peace through embracing the indictments of their enemies and seeking to appease them. These psychological responses, their translation into communal and national policy, and the disasters that have followed offer lessons for those whose predicaments are in many ways so very different and yet similar, including an America under attack.[348]

The Oslo Syndrome not only expects psychology to translate directly into national policy, and expects that those policies could be accurately predicted with psychoanalysis, but it also prevents discussion of policy failures as failures of the policy makers and administrations. This neatly removes blame of incompetence or suspicion of subversion from those institutions and individuals who have failed in their stated policy objectives, switches cause for effect, and changes the possible objectives of the conversation entirely. The familial psychology framework most dangerously precludes considerations of traditional concepts of military and political strategy informed by a keen awareness of military might and political power structures. The structuring of the Middle East conversation as child-adult or child-child creates a false sense of literal familiarity with informed policymaking, which can *create* rather than *explain* dangerous situations, and it significantly trivializes the actual issues. The effect of such framing lends itself to the acceptance of wargame and other chance-based policy risks based on predictive thought-policing by institutions and individuals that have already proven themselves to be destructive and intentionally ill-informed.

---

[345] Kovach, Nicholas S., Alan S. Gibson, and Gary B. Lamont. “Hypergame Theory: A Model for Conflict, Misperception, and Deception.” *Game Theory,* Vol. 2015. 19 August 2015, p. 2.
[346] https://www.eur.army.mil/DefenderEurope/
[347] Karanth, Sanjana and Roque Planas. “Trump On Turkey And Kurds: ‘You Have To Let Them Fight Like 2 Kids’”. *The Huffington Post.* 17 October 2019.
[348] Levin, Kenneth. *The Oslo Syndrome: Delusions of a People under Siege.* Smith and Kraus, 2005, p. viii.

"Game" understood to mean "deception" at policy level since 19th century. (https://www.thebritishacademy.ac.uk/pubs/proc/files/111p179.pdf)

+ADD "**Historical laws were in reality historians' laws**, just as 'the two forms of humanity' drew attention less to actuality than to a European capacity for lending man-made distinctions an air of inevitability. As for the other half of the phrase – 'will at last be soldered together' – there Flaubert mocked the blithe indifference of science to actuality, a science which anatomized and melted human entities as if they were so much inert matter**. But it was not just any science he mocked: it was enthusiastic, even messianic European science, whose victories included failed revolutions, wars, oppression, and an unteachable appetite for putting grand, bookish ideas quixotically to work immediately**."[349]
+ADD "Flaubert frankly acknowledges that this is grotesquerie of a special kind. 'All the old comic business' – by which Flaubert meant the well-known conventions of 'the cudgeled slave... the coarse trafficker in women… the thieving merchant' – acquire a new, 'fresh… genuine and charming' meaning in the Orient. This meaning cannot be reproduced; it can only be enjoyed on the spot and 'brought back' very approximately. The Orient is watched, since its almost (but never quite) offensive behavior issues out of a reservoir of infinite peculiarity; the European, whose sensibility tours the Orient, is a watcher, never involved, always detached, always ready for new examples of the *Description de l'Egypte* called 'bizarre jouissance.' The Orient becomes a living tableau of queerness. And this tableau quite logically becomes a special topic for texts. Thus the circle is complete; from being exposed as what texts do not prepare one for, the Orient can return as something one writes about in a disciplined way. Its foreignness can be translated, its meanings decoded, its hostility tamed; yet the *generality* assigned to the Orient, the disenchantment that one feels after encountering it, the unresolved eccentricity it displays, are all redistributed in what is said or written about it."[350]

"Like many CIA officers of their generation, Kim [Roosevelt] and his cousin Archie Roosevelt, another chief of the Agency's Middle East division in the early years of the Cold War, had been raised and educated in an elite environment that conditioned them, long before they ever directly experienced the region itself, to look upon the Middle East much as the British imperial agents of an earlier generation had: as a place for heroic individual adventure, where a handful of brave and resourceful Western spies could control the fate of nations. To a certain extent, this legacy of spy games and kingmaking was offset by the American missionary tradition conveyed to the early CIA by the OSS, which tended to emphasize instead moral values of Arab self-determination and mutual cultural exchange. However, the adventurist tendency was also reinforced by the presence in the early CIA's Middle East division of another distinct social type best exemplified by the southerner Miles Copeland: bright, ambitious young men from nonelite backgrounds who had gotten into the CIA thanks to the opportunities for social mobility opened up by World War II (usually via the Counter Intelligence Corps rather than the more aristocratic OSS) and who, while not possessing the same social origins as the Roosevelt cousins, did share their **appetite for game playing… The playing of games, whether it was an American version of Britain's "Great Game,"** or the clash of personal wills that eventually arose between Kim Roosevelt and Gamal Nasser, **or Miles Copeland's abiding interest in game theory, was not merely a metaphor**. It was a crucial historical determinant in the formation and eventual demise of CIA Arabism… **Fiction is another important medium for understanding the CIA**

[349] Said, Edward. *Orientalism*. Vintage Books: New York. 1978, p. 115-116.
[350] Said, Edward. *Orientalism*. Vintage Books: New York. 1978, p. 103.

Arabists, whose perceptions and actions (including, I will argue, some of the major covert operations of the period) were strongly influenced by the adventure stories of a previous generation and who themselves inspired fictional portrayals by other writers."[351]

"He brought a very heavy load of personal objectives and suppositions to the Orient, unloaded them there, and proceeded thereafter to push people, places, and ideas around in the Orient as if nothing could resist his imperious imagination."[352]

+ADD ISIS media outlet *Al-Hayat* (by same name as London-based major Arabic language newspaper) video called Sykes-Picot Agreement on Syria-Iraq borders described in media reports.

+ADD [REWORD- repeated in Spectacular Security State] "George Kennan—head of the State Department's Policy Planning Staff, former chargé d'affaires at the U.S. Embassy in Moscow, and arguably the chief architect of the Cold War—insisted that the United States embrace 'covert political warfare' and 'propaganda as a major weapon of policy.' Although Kennan claimed he was promoting 'organized public support of resistance to tyranny in foreign countries,' he secretly crafted NSC-10/2, which transformed the CIA from an intelligence gathering agency to an operational outfit with a charter to engage in 'propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-Communist elements in threatened countries of the free world.' More important, NSC-10/2 specified that such actions must be carried out so that 'if uncovered the U.S. Government can plausibly disclaim any responsibility for them.' When **President Truman signed this directive on June 18, 1948, he institutionalized not simply secret warfare but also public deception as a fundamental element of U.S. policy**… NSC-68 ensured that what first seemed a minor exception to democratic oversight would eventually become **a major basis for U.S. foreign policy. The scale of psychological operations in the early Cold War so overwhelmed the CIA that Truman was forced to create a Psychological Strategy Board** packed with public relations and advertising executives."[353]

"The PWB **[Psychological Warfare Branch] was a haven for dissidents from the official US line of cooperation** with the Vichy French, and its officers were **prone to taking vigilante actions** against alleged local fascists **and to illegally protecting** Gaullist **resistance fighters [**MOVE THIS PART?]; Eisenhower reputedly complained that the PWB [Psychological Warfare Branch] gave him 'more trouble than all the Germans in Africa.'"[354]

---

[351] Wilford, Hugh. *America's Great Game: the CIA's Secret Arabists and the Shaping of the Modern Middle East.* NY: Basic Books. 2013, p. xxi-xxii.
[352] Said, Edward. *Orientalism*, PAGE
[353] Melley, Timothy. *The Covert Sphere : Secrecy, Fiction, and the National Security State*. Cornell University Press. 2012, p. 3-4
[354] Wilford, Hugh. *America's Great Game: the CIA's Secret Arabists and the Shaping of the Modern Middle East.* NY: Basic Books, 2013, p. 28.

+ADD Reintroduction of mid-19th century *glasnost* reforms into late-era Soviet Union. The introduction of concepts of democratization and transparency via political media/technology defined the Arab Spring. G*lasnost*, a term repurposed from Russia's Great Game period, reappeared in the late 1980s as a rallying concept less than a decade before the collapse of the Soviet Union. The similar concept driving the Arab Spring appeared across the Arab World, and within a decade those countries collapsed into coups and wars. (on Ebsco *Gorbachev's Glasnost: The Soviet Media in the First Phase of Perestroika*, Joseph Gibbs)

Arab Spring changes by country

+ book Arab Movements in WWI

Monopoly on Violence, Monopoly on Infringement

War, they say, is the instrument of national policy.
John W. Thomason

"The state must not only establish sovereignty over cyberspace, it must also legitimise its position of authority in a space that has potentially challenged the long-term authority in a space that has potentially challenged the long-term relevance of the nation state concept itself. No notion of authority can exist in a liberal democratic society without the explicit consent and blessing of its electorate; to do so in cyberspace while fundamentally redressing the balance of individual insecurity online requires a revision of the social contract as it exists with citizens. Powers and Jablonski note this problem well in the conclusion, in stating this issue of legitimate state authority is a 'stagnant area' of academic inquiry."[355]

The perceived inability of 'them to govern themselves' is a trademark of imperial thought constantly addressed in post-colonial studies. Here I point out that this perceived lack of legitimacy is the foundation for the US or other hegemons to authorize, in other words *legitimize*, violence in other nations.

US interventions in other nation's democratic processes, by overt and covert means, is socially and politically acceptable to interventionists despite their alleged intent to 'support' democracies. It matters little whether democracy is practiced in other nations because, in actuality, it is legitimacy that is perceived lacking in other nations' governance, not democracy.

Those with the state monopoly on violence are the same who hold what I call the monopoly on infringement. In this essay, as in Weber's *Politics as a Vocation*, the phrase refers to the right to infringe on the State's monopoly on violence.

Here, it also refers to infringement in the judicial sense of 'non-violent breach, encroachment or transgression'. The blurred line between the monopoly on violence and monopoly to infringe in the Information Age (IA) and in irregular warfare conduction is explored in this section.

---

[355] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 98.

The ability to alter and control perception is part of what I call here a 'monopoly on infringement'. Perception of an inability to self-govern is the legitimization for transnational use of force. The actual imposition of violence reinforces the perceived lack of legitimacy. Likewise, the ability to impose violence forces a perception of legitimacy. This concept is addressed also in the section Proxy Wars and 'Going Native'.
+ADD summary of above 2 paragraphs
This process can be applied to self-state – feature of genocide in 20th-21st centuries is transnational cooperation against apparent interest of the nation and national sovereignty.

"Collective identities become political when people make public claims based on these identities and when governments are involved in these claims either as objects or as third parties. Meyer believes that states directly impact the formation and salience of particular identities by endorsing or prohibiting certain practices, regulating access to socially valued goods and setting rules for intergroup relations. As a result, states create dissident collective identities and set clear boundaries between their members and the rest of society. These state-dictated conditions impact the emergence of social movements. **Given the state's position as the legitimate monopolizer of the use of physical force, the state is 'simultaneously target, sponsor, and antagonist for social movements as well as the organizer of the political system and the arbiter of victory'**."[356]

"Although resilience increases in importance in a more chaotic world, traditional calculations of state power rarely factor in a state's resilience. The **sudden collapse of the Soviet Union and the breakdown of state authority in the aftermath of the "Arab Spring"** suggest that states can be fragile in **ways that conventional measures of power do not capture**."[357]

If we are to use sociologist Max Weber's definition of the State as those who hold a monopoly on violence and coercion over a territory, which must become defined as such through "a process of legitimation", we would be compelled to assume that **either hacker collectives have become the authorized state over the State, or that they act with the authority and permission granted by the State**. In fact, Anonymous, the hacking collective, explicitly claims to "have launched other efforts while also building new strategies and recruiting individuals from across the globe - some of whom **hold significant positions in media, industry, and the sciences**."[358] [repeated in Cyber Realism] +ADD failed state articles
"State failure is characterized by government predation and the militarization of civic society… Were the abuse of power the sole distinctive characteristic of state failure, then we would be unable to differentiate it from authoritarianism. The difference between the two arises from the second key characteristic **of state failure: a loss of the monopoly over the means of coercion.** When states fail, political competition takes place between groups bearing arms. **Political parties become political militias as elites transform them into military bands.** Private firms seeking protection and private citizens seeking security affiliate with these militias as they search for sources of the security that the state no longer provides. Note the distinction between state

---

[356] Karolak, Magdalena. *The Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Academica Press. 2014, p. 13.
[357] National Intelligence Council. *Global Trends: Paradox of Progress*. P. 65
[358] Anonymous. "Opinion: Anonymous and the global correction".

failure and revolution. Both lead to violence; but revolution creates a new order, whereas state failure yields disorder."[359]
"two aspects of state failure: the **self-interested use of the power of the state by those who occupy positions** within it and **the state's loss of a monopoly on violence**." [360]
"In 60% of the country-years in which there were failed states in Africa between 1970 and 1995, there were also civil wars; and in 70% of the country-years in which there were civil wars, there were failed states… roughly 40% of civil wars resume after their termination." [361]
"[Bates] argues that **forces favoring democratization originated at the global level and were especially strong at the end of the Cold War**. Had incumbent autocracies prepared for a transition to democracy, they would have behaved with great restraint, he argues; having failed to do so, they had reason to fear **political reprisals following the loss of power**. In response to the increase in **insecurity inspired by the transition** to democracy, incumbents turned predatory, increasing the level of corruption, looting public assets, and suppressing those who attempted to displace them. Facing threats from their putative guardians, people began to provide their own security. They formed militias and states broke down."[362] Connect to Post-Cold War cyberarms reforms not taken seriously by State… The failure of the State to implement cyberpolitical reforms is addressed further in the chapter The Satellite Empire in the final section A Kafkaesque Answer To An Orwellian Problem.

***Theories that apply to motives of military action, meaning war or military occupation, do not cross-apply to genocide just because some elements are shared between them*. For example, in a stateless country experiencing genocide (a 'failed' state) there exist policies or pogroms toward genocide that cannot be enacted or devised in the absence of a state. Genocides are by definition systematic, and could not be conducted by a 'failed' state. This is further evidence for the existence of the 'Satellite Empire' and its primacy in coups, wars and resulting genocides.**

This is however possible in war between states or in occupations of states by states. Therefore, there must be open facts and theories to explain *which* existing state is devising and enacting the pogrom policies. In specific historic example, the Nazi pogroms halted upon collapse of the Nazi State, completely ceasing and liberating those people, or, became persecutions led by the Allied and Soviet States. [REWORD – repeated]

https://journals.sagepub.com/doi/pdf/10.1177/0192512113480054 Fragile and Failed States
https://doi.org/10.1111/j.1468-2486.2007.00728.x Failed States and Global Security, Stewart Patrick

[REMOVE text from Weber block quote]

In presenting his essay *Politics as a Vocation*, Max Weber: "force is a means specific to the state… a state is a human community that (successfully) claims the *monopoly of the*

[359] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 1-2.
[360] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 5.
[361] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 3; 9.
[362] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 9.

legitimate use of physical force within a given territory. Note that 'territory' is one of the characteristics of the state. Specifically, at the present time, the right to use physical force is ascribed to other institutions or to individuals only to the extent to which the state permits it. The state is considered the sole source of the 'right' to use violence. Hence, 'politics' for us means striving to share power or striving to influence the distribution of power, either among states or among groups within a state… the state is a relation of men dominating men, a relation supported by means of legitimation (i.e. considered to be legitimate) violence."(78)

"How do the politically dominant powers manage to maintain their domination? The question pertains to any kind of domination, hence also to political domination in all its forms, traditional as well as legal and charismatic. Organized domination, which calls for continuous administration, requires that human conduct be conditioned to obedience towards those masters who claim to be the bearers of legitimate power. On the other hand, by virtue of this obedience, organized domination requires the control of those material goods which in a given case are necessary for the use of physical violence. Thus, organized domination requires control of the personal executive staff and the material implements of administration."(80)

"the modern state is a compulsory association which organizes domination. It has been successful in seeking to monopolize the legitimate use of physical force as a means of domination within a territory. To this end that state has combined the material means of organization in the hands of its leaders, and it has expropriated all autonomous functionaries of estates who formerly controlled theses means in their own right. The state has taken their position and now stands in the top place… Proprietors of military implements in the own right, or proprietors of goods important for the administration, or proprietors of personal prerogatives may be called 'estates'." (82-83)

"The decisive means for politics is violence."(121)

"It is the specific means of legitimate violence as such in the hand of human associations which determines the peculiarity of all ethical problems of politics. Whosoever contracts with violent means for whatever ends – and every politician does – is exposed to its specific consequences."(124)

"…Therefore he also depends upon whether or not the premiums can be permanently granted to the following, that is, to the Red Guard, the informers, the agitators, whom he needs."(125)

"Naturally power actually rests in the hands of those who, within the organization, handle the work *continuously*. Otherwise, power rests in the hands of those on whom the organization in its processes depends financially or personally…It is decisive that this whole apparatus of people – characteristically called a 'machine' in Anglo-Saxon countries – or rather those who direct the machine, keep the members of parliament in check. They are in a position to impose their will to a rather far-reaching extent, and that is of special significance for the selection of the party leader. The man whom the machine follows now becomes the leader, even over the head of the parliamentary party. In other words, the creation of such machines signifies the advent of *plebiscitarian* democracy… That is about what the old party organization looked like. It was half an affair of notables and half an entrepreneurial organization with salaried employees. Since

1868, however, the ‘caucus’ system developed…a nonconformist parson and along with him Joseph Chamberlain brought this system to life. The occasion for this was this development was the democratization of the franchise. In order to win the masses it became necessary to call into being a tremendous apparatus of apparently democratic associations. An electoral association had to be formed in the very city district to help keep the organization incessantly in motion and to bureaucratize everything rigidly. Hence, hired and paid officials of the local electoral committees increased numerically…The elected party managers had the right to co-opt others and were the formal bearers of party politics. The driving force was the local circle…These local circles were also first to call upon the world of finance. This newly emerging machine, which was no longer led by members of Parliament, very soon had to struggle with the previous power-holders, above all, with the ‘whip’. Being supported by locally interested persons, the machine came out of the fight so victoriously that the whip had to submit and compromise with the machine. The result was centralization of all power in the hands of the few and, ultimately, of the one person who stood at the top of the party…It soon became obvious that a Caesarist plebiscitarian element in politics – the dictator of the battlefield of elections – had appeared on the plain. In 1877 the caucus became active for the first time in national elections, and with brilliant success, for the result was Disraeli’s fall at the height of his great achievements. In 1866, the machine was already so completely oriented to the charismatic personality that when the question of home rule was raised the whole apparatus from top to bottom did not question whether it actually stood on Gladstone’s ground; it simply, on his word, fell in line with him: they said, Gladstone right or wrong, we follow him. And thus the machine deserted its own creator, Chamberlain... The caucus machine in the open country is almost completely unprincipled if a strong leader exists who has the machine absolutely in hand. Therewith the plebiscitarian dictator actually stands above Parliament. He brings the masses behind him by means of the machine and the members of Parliament are for him merely political spoilsmen enrolled in his following. How does the selection of these strong leaders take place? First, in terms of what ability are they selected? Next to the qualities of will – decisive all over the world – naturally the force of demagogic speech is above all decisive. Its character has changed since the time speakers like Cobden addressed themselves to the intellect, and Gladstone who mastered the technique of apparently ‘letting sober facts speak for themselves.’ At the present time often purely emotional means are used – the means the Salvation Army also exploits in order to set the masses in motion. One may call the existing state of affairs a ‘dictatorship resting on the exploitation of mass emotionality.’…The [U.S.] President, who is legitimized by the people, confronts everybody, even Congress; this is a result of ‘the separation of powers.’ In America, the spoils system, supported in this fashion, has been technically possible because American culture with its youth could afford purely dilettante management. With 300,000 to 400,000 such party men who have no qualifications to their credit other than the fact of having performed good services for their party, this state of affairs of course could not exist without enormous evils. A corruption and wastefulness second to none could be tolerated only by a country with as yet unlimited economic opportunities. Now then, the boss is the figure who appears in the picture of

this system of the plebiscitarian party machine. Who is the boss? He is a political capitalist entrepreneur who on his own account and at his own risk provides votes. He may have established his first relations as a lawyer or saloonkeeper or as a proprietor of similar establishments, of perhaps as a creditor. From here he spins his threads out until he is able to 'control' a certain number of votes. When he has come this far he establishes contact with the neighboring bosses, and through zeal, skill, and above all discretion, he attracts the attention of those who have already further advanced in the career, and then he climbs. The boss is indispensable to the organization of the party and the organization is centralized in his hands… He who wishes to trespass with impunity one of the many laws needs the boss's connivance and must pay for it; or else he will get into trouble. But this alone is not enough to accumulate the necessary capital for political enterprises. The boss is indispensable as the direct recipient of the money of great financial magnates, who would not entrust their money for election purposes to a paid party official, or to anyone else giving public account of his affairs… In contrast to the English leader, the American boss works in the dark. He is not heard speaking in public; he suggests to the speakers what they must say in expedient fashion. He himself, however, keeps silent. As a rule, he accepts no office, except that of senator. For, since the senators, by virtue of the Constitution, participate in office patronage, the leading bosses often sit in person in this body. The distribution of offices is carried out, in the first place, according to services done for the party. But, also, auctioning offices on financial bids often occurs and there are certain rates for individual offices; hence, a system of selling offices exists which, after all, has often been known also to the monarchies, the church-state included, of the seventeenth and eighteenth centuries. The boss has no firm political 'principles'; he is completely unprincipled in attitude and asks merely: What will capture votes? Frequently he is a rather poorly educated man. But as a rule he leads an inoffensive and correct private life… Thus the structure of these unprincipled parties with their socially despised power-holders has aided able men to attain the presidency – men who with us [Germany] never would have come to the top. To be sure, the bosses resist an outsider who might jeopardize their sources of money and power. Yet, in the competitive struggle to win the favor of the voters, the bosses frequently have had to condescend and accept candidates known to be opponents of corruption. Thus there exists a strong capitalist party machine, strictly and thoroughly organized from top to bottom, and supported by clubs of extraordinary stability."[363]

+ADD "**If it's a legitimate rape**, the female body has ways to try to shut that whole thing down." Representative Todd Akin, Republican Senate nominee from Missouri[364] re: strategic rape concept in irregular warfare

Monopoly on Infringement

---

[363] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 103-10.

[364] Eligon, John and Michael Schwirtz. "Senate Candidate Provokes Ire With 'Legitimate Rape' Comment". *The New York Times*. 19 August 2012. Electronic resource. <https://www.nytimes.com/2012/08/20/us/politics/todd-akin-provokes-ire-with-legitimate-rape-comment.html>.

As I address in this section Monopoly on Infringement, the line between the monopoly on violence and the monopoly to infringe is blurred in the Information Age (IA).

To illustrate this, consider the findings of an analytic team at Sonoma State University which determined that within the US, four of the top ten American media corporations are directed by Department of Defense contractors. These include William Kennard of the Carlyle Group directing *The New York Times* board, Douglas Warner III of Bechtel directing the board of NBC/General Electric, John Bryson of Boeing and Alwyn Lewis of Halliburton both directing the board of Disney/ABC, and Douglas McCorkindale of Lockheed-Martin directing Gannett's board.[365] The lack of distinction between the monopoly on violence and the monopoly on infringement is explored in continuation in the section The Satellite Empire.

Monopoly on violence occurs alongside legitimized infringements on the State's legitimate use of violence. Weber uses the term 'legitimate infringement' to refer to the use of State sanctioned non-governmental force. In this section, I discuss the monopoly on infringements as non-violent transgressions, breaches, encroachments that prevail in the Information Age (IA).

Monopoly on infringement here refers to permission given by the State to non-governmental actors to commit non-violent crimes with full knowledge that the infringement may lead to violence. Infringements take the form of bulk data mining, surveillance, cyber-trespassing, cyber-theft, invasion of privacy, disregard of sovereignty, identity theft, assuming another's identity, slander and libel, copyright infringement, falsification of information, withholding of national security information, intentional security breaches, and other infringements regularly practiced and sanctioned by the State in the Information Age which can lead to violence. These infringements are encouraged by the State which holds the monopoly on violence.

Within the paradigm of cyber-realism, this must refer to the State that is *actually* in control of the three elements of Clausewitz's triad of war: operational instruments, popular passions, and policy. If it is shown that there is significant ability or disability for a state or person to control either instruments, public opinion, or policy, then that fact must be taken into account to determine actual monopoly holder status.

This is exemplified in claims in the US that the US has been victimized by state-sponsored infringements from Russia. Cyber defense analyst Daniel Steed classifies commercial concerns over monopolies of infringements as principally Western cyber concerns, while other nations more closely allied with Russia or China invariably are concerned with violence resulting from infringements. As of 2020, nearly all states have claimed victimhood from loss of control over IA operational instruments, public opinion, or policy decisionmaking.

The ethereal nature of computerized operational instruments makes it extremely unclear who is in control. This vagueness is exploited to manipulate perception of infringements and

---

[365] Phillips P. 9-10. BOOK/ARTICLE TITLE? Alt. cite https://www.projectcensored.org/inside-the-military-media-industrial-complex-impacts-on-movements-for-peace/?doing_wp_cron=1599752607.1986830234527587890625

attributions of violence. Such a tactic is not as convoluted as it may seem. Creating dubious operational control is a product of primarily utilizing popular passions and policy of war rather than instruments; that is, favoring the use of popular passions and policy to effect war *defines irregular warfare* from traditional warfare, which wrongly assumes direct deployment of operational instruments.

Senior Information Scientist Dr. Rand Waltzman of the RAND Corporation has said of the news media relation to monopolies on infringement:

> Somebody did a study and estimated that at least 75 percent of everything that appears in the newspaper across the United States are basically press releases written by a public relations firm. That tells you that the news is essentially manufactured. And of course for them it makes economic good sense because if someone comes to them with a press kit that's all done well they don't need a reporter – they've got to get the content out so they just take it. Now it's much more extreme I would say. And especially as the economics for their business gets more difficult, this kind of thing looks a lot more attractive. Then you have the corporations that use the same people – American corporations, foreign corporations – all corporations are using the same kinds of people plus their own in-house efforts. Then you have politicians that are using the same people. So everybody is using the same people. So, when you see, for example, the FCC and net neutrality – did you see the analysis that somebody did that said 80 percent of these comments were bogus? Not real? They were astroturfed. A lot of them were traced back to Russian websites. But that doesn't mean the Russian government was involved. All that means is the people who did it were using the same contractors the Russian government uses. So you can't tell: the Russian government uses contracting, the Chinese government uses contracting, everybody uses contractors, so these contractor will work for anybody for a fee. That kind of thing is on the upswing. And I expect it to get a lot worse. [366]

The RAND Corporation, which maintains some of the most costly and long-standing contracts in US government history, and other weapons development centers and think tanks openly admit that their corporate analysts act under assumed identity as States at the request and paid permission of those States, and even as other corporate or private industries. That is to say, publicity and policy contractors are both State and Press with permission of the State. +ADD Weber's analysis here

With this system of legitimate infringement intact, there is only one actor in the entire political landscape – pay-per-page information contractors, like Dr. Rand Waltzman himself. This is why Waltzman enjoys quoting in the same article that, "Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country."

As one of the few policy and publicity think-tanks with a defense weapons sector, the RAND Corporation enjoys both legitimized infringement and legitimized violence. Dr. Waltzman's use of the quotation on an invisible government that actually holds the power of

---

[366] Magee, Tamlin. "US government can't compete in information war, warns RAND Corporation: The RAND Corporation's Dr Rand Waltzman speaks with Techworld on the state of 'cognitive security' in the world and the 'democratization of weapons of mass disruption". *TechWorld*. 12 February 2018.

the country, while what is apparently the State does not, precisely describes the RAND Corporation. With the capabilities for legitimized infringement of both kinds – infringement and violence – RAND, by its own description, holds the end-to-end power to use physical force and non-violent deception. In the Information Age, the geographical scope of the power of this intellectually and morally vacuous, unaccountable corporation extends as far as RAND's own nuclear engineers have designed nuclear weapons to fly and as far as the telecommunications may penetrate.

Weber spends a significant amount of time in his essay discussing the role of news media in relation to anonymity and power politics. He writes:

> **The political publicist, and above all the journalist, is nowadays the most important representative of the demagogic species**… Thus far, however, **our great capitalist newspaper** concerns, which attained control, especially over the 'chain newspapers,' with 'want ads,' **have been regularly and typically the breeders of political indifference**. For no profits could be made in an independent policy; especially no profitable benevolence of the politically dominant powers could be obtained. The advertising business is also the avenue along which, during the war, the attempt was made to influence the press politically in a grand style - an attempt which apparently is regarded as desirable to continue now. Although one may expect the great papers to escape this pressure, the situation of the small ones will be far more difficult. In any case, for the time being**, the journalist career is not among us, a normal avenue for the ascent of political leaders**, whatever attraction journalism may otherwise have and whatever measure of influence, range of activity, and especially political responsibility it may yield. One has to wait and see. Perhaps journalism does not have this function any longer, or perhaps journalism does not yet have it. **Whether the renunciation of the principle of anonymity would mean a change in this is difficult to say. Some journalists - not all - believe in dropping principled anonymity.** What we have experienced in the war in the German press, and in **the 'management' of newspapers by especially hired personages and talented writers who always expressly figured under their names**, has unfortunately shown, in some of the better known cases, that an increased awareness of responsibility is not so certain to be bred as might be believed. Some of the papers were, without regard to party, precisely the notoriously worst boulevard sheets; **by dropping anonymity they strove for and attained greater sales.** The publishers as well as the journalists of sensationalism have gained fortunes but certainly not honor. Nothing is here being said against the principle of promoting sales; the question is indeed an intricate one, and the phenomenon of irresponsible sensationalism does not hold in general. But thus far, **sensationalism has not been the road to genuine leadership or to the responsible management of politics**. How conditions will further develop remains to be seen. Yet **the journalist career remains under all circumstances one of the most important avenues of professional political activity**... It is indeed no small matter to frequent the salons of the powerful on this earth on a seemingly equal footing and often to be flattered by all because one is feared, yet knowing all the time that having hardly closed the door the host has perhaps to justify before his guests his association with the '**scavengers of the press**'. Moreover, it is no small matter that one must express oneself promptly and convincingly about this and that, on all conceivable problems of life - whatever the 'market' seems to demand - and this without becoming absolutely shallow and above all without losing one's dignity by baring oneself, a thing which has merciless results. **It is not astonishing that**

> **there are many journalists who have become human failures and worthless men.** Rather, it is astonishing that, despite all this, this very stratum includes such a great number of valuable and quite genuine men, a fact that outsiders would not so easily guess.[367]

The VNN Effect

When news of war is proclaimed, wisdom is thrust aside, with violence is action done, scorned is the speaker of good counsel, dear is the rude warrior. Not with learned speeches do men strive, but with evil speaking fall foul one of another, brewing unfriendliness. They rush to make joint seizure - not by law; rather by the sword do they seek a due return and aim at the first place, and move on with pack and press.
Quintus Ennius (239-169 B.C.)

[REVISIT TOPIC - VNN effect and infringement]

The VNN effect is the use of wargames/scenario-based media to set policy agendas, impede opposing agendas, and push decision-makers into action. 'VNN' is taken from the name of the mock news channel used in disaster scenario trainings by FEMA. While the CNN effect is understood to be the use of authentic news stories to alter policy agenda and action, by terming this phenomenon 'the VNN effect', I trace the media used under CNN effect conditions to their wargame/scenario origins. The media used in the VNN effect are based on speculative fiction by policy and military industries, unlike media used to create the CNN effect, which are understood to be true but promoted for political purposes. Like the CNN effect, the VNN effect is used to propel nations into war.

State controlled news media reporting policy objectives or enacted policy determined by game theory analysts are essentially no different than false news broadcasts created for wargames. +fake newscasts for wargames This is an extreme level of social engineering which is meant to be deceptive, and is identifiable as a wargame product. [REWORD – repeated]

"The cornerstone of any deception operation is the deception story. The deception story is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe to be the true situation, then decide and act on that basis. In other words, the deception story parallels what the deception would want the opponent's intelligence estimate to say about your own commander's intentions and your own unit's actions. The deception story identifies those friendly actions, both real and simulated, that when observed by the deception target will lead it to develop the desired perception. Deception story development is both an analytic and creative process that involves a variety of information on enemy data acquisition and processing. An exact understanding of the perceptions and observables required for the deception provides a concrete basis for crafting the deception story. The deception story weaves these elements together into a coherent depiction of the situation the target will reconstruct from the information provided. Ideally, the deception planner wants the deception story to be the exact mental picture of the target forms as the deception unfolds. **The deception story should read like the adversary's own intelligence estimate**. The deception story is, in effect, the equivalent of a completed puzzle. As such, it serves as a means of checking

[367] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 97-99.

the logic and consistency of the internal elements of the deception. **This allows the deception planner to identify desired perceptions, observables, and executions that may need refinement, and to add supporting observables as needed to strengthen certain elements of the deception story or diminish the impact of troublesome competing observables. Each element of the deception story should have associated deception means that can credibly portray the data, plus identified conduits that transfer this information** into the enemy's information processing system. Unavoidably, various nodes in this line of communications also become filters of the information conveyed, **allowing the target to introduce their own predispositions and biases that the MILDEC planner must anticipate. As the story is developed and elaborated, the MILDEC planner continuously monitors changes in the situation and validates the deception story** against other friendly plans and/or actions. The story should be believable, verifiable, consistent, and executable**. (1) Believable**. The story must correspond to the deception target's perceptions of the friendly force's mission, intentions, and capabilities. **(2) Verifiable. The adversary should be able to verify the veracity of the deception story through multiple channels and conduits. The deception story, therefore, takes into account all of the adversary's intelligence sources and is made available through all or many of those sources.**"[368] [REPEATED from Spectacular Security State]

+ADD US Capitol riot January 6, 2021: "A man the FBI has identified as Grapevine resident Larry Brock is seen in the video giving instructions to people inside the US Senate. 'I love you guys. We're brothers but we can't be disrespectful,' Brock says in the video as people took photos on the dais. 'It's a PR war**. You have to understand it's an IO war. We can't lose the IO war. It's information, information operation.**'… Throughout the 12-minute video, the mob attacking the US Capitol is seen fighting with officers and can be seen at the end of the video chanting "F--- the blue."… [University dean of criminology] Del Carmen said the mob taking photos of documents once they're inside is something military members are trained to do during operations. 'The individuals that have a mission — in some cases military background, law enforcement background — they're the ones that are sort of driving this,' he said. 'It's hard to say if the people who were actually doing this were doing it for the sake of preserving evidence or because they had some kind of military background.'"[369] [Repeated]

+ADD "As journalist and media scholar Peter Pomerantsev puts it, **the authoritarian notion of 'information warfare'** is part of a world view and interpretation of history **'where all values, ideals, ideas are mere fronts to subvert the other side**, where there is **no qualitative difference between independent journalism and a covert social media psy op**.'"[370]

+Multimedia approach to the CNN effect: "To describe Hollywood's corporation strategies aimed at creating new nonlinear narrative trends, Jenkins wrote, A transmedia story unfolds across multiple media platforms, with each new text making a distinctive and valuable contribution to the whole. In the ideal form of transmedia storytelling, each medium does what it does best—so that a story might be introduced in a film, expanded through television, novels,

---

[368] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-5 – I-6.

[369] Joy, William. "New video reveals more about Texas connections to attack on US Capitol". *WFAA-ABC.* 17 January 2021.

[370] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 76-77.

and comics, and its world might be explored through game play or experienced as an amusement park attraction. (p. 95) Centered on popular Hollywood movies such as *The Matrix* or *Fight Club*, Jenkins's contribution reveals important trends also in the creation of contemporary media narratives, emphasizing the development of complex storytelling structures organized on different media platforms with a specific goal, namely, to engage a dispersed audience of people with different dedicated contents (video, texts, social mobile media contents) disseminated by all media available. Along with fiction, more recently a nonfiction International Journal of Communication 11(2017) Islamic State's Online Media Strategy 2847 transmedia field has emerged especially in relation to documentaries (O'Flynn, 2012), serious gaming (Morreale & Bertone, 2015; von Stackelberg & Jones, 2014), and social online campaigns, such as the "Red Nose Day" campaign in the United Kingdom (Freeman, 2016b). According to Freeman (2016b), nonfiction transmedia could be referred to the concept of infotainment—a mix of information and entertainment aimed at engaging the audience across multiple media platforms through an extensive use of social media and storytelling strategies based on real facts or events. Compared with fiction transmedia, nonfiction tends to "generate impact on the public sphere" (Freeman, 2016b, p. 95)with a pragmatic call to action aimed at raising funds, engaging people for an active commitment in their communities, or influencing their opinions in the context of political election. A common ethos (i.e., the complex of tradition, social values, and habits) shared by the targeted community is the premise for an effective transmedia strategy."[371]

In the VNN Effect, it is further shown that media are regularly used, without the informed consent of the public, as The Public Space for the manipulative wargaming of real-life situations and crises. That is, what is alleged to be comprehensive coverage of current events, or mere fictional entertainment, is actually used as "a central place to display and update information relevant to the game," meaning the wargame scenarios which the public is non-consensually involved in nearly constantly.

The media pieces are fabricated by an immense systematized industry of speculative fiction writers/producers, including the US military. They are portrayed as comprehensive coverage of events in order to solicit 'authentic' responses from unaware consumers. Decisionmakers aware of the speculative nature of the media blithely use The Public Space (i.e., public media) to communicate "vital strategic information" to opponents or cohorts, and "to make strategic decisions about [their] opponents" – which they easily could do through more direct communication (if not for their criminally deviant fetish for gameplay, already detailed in the section Out of the Blue). A hijacked public media serves to maintain plausible deniability of conspiracy and inflates the influence of the defense wargaming industry.

+ADD Monopoly on Infringement: on non-violent harm and low-intensity violence as feature of the 'soft power' of Information Age "soft power of softwares", (ie surveillance/intelligence/policy deceptions/tech deceptions/corporate empires), especially when

[371] Monaci, p. 2846-47.

it has led to violence on a significant scale, National Intelligence Council pg 90 fake Financial Times article in scenario report, VNN similar to CNN effect (https://www.fema.gov/media-library-data/20130726-1833-25045-2267/mom_ttx_video_inject_scripts_final_508.pdf , https://www.fema.gov/pdf/privatesector/ps_notes_ttx_power.pdf , wargames) ; FBI forges flyers in name of black community children's breakfast program, white nationalist group meetings, FBI memos approving infringements in name of fake canvasing white supremacist group "Storm Warning" in 1969 declassified COINTELPRO docs https://vault.fbi.gov/cointel-pro/cointel-pro-black-extremists/cointelpro-black-extremists-part-13-of-1/view , 2019 FBI cannot complete FOIA request on "StormFront" white supremacist group website, indicate StormFront is FBI https://www.muckrock.com/news/archives/2019/jul/01/fbi-stormfront-missing-records/ ; +ADD Tech CEOs employing Stasi-created COINTEL tactics https://www.washingtonpost.com/technology/2020/06/15/ebay-former-employees-cyberstalking/

+ADD New York Governor Andrew Cuomo and his prominent role in draconian measures taken during the pandemic, media-policy relaying interactions with his brother Chris Cuomo CNN News Anchor who publicizes his contraction of virus[372] "Andrew Cuomo lauds Chris Cuomo for broadcasting despite coronavirus diagnosis: 'Gutsy, courageous thing to do'" *The Hill*, Joe Concha - 04/01/20; "Andrew and Chris Cuomo Bickering Like Children on Live TV Is Just the Social-Isolation Tonic I Needed" *The Slate* Heather Schwedel March 17, 2020: "I report that there's a clip circulating of CNN host Chris Cuomo and his brother, New York Gov. Andrew Cuomo, in the midst of an actual pandemic, bickering on-air about which one is their mother's favorite—… The segment, which aired on CNN on Monday night, started to go off the rails when, in response to a question about the possibility of imposing a curfew to keep people from spreading the virus, the governor said, 'I don't like the word curfew. Dad tried to have a curfew with me. I never got past the resentment.' The anchor, younger brother Chris, was clearly surprised—watching the comment register on his face is amazing—and tried to come up with a funny response, but this only triggered the elder Andrew ('YOU violated the curfew all the time'), and the interaction devolved from there: Chris told Andrew to call Mom, Andrew said he did and that Mom said he was her favorite, and so on. Yet, all while the state that Andrew governs—and the country that Chris covers as a journalist—is experiencing a literal once-in-a-lifetime emergency."[373]

[TOPIC - VNN as media spectacle and speculative fiction]

https://www.fema.gov/pdf/privatesector/ps_notes_ttx_power.pdf (pg 10 VNN fake news broadcast video from FEMA for disaster scenarios); https://www.govtech.com/em/emergency-blogs/disaster-zone/FREE--FEMA-Tabletop.html ; https://www.youtube.com/watch?v=FtFPUdzPz6I "VNN Disaster Scenario News Broadcast"

[372] https://thehill.com/homenews/media/490613-andrew-cuomo-lauds-chris-cuomo-for-broadcasting-despite-coronavirus-diagnosis
[373] https://slate.com/news-and-politics/2020/03/andrew-chris-cuomo-cnn-arguing-clip.html

; https://www.fema.gov/media-library-data/20130726-1833-25045-2267/mom_ttx_video_inject_scripts_final_508.pdf ; https://www.youtube.com/watch?v=udemJGMEN54 RaffertyWeiss Media uploaded 2016 pt 3, pt 2 https://www.youtube.com/watch?v=JMCZrCkjnxs 2014 (on fictional Puerto Rico hurricane earliest upload 2014 - hurricane Maria in 2017), Part 1 https://www.youtube.com/watch?v=K-bMnQRobqw ; Fake Northeast Africa countries 'Bloomland' & 'Golva' shown on map VNN report scenario w/ Persian and Arabic speakers featured from real news reel https://www.youtube.com/watch?v=UTqbmqkYuqw

Event 201 10/18/2019 pandemic simulations in NY (World Military Games Oct. 18-27 in Wuhan) http://www.centerforhealthsecurity.org/event201/media

+ADD more on performance theory https://www.brown.edu/Departments/Joukowsky_Institute/courses/architecturebodyperformance/files/257077.htm

Cyber Realism

The whole political world is swirling around, even for the eyes of the shrewdest observer, like dispersing atoms.
Carl von Clausewitz, *Letters from Berlin*, 1808

Units – Structural – Politics of Force – Security

+ADD on Nuclear combat through cyberarms and cyberspace. Nuclear combat is real phenomenon, aka "cyberwarfare"

Cyber realist assessments can be achieved with just functional knowledge of information today. Take, for example, the glaring inconsistencies between US Army Intelligence accounts of an US attack on a Doctors Without Border hospital in Afghanistan and other information that can be found online about that and other attacks in Afghanistan.

The Army Intelligence account comes in the form of a book review of the 2021 publication *Eagle Down: The Last Special Forces Fighting the Forever War* by Wall Street Journal reporter Jessica Donati. The book focuses specifically on retelling US Special Forces accounts of the continued presence of Special Forces despite the alleged end of US occupation in Afghanistan. Written by Army Intelligence Officer James King, the review begins: "On October 3rd 2015 a United States Air Force AC-130 conducted an air strike in support of US Special Forces under attack in Kunduz, Afghanistan. **Mistaking the building below for a Taliban stronghold, the AC-130 instead hit a Medecins Sans Frontieres (Doctors without Borders) hospital** in the heart of the city, ultimately killing 42 people."[374]

It is nearly impossible that Army Intel Officer King is being frank in his assessment of the airstrike. His book review is an attempt to control the narrative on the October 2015 attack. It

[374] King, Lieutenant Colonel James. "Review - Eagle Down: The Last Special Forces Fighting the Forever War". *Small Wars Journal*. 23 February 2021.

is a contribution to a military deception operation obscuring an attack taken in violation of International Humanitarian Law. With a simple Internet search, one can find a map identifying cities hosting Doctors Without Borders sites in Afghanistan, as well as the names of the hospitals and a description of the services of all DWR-affiliated hospitals, readily available on the Doctors Without Borders public-facing website.[375] Furthermore, the hospital had been publicly designated a Doctors Without Borders trauma center since 2011.[376]

In contrast to Army Intel Officer King's assessment, DWB, or *Medecins Sans Frontieres* (Doctors without Borders), reports that the hospital was the target of *multiple* airstrikes by the US Air Force at the behest of US Special Forces. DWB reports:

> During the early morning hours of Saturday, October 3, 2015, MSF's trauma hospital in Kunduz, Afghanistan, came under precise and repeated airstrikes by United States forces. The main hospital building, which housed the intensive care unit, emergency rooms, laboratory, X-ray, outpatient department, mental health, and physiotherapy ward, was hit with precision, repeatedly, during each aerial raid, while surrounding buildings were left mostly untouched.[377]

In the *Eagle Down* publication, US Special Forces depict their situation as pathetic. "'We don't know what our goals are because they keep changing all the time,' one of the main Green Berets featured in the book tells his superior while deployed to Helmand province. 'You don't know what we're supposed to be doing, yet you keep sending us on crazy missions where we could all die for no reason.'"[378]

In complete contrast to the depiction of an underfunded group conducting hapless airstrikes and braving deadly missions, security in Afghanistan has deteriorated in highly strategic ways under the authority of US Special Forces and a party deemed strategic partners of US forces since the signing of the U.S.-Taliban Agreement of February 2, 2020.[379]

In a report found on *Stars and Stripes*, it is reported that not a single US soldier has been killed in Afghanistan in 2020, and that the billions of dollars funding exclusively Special Forces operations in Afghanistan are reportedly not making their way to Afghan national forces. **In strategic attacks that seem to be confused over whether the year is 2002 or 2020, the Taliban, now US Special Forces strategic allies, are used to justify the deterioration of plans for national peace talks.** The article reports:

> Instead of peace, **Taliban offensives swept the country, overrunning checkpoints and surrounding key cities** like Kandahar and Lashkar Gah. Attacks last summer and fall [2020] were 18% higher than the same period the year before the deal, the United Nations said. **While no U.S. troops have died in combat since the signing of the deal last February, Afghan forces lost nearly 10,000 soldiers and police in dozens of Taliban attacks last year [2020]**, officials said. **More than 3,000 civilians also died amid a surge in assassinations against government officials and religious leaders, the U.N. said**. Afghan

---

375 https://www.doctorswithoutborders.org/what-we-do/countries/afghanistan
376 https://www.doctorswithoutborders.org/what-we-do/news-stories/news/afghanistan-msf-demands-explanations-after-deadly-airstrikes-hit
377 https://www.doctorswithoutborders.org/what-we-do/news-stories/news/key-msf-publications-about-kunduz-hospital-attack
378 https://www.stripes.com/news/middle-east/eagle-down-examines-the-secretive-role-of-us-special-forces-in-afghanistan-1.659578
379 https://www.state.gov/wp-content/uploads/2020/02/02.29.20-US-Afghanistan-Joint-Declaration.pdf

> security forces faced severe morale and supply issues as they fought the emboldened Taliban, said **Abdul Mateen Sulaimankhail, a brigade commander** in eastern Logar province last year. **"I had to lie to my soldiers, that we had air support and ammunition**, to keep them fighting," Sulaimankhail said. **The continuing bloodshed has undermined public support in Afghanistan for the long-delayed peace talks between the Kabul government and the Taliban,** the Freedom's Sentinel report said.[380]

In strategic assessment, the 2020 resurgence of the Taliban as *mujahidin* situates the US as strategic interlocuters between irreconciled domestic authorities in Afghanistan. In **cyber realist assessment, the narrative inconsistencies highlighted here and their strategic publication as part of a military deception**, as well as the political strategy behind the attacks, **could be ascertained with a basic Internet search.**

"The rate of acceleration that events alone – without consideration of technological advancement – have brought into the world of cyberspace has certainly left such a view well in the rear view mirror. **Uncertainty no doubt still exists, but it can be argued to exist as a purposely strategic application of cyber methods**…"[381]

Joint Forces: "**MILDEC employs three basic means: physical, technical, and administrative.** Employ these means independently or in collaboration depending on the situation. The applications of tactics vary with each operation depending on variables such as time, assets, equipment, and objectives and are assessed for feasibility accordingly. MILDEC operations apply four basic deception techniques: feints, demonstrations, ruses, and displays. MILDEC procedures vary with each MILDEC operation and are conducted in accordance with the commander's guidance and **the processes used to synchronize the tactics and techniques in real time**. MILDEC as a Capability of Information Operations: MILDEC and other information operations (IO) capabilities must be planned and integrated to support the commander's campaign and/or operation. **Collectively, these capabilities target adversary decision makers to affect their information systems and decision-making processes**."[382]
[MOVE?] "Technical Means: Those military material resources and their associated operating techniques used to convey or deny selected information to an adversary. As with any use of US military material resources, any use of technical means to achieve MILDEC must comply with domestic and international law. A variety of technical means include: **(a) Deliberate emission, alteration, absorption, or reflection of energy. (b) Emission or suppression of chemical or biological odors. (c) Multimedia (radio, television, sound broadcasting, computers, computer networks, smart phones, and personal digital assistants).**"[383]
"The deception target must be capable of causing the desired action(s) or inaction(s) to occur. The target has the authority to make decisions that will aid US forces in achieving the desired deception objective. There must either be existing conduits to the deception targets, or there must be a reasonable expectation that conduits to the deception targets can be established. During

---

[380] https://www.stripes.com/news/middle-east/deal-meant-to-end-war-in-afghanistan-seen-to-embolden-taliban-1.663800
[381] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 93.
[382] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. ix
[383] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-8

development of the deception, sufficient intelligence regarding the deception target should exist to determine what (if any) preconceived perceptions the deception target may have. History has shown that deception operations that play upon the preconceived perceptions of a deception target have been very successful. The MILDEC planner should submit request for information (RFI) inputs to the intelligence community (IC) requesting behavioral influence analysis (BIA)/human factors analysis (HFA) data on adversary military, paramilitary, and VEO [violent extremist organization] decision makers."[384]
"Within MILDEC, conduits are information or intelligence gateways to the deception target. Conduits may be used to control flows of information to a deception target. It is rare that a deceptive message is sent directly to the deception target itself. Most often, deception messages are sent to intelligence collectors (conduits) with the expectation that the deceptive message will systematically make its way to the deception target. Examples of conduits include FISS, intelligence collection platforms, open-source intelligence, and individuals through whom information reaches the deception target. The development and utilization of conduits should be approached systematically. A path should be discernable from the initial input to the conduit to the deception target. Ideally, conduits are part of a closed loop system which facilitate and enable feedback regarding receipt of the deceptive message by the intended deception target and whether or not the desired adversary actions are occurring or will occur. Factors to be considered include: Are there stop gaps between the initial receptor and the final desired end point (the deception target)? Are there filters that might skew the desired perception? Are there conduits that might potentially validate or contradict the desired message? In the case of FISS, could the conduit potentially serve as a feedback mechanism?"[385]

"Political realism is the oldest and most venerated theory of international politics. Yet, there is no institutional center dedicated solely to its study. Its thinkers and practitioners range from Thucydides, Machiavelli, and Hobbes, to E.H. Carr, Hans Morgenthau, Reinhold Niebuhr, Winston Churchill, George Kennan, to Kenneth Waltz, Robert Gilpin, Robert Jervis, and John Mearsheimer. As this extensive list suggests, there is no single realist theory. **Realism is, instead, a theoretical perspective—a family of theories and explanations, differing from each other in the emphasis they place on distinct causal variables.** That said, there is no doubt that realism constitutes a coherent tradition of explaining political behavior. Centered on an understanding of politics as an enduring struggle for power and security, realism has consistently sought to explain how entities seek to survive and thrive in an environment in which dangers to security and welfare are ever-present, and even survival itself is not assured.
All realists agree that the balance of power (and changes to it), as well as the systemic pressures generated by an anarchic international order more generally, inform the environment in which all states act. In that context, however, all states, and especially great powers, enjoy considerable discretion with regard to how they pursue their goals and what sacrifices they make in the face of constraints. It is thus impossible to understand and anticipate the behavior of states by looking solely at structural variables and constraints. To explain world politics, it is necessary to appeal to a host of other factors, including domestic politics, history, ideology, **and perceptions of legitimacy.** Unlike contemporary structural realists, classical and neoclassical realists take

[384] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-4
[385] https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf p. I-4 – I-5.

domestic politics and other such variables seriously. They understand that state behavior is shaped by the lessons of history, ideas, and ideology and that **states are not best understood as hyper-rationalist machines but that they make choices conditioned by those influences** and in a context of considerable uncertainty… In stark contrast with liberal hegemony, realism champions a narrow definition of the national interest, **which does not include things like democracy promotion, humanitarian intervention, the responsibility to protect people from atrocities or the advocacy of human rights abroad, or nation building**."[386] [causal variables as opposed to paradoxical thinking; perceptions/recognition of legitimacy as opposed to roleplay and assuming identity of other; hyper-rational machines (while not researching conditions in which choices are made – Chalmers book review critique of RAND as hyper-numerical[387]; against democracy promotion: premise of this essay, spells out the devastating results of democracy promotion and international interventions by the US and proves that claims that those promotions/interventions are done with good intention are false and explicitly contradicted by same.

+ REWORD As it applies today to warfare as targeted genocides based on *de*aggregated data, 'genocide' may defy traditional concepts of 'group' or 'community'. Persecutions may be based on other information collected, which was the case as well in the European Holocaust, wherein IBM cross-indexed career, place of residence and other factors with race, religion and ethnicity in order to identify targets.

In the 21st century Information Age, concepts of 'group' may include groupings of individuals by web queries, Internet search history, IP addresses, purchases, payment methods, location check-ins, software downloaded, e-books viewed, languages enabled on computer, disability plug-ins, voice recognition identification, and a host of other behavioral traits collected regularly by corporate advertisers. For example, a surveillance State could feasibly choose to target for genocide all individuals who search "symptoms of cancer", "international adoption agencies", "secret government societies", "how to tell if your phone is hacked", "side effects of PTSD medication", "how to apply for a foreign work visa". A surveillance state could target individuals who download an encrypted browser and firewall software, a language learning software to study Chinese, or audio books regularly downloaded by the blind. A state could have reason to target individuals who regularly make late bill payments, listen to songs with violent lyrics, routinely do app check-ins at very expensive restaurants and boutiques, have more than two children identified in a contact list, visit the medicare website, do not use social media at all or use it excessively, or who telecommunicate so infrequently as to be termed anti-social. Without there being an apparent link to religion, race, ethnicity, or disability, these groups are regularly identified by behavioral traits in their use of technology, and grouped in demographic categories for targeted advertising. These demographics, as specific as they may seem, may be produced and purchased by government agencies and contractors in order to identify, target and eliminate undesirable targets, rising targets (such as children, young adults, or persons in change), or high-value targets, without fitting existing definitions of genocide as the intended destruction of "national, ethnical, racial or religious groups".

---

386 "About: Program for the Study of Realist Foreign Policy". Program for the Study of Realist Foreign Policy of The Ohio State University's Mershon Center for International Security Studies. https://u.osu.edu/psrfp/about/

387 Johnson, Chalmers. "A Litany of Horrors: America's University of Imperialism". *Tomgram: Chalmers Johnson, Teaching Imperialism 101*. TomDispatch. 29 April 2008.

[TOPIC – emphasize physical violence capabilities of EW radar]

+ADD Monopoly on Violence - Hard power of hardwares, https://www.who.int/peh-emf/publications/facts/fs226/en/ WHO "Electromagnetic fields and public health: radars and human health", National Intelligence Council: "Although we believe the appeal of al-Qa'ida and other international terrorist groups will diminish over the next 15-20 years, pockets of support will remain, ensuring a continuing threat, particularly as lethal technology is expected to become more accessible."[388] The physical violence capable with cyber hardware and software is addressed in detail in the section The Hacker's Arsenal.

Daniel Steed, lecturer of Strategy and Defense at the University of Exeter, writes in *The Politics and Technology of Cyberspace:*

> The sheer resilience of cyberspace networks poses a security challenge to the state itself... increasing internationalisation and privatisation have been enhanced by these technological developments, diminishing the importance of the state. That diminishment lies in the reduction of the state's monopoly over information itself, enabling the creation of new breeds of non-state actors to operate in this low cost of entree space. Actors such as Wikileaks, Anonymous, and the range of advanced persistent threats (APT) groups are the clearest example of those widely known about, who have delivered disproportionate effect thought their actions in cyberspace. If a state wishes to throttle and block the dissemination of information, packet switching is a reliable and automated means of ensuring that the packets simply find the most reliable route - through, around, and beyond sovereign territorial boundaries - to its recipient. If 'Information is a key way by which… power operates and develops,' then packet switching is a key enabler for the distribution of information, and therefore power, away from the state and to the individual.[389]

The US National Intelligence Council concurred with this estimate when it wrote in 2009 that in the future:

> Even in the military realm, where the US will continue to possess considerable advantages in 2025, advances by others in science and technology, expanded adoption of irregular warfare tactics by both state and nonstate actors, proliferation of long-range precision weapons, and growing use of cyber warfare attacks increasingly will constrict US freedom of action… Concurrent with the shift in power among nation-states, the ***relative*** power of various nonstate actors—including businesses, tribes, religious organizations, and even criminal networks—will continue to increase. Several countries could even be "taken over" and run by criminal networks.[390]

This emphasis on cyber threats, cyber measures to mitigate real world threats, and the lack of strategic historic precedent that may diminish quality of life in the future indicates to many that an approach defined by cyber-realism can be applied to already experienced threats and harms, not necessitating risky experimentation with current threats, or dystopian imaginings.

---

[388] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 61.

[389] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 10.

[390] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. xi; 1.

Cyber realism is not only an effective approach once applied, but it is optimistic despite its name. Its basis suggests that we already have the answers to our problems in our knowledge of the systems in which they occur. **Cyber realism can also be called 'operational analysis'.**

Preeminent sociologist Max Weber in *Politics as a Vocation* named "matter-of-factness" to be a necessary quality in political vocations:

> This is the decisive psychological quality of the politician: his ability to let realities work upon him with inner concentration and calmness…Whoever wants to engage in politics at all, and especially in politics as a vocation, has to realize these ethical paradoxes ['ethic of ultimate ends' and 'ethic of responsibility'(ADD page cite)]. He must know that he is responsible for what may become of himself under the impact of these paradoxes. I repeat, he lets himself in for the diabolic forces lurking in all violence… Everything that is striven for through political action operating with violent means and following an ethic of responsibility endangers the 'salvation of the soul.' If, however, one chases after the ultimate good in a war of beliefs, following a pure ethic of absolute ends, then the goals may be damaged and discredited for generations, because responsibility for *consequences* is lacking, and two diabolic forces which enter the play remain unknown to the actor… what is decisive is the trained relentlessness in viewing the realities of life, and the ability to face such realities and to measure up to them inwardly.[391]

Steed defines cyber realism as threats to States' fear, honor, and interests. He cites political "talk of a 'digital Pearl Harbor'," the risk of cybercrime towards "the exposure of intimate state secrets... and providing instant ways of going viral." Additional risks include the fact that "American cyber interests lie everywhere—from the communications that its military relies on, to the infrastructure that now underlies the global economy". He writes of his efforts toward cyber realism:

> Strategy is an instrumental activity that cannot operate in ignorance of the purpose toward which means are applied… beginning to apply existing models of political thought to the *why* such a thing [cyber war] matters illustrates the political implications of the subject… To neglect the political nature of war in our talks on cyber affairs is to jettison our own foundation of thinking about war and strategy. We cannot make the instrumental linkage between cyber power and political design that strategy is intended to support until the politics of cyber are better understood. For an arena as important as cyberspace, it is about time we start applying the realist view to the politics of any potential cyber war, lest we find ourselves up against an adversary who matches their cyber ends, ways and means in a better strategic fashion than we do.[392]

[TOPIC – Infringement]

In 2008 the US National Intelligence Council anticipated in *Global Trends 2025* in a section titled "The Prominence of the Non-military Aspects of Warfare" that, "Non-military means of warfare, such as cyber, economic, resource, psychological, and information-based forms of conflict will become more prevalent in conflicts over the next two decades. In the future, states

---

[391] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 115, 125-26.

[392] Steed, Daniel. "Cyber War, let's get reali(ist)". *War on the Rocks*. 14 October 2013. Internet resource.

and nonstate adversaries will engage in 'media warfare' to dominate the 24-hour news cycle and manipulate public opinion to advance their own agenda and gain popular support for their cause."[393] … "that democracy not break out"[394]

In *The CNN Effect in Action: how the news media pushed the West toward war in Kosovo*, author Bahador writes:

> Realism assumes that state behavior is determined by the pursuit of national interests and security, bounded by power relative to other states... Such models, like realism, assume unitary governmental decision-making with a high degree of control over implementation and access to near-perfect information.[395]

I suggest defining high degree of control and high degree of access to information in the terms defined in the same chapter, characterized by control of and information to the three domains necessary to war: "popular passions, operational instruments, and political objectives". These could alternatively be called public opinion, technology, and policy.

An additional realist paradigm made on the three domains of war "To carry on war, three things are necessary: money, money, and yet more money."[396] Gian Jacopo Trivulzio (1440-1518)

These three arms of war from Carl von Clausewitz's *On War* (1832) are outlined in Bahador's chapter "The CNN Effect and War".[397] Due to political proclivities towards bureaucratic stances of plausible deniability, it is important to imbue states or quasi-states with responsibility for war when they reasonably have access and control over a nexus of these three domains.

+ADD "In the west, we see a complete media darkness where it comes to Yugoslavia, because world global networks have been assigned the task of being an instrument of war and of disinforming the public."[398] Milosevic at The Hague War Crimes Trials

http://law.emory.edu/eilr/content/volume-33/issue-1/articles/quasi-states-aggression-ICC-statute.html

If we are to use sociologist Max Weber's definition of the State as those who hold a monopoly on violence and coercion over a territory, which must become defined as such through "a process of legitimation", we would be compelled to assume that either hacker collectives have become the authorized state over the State, or that they act with the authority and permission granted by the State. In fact, Anonymous, the hacking collective, explicitly claims to

---

[393] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 71.
[394] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 39.
[395] Bahador. *The CNN Effect in Action*, p. 57-58.
[396] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 362.
[397] Bahador. *The CNN Effect in Action*, p. 47.
[398] https://www.theguardian.com/world/2002/feb/14/warcrimes1

"have launched other efforts while also building new strategies and recruiting individuals from across the globe - some of whom hold significant positions in media, industry, and the sciences."[399]

This represents yet another fairly early explicit claim by a hackers' group ignored by should-be-critics-turned-defenders, individuals who do not admit belonging to the group or acting on behalf of it - likely in order to fulfill their roles within the group as fair-minded third-party vouchsafes to the outside.

https://www.cyberscoop.com/western-allies-consider-offensive-cyber-warfare-pact-as-russia-launches-plan-for-independent-internet/

+ADD "NATO will establish new command centers allowing the transatlantic alliance to incorporate cyberweapons and cybersecurity across the board in operational planning"… "For NATO, it is always our aim to use minimum force to achieve maximum effect and therefore cyber effects may be the best response."

This statement in late 2017 from NATO Secretary-General Jens Stoltenberg states clearly that cyber warfare is now NATO's weapon of choice for all strategic and tactical action it takes. The article goes on to state:

> In July, U.S. intelligence community veteran Kevin Scheid became general manager of NATO's Communications and Information Agency, which controls a $3.4 billion IT and cybersecurity modernization program. 'We must be just as effective in the cyber domain as we are on land, at sea and in the air, with real-time understanding of the threats we face and the ability to respond however and whenever we choose,' Stoltenberg said...[400]

The statement and actions of NATO and the US cyber intelligence community indicate that they will have increasing reason to prevent cyber laws from being applied, with no comparable oversight of their cyber or 'kinetic' actions, no matter however or whenever they act illegally or unfairly.

An indication of what however and whenever may mean in the cyber domain, beyond capabilities, represents the position of the Free Internet movement. Free Internet-ers earliest proclamation was issued in 1996 from the Electronic Frontier Foundation's John Perry Barlow, copied in full as follows:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you

[399] Anonymous. "Opinion: Anonymous and the global correction".

[400] O'Neill, Patrick Howell. "NATO will establish new cyber command centers". *Cyber Scoop.* 9 November 2017.

know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and

> distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.
>
> These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.
>
> We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.
>
> Davos, Switzerland, February 8, 1996[401]

+ADD "The leader of the US delegation to the GGE [Group of Government Experts] Michele Markoff, released a statement in the aftermath of the collapse berating 'those who are unwilling to affirm the applicability of these international legal rules and principles,' with such countries believing that they 'are free to act in or through cyberspace… with no limits or constraints on their actions… This is a dangerous and unsupportable view.' Two core narratives have emerged to explain the breakdown of the GGE, the first focuses on the intransigence of Cuba late in the process, who argued that proceeding as outlined would lead to a militarisation of cyberspace because of the right to self-defence included in the UN Charter, insisting instead on seeking peaceful resolution to disputes. The other narrative is that the difference of positions between those for Cyber Sovereignty and those for the Free Internet Coalition are simply irreconcilable… Second is simply the question of how diplomacy will now continue. This is a very concerning position, because while diplomacy to shape acceptable international standards and norms stagnates, the continued occurrence of cyber security events in the vein of WannaCry and Not-Petya all help the Cyber Sovereignty advocates in 'making headway with their core wish: the framing of information as a weapon.'"[402]

Anonymous is, as it claims, a "worldwide" collective,[403] this much in the way, I suggest, NATO could be called a loose collective of like-minded individuals representing many significant positions in significant industries, with the option to take part or refrain from taking part in any operation. [CITE NATO charter]

+ADD "**NATO's StratCom Center of Excellence** has reported on the limited effect of social media trolling on Latvia's population. However, the publication, entitled **'Internet Trolling as a Tool of Hybrid Warfare**: the Case of Latvia,' notes the increasing use of **'hybrid trolls' — hired trolls that communicate particular messages as determined and directed by a particular state** — as opposed to individual social media spammers who merely intended to shock or threaten. **This has triggered the emergence of Baltic 'elves'** — volunteer internet users dedicated to tracing trolls and challenging Russian propaganda online. Ricardas Savukynas

---

[401] Barlow, John Perry. "A Declaration of the Independence of Cyberspace". *Electronic Frontier Foundation webpage*. 8 February 1996.

[402] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 77-78.

[403] Anonymous representative of Anonymous. "A hacktivist message announcing at 'Anonymous Operation Last Resort'".

started the elves network following events on Maidan Square in Ukraine that included clashes between protestors and pro-government forces of the Russian-backed President Victor Yanukovych… 'Now, we see signs of the Kremlin increasingly recruiting Lithuanian speakers abroad to spam indistinguishable comments from bots,' said Savukynas. 'They receive small amounts of money, we found, when Kremlin recruiters mistakenly contacted some of our 'elves.'"[404]

Cyberpolitical analysts from NATO Strategic Communications Centre write in *Internet Trolling as a Tool of Hybrid Warfare: the Case of Latvia*: "Herein lies the difference: a classic troll acts with no apparent instrumental purpose, whereas purported hybrid trolls (as we have labelled hired, pro-Russian trolls), communicate a particular ideology and, most importantly, operate under the direction and orders of a particular state or state institution."[405]

The backstage of information warfare is described by *The Guardian* journalist Shaun Walker in his 2015 article "The Russian Troll Factory at the Heart of the Meddling Allegations":

> Just after 9pm each day, a long line of workers files out of 55 Savushkina Street, a modern four-storey office complex with a small sign outside that reads 'Business centre'. **Having spent 12 hours in the building, the workers are replaced by another large group, who will work through the night. The nondescript building has been identified as the headquarters of Russia's 'troll army', where hundreds of paid bloggers work round the clock** to flood Russian internet forums, social networks and the comments sections of western publications with remarks praising the president, Vladimir Putin, and raging at the depravity and injustice of the west. The Guardian spoke to two former employees of the troll enterprise… both said **they were employed unofficially and paid cash-in-hand.** They painted a picture of a work environment that was humourless and draconian, with fines for being a few minutes late or not reaching the required number of posts each day. Trolls worked in rooms of about 20 people, each controlled by three editors, who would check posts and impose fines if they found the words had been cut and pasted, or were ideologically deviant… **There was no contract - the only document she signed was a non-disclosure form.** She was ordered not to tell her friends about the job, nor to add any of them to the social media accounts she would run under pseudonyms. 'We had to write 'ordinary posts', about making cakes or music tracks we liked, but then every now and then throw in a political post about how the Kiev government is fascist, or that sort of thing,' she said. **Instructions for the political posts would come in 'technical tasks' that the trolls received each morning, while the non-political posts had to be thought up personally**… 'First thing in the morning, **we'd come in, turn on a proxy server to hide our real location**, and then read the technical tasks we had been sent,' he said… Lawyers in St Petersburg said it was extremely rare for such **a big enterprise to be working entirely on the 'black economy', not paying any tax and not officially registering its employees.**[406]

+ The Hacking Team, etc and US government employment of hackers, Bill Clinton's thriller novel The President is Missing about hackers employed by US in cyberterrorism attack. Hacking

---

[404] https://www.dw.com/en/baltics-battle-russia-in-online-disinformation-war/a-40828834

[405] Spruds, Andris, Anda Rozukalne, Klavs Sedlenieks, Martiins Daugulis, Diana Potjomkina, Beatrix Tolgyesi, Ilvija Bruge, and Alexander Fokin. *Internet Trolling As a Tool of Hybrid Warfare: The Case of Latvia*. Riga: NATO Strategic Communications Centre of Excellence, 2015. Internet resource. https://stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0 p. 10

[406] https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

culture of crime, The Hacker Forums and human 'girl slave' trafficking. State sponsored terrorism.

I would not be surprised to come across more information suggesting ISIS to be an offshoot of Anonymous in Syria and Iraq due to their appearance following the Arab Spring, common forums used online, recruitment methods, age and gender of members, practices of female and child sex trafficking, hacking, coups, war crimes, cooperation at one time with the US government, and other elements of their organized criminality.

In apparent return business for Twitter following the 2011 Twitter Revolution in Syria, in March 2013, Senator McCain shared news on his Twitter account that the US was shipping 200,000 MREs [meals ready-to-eat] to the "Free Syrian Army".[407]

In 2013 Syrian fighters' groups were not determined to be in-line or out-of-line with US policy objectives as they were especially amorphous (even for the region) and unreliable in their ideologies. Nevertheless, US politicians associated and even boasted about sending US military food supplies to the groups.

A few months after his MRE tweet, in May of 2013 McCain shared a group photo of himself on an "Important visit with brave fighters in #Syria who are risking their lives for freedom and need our help".[408]

+ADD, Aug 1 2013(?) (Reuters) – "President Barack Obama has signed a secret order authorizing U.S. support for rebels seeking to depose Syrian President Bashar al-Assad and his government, U.S. sources familiar with the matter said."[409]

Unsurprisingly then, in August 2014 Senator McCain wrote on his Twitter account as part of a domestic partisan argument that, "#ISIS is largest, richest terrorist group in history & 192,000 dead in #Syria".[410]

In the 2014 VICE News documentary *The Islamic State (Part 1),* what appears to be the same Syrian man pictured with John McCain as "a brave fighter" is shown as ISIS Press Officer nicknamed "Abu Mosa". [411] Ideologically, we learn from the documentary that ISIS members are obsessed with removing the borders created through the Sykes-Picot Agreement – another reference to The Great Game political era. [ELABORATE]

Tactically, we learn from VICE News that ISIS members drive US tanks with extreme facility, and it is of course no secret that ISIS has driven US military tanks throughout their occupation of Syria and western Iraq.[412] [+ADD electronic weaponry discussion here]

+NATO supplies through Turkey, Turkish officials protecting ISIS members, Turkish police sent to guard ISIS article [413]

---

[407] https://twitter.com/senjohnmccain/status/312334156665335808

[408] https://twitter.com/senjohnmccain/status/339455679800700928?lang=en

[409] https://www.huffpost.com/entry/obama-secret-syria-order_n_1730712?tw_p=twt&guccounter=1

[410] https://twitter.com/senjohnmccain/status/505094561434451968?lang=en

[411] https://video.vice.com/en_us/video/the-islamic-state-part-1/55a8222337d5f90048b624c9

[412] https://video.vice.com/en_us/video/the-islamic-state-part-1/55a8222337d5f90048b624c9

[413] Nafeez, Ahmed. "Whistleblower exposes how NATO's leading ally is arming and funding ISIS: 'I am the police chief who was asked to guard ISIS terrorists'". *Insurge Intelligence.* 16 September 2016.

+ADD "Security analysts and cartel sources agree that a key factor in the transformation of underworld rivalries **into a full-throttle war** has been **the cartels' recruitment of elite soldiers. The leakage of Mexican special forces into organized crime** began in the 1990s when the powerful Gulf cartel recruited a group of ex-Gafe troops to create its own paramilitary enforcement unit, known as Los Zetas. … According to Mexico's defence ministry, **about 1,383 elite soldiers deserted between 1994 and 2015**. Defectors included members of **units that received training in counter-terrorism, counter-intelligence, interrogation and strategy** from French, Israeli and US advisers, according to a 2005 FBI intelligence document. … **According to Kate Doyle, senior analyst at the National Security Archive** in Washington DC, the US focus on military aid to the region has helped drive the militarization of Mexico's drug conflict. **'That US military training and intelligence techniques ended up in the wrong hands is far from unusual. Its lethal spillage into the contemporary criminal context is one of the legacies of US security policy in Latin America,'** she said. … At the height of the cartel's power, nothing in Michoacán moved without the cartel's permission. It monopolized crime, but it also penetrated ordinary life, **using the threat of lethal violence to arbitrate anything from land disputes to marital conflicts. That soft power was fused with strategic sophistication, thanks to the influx of former soldiers**, said Correa-Cabrera. **'Their rapid expansion, the way they controlled territories, used communications and armament** – they were now doing it like the army,' she said. … Delfino's role in the bloodletting **is no secret to his former brothers in arms. He remains in touch with soldiers on active duty, and even meets up to reminisce when security conditions allow**, he said. 'We like each other, and they respect my decision,' he said, '**but if they learn that I'm out here doing something which doesn't square with our values – if I mess with innocent people – they will come for me**. From them, there's no hiding.'"[414]

Under the Trump Administration, the Pentagon ordered the assassination of Iranian General Solemani, who is understood to have been a principle strategist against ISIS forces in Iraq.[415]

+ADD "While the media's attention is focused on the transgressions of social media companies relating to privacy, data collection, and Putin's election interference, ISIS has slowly rebuilt its online presence after its battlefield defeats in Iraq and Syria. Although the Islamic State was forced out of nearly all the lands it conquered, it still controls over 1,000 square miles of Syrian territory, or roughly the size of the city of Los Angeles, according to the NYT. Counter terrorism officials are increasingly worried that ISIS has shelved its "incite and recruit" social media campaigns in favor of creating multi-lingual social media "terrorist academies" providing elementary instruction on how to manufacture lethal poisons and explosives such as triacetone triperoxide (TATP), how to make pipe and gas tank bombs, how to navigate the ins and outs of "rent and ram" terrorism, and, most recently, how to breach cyber security safeguards protecting soft targets, such as surface transportation links in European cities."[416]

---

[414] Ernst, Falko. "'The training stays with you': the elite Mexican soldiers recruited by cartels". *The Guardian*. 10 February 2018.

[415] https://www.bbc.com/news/world-middle-east-51021861 (2020)

[416] https://thehill.com/opinion/national-security/401282-what-isis-is- -to-during-your-summer-vacation

Jesse Morton now works with the same NYPD Director of Intelligence Analysis who arrested him, Mitch Silber, now Columbia University Professor of Public and International Affairs. Morton is still disseminating publications (of a now different opinion) after serving 3.5 years of an 11.5 year sentence for al-Qa'eda-linked "terrorist activity".[417] As Morton recollects, "I'd begun my trek out of extremism and had become an asset of the FBI,"[418] and now of Columbia University's Public and International Affairs Department Chair.

Overall, I would argue that ISIS is at its base a hacker group facilitated in its methods of spreading by the US media technology industry. Media do not only form public opinion on these groups and issues in their analyses disguised as reports, but the US media has functioned as point persons for guerilla groups that are alleged not to have connections with States or official ways to be communicated with. US media offers themselves as sole channels to enemy groups for statesmen who cannot be seen 'negotiating with terrorists', yet who are alleged to be too important to international security to be ignored.

Simultaneously we are supposed to accept media as the gatekeepers to communication with these groups and also to assume no cyber realism. That is, that media and states are completely unaware and powerless to stop the militants from misusing their channels to disseminate terrorist propaganda, like seen in ISIS Twitter recruitment, or in state officials' cavorting with guerilla fighters in the media.

Early on, US politicians denied realities on the ground and funded militants of any identification or ideological persuasion, feeding them US military rations and arming them. US motives, I believe, are clear in the results of their efforts in Syria and Iraq; lifelong politicians like Senator McCain and any in the establishment cannot be considered ineffectual by any measure. Interference by these individuals invariably leads to situations like that termed by former Vice President Joe Biden "the Bosnia Model".

These groups are not investigated and are licensed and paid by the State to commit cybercrime. The individuals are allowed to conduct their crimes in full view of the State, to act as semi-contracted criminal organizations, like Anonymous, that can be thrown at any legitimate or other criminal enterprise as seemingly non-state actors to sabotage, harass, surveil and physically harm, without damaging the reputation of the State. Such as in this instance:
False flag attacks/false flag terrorists
https://reason.com/2016/08/31/the-fbi-distributes-child-pornography-to/
https://www.theguardian.com/world/2011/nov/16/fbi-entrapment-fake-terror-plots
https://www.thedailybeast.com/the-fbi-makes-a-bizarre-claim-about-pro-choice-terrorism
+ADD from "False Flags as a Method of Information Warfare"[419] International Affairs Vol. 65, No. 3 (2019), pp. 119-132 by Ivanov

---

[417] Morton, Jesse and Mitchell Silber. "NYPD vs. Revolution Muslim: The Inside Story of the Defeat of a Local Radicalization Hub". *CTC Sentinel, Vol. 11, Issue 4.* Combating Terrorism Center at West Point. April 2018.
[418] Morton, Jesse. "Opinion: I Invented the Jihadist Journal: I deradicalized after 3½ years in prison. Now I'm reclaiming the medium to combat violent extremism". *Wall Street Journal.* 3 June 2019.
[419] https://www.eastviewpress.com/false-flags-information-warfare/

The Satellite Empire

The starry firmament is peopled with oppressors and despots; the planetary spheres are customs stations or jails…
Henri-Charles Peuch, *Gnosis and Time*

In the context of cyber politics, cyberspace and cyber arms, alternatively called nuclear defense technology architecture and the global telecommunications grid, constitute the periphery of the US empire. Current events and cybertechnology are analyzed in this section to substantiate the sovereignty of an extant (and literal) 'Satellite Empire'.

[TOPIC – American nuclear telecommunications empire]

Defined by the "startling political change of 1951 is the emergence of Soviet Russia as a great European and Asiatic power", the "most obvious manifestation of this is the creation of the Satellite Empire, the communization of China, and various degrees of major war, civil war, or insurrection in Korea, Indochina, Greece and Iran. A more subtle result of this expansion of Soviet interests is the creation of a bipolar world – a bipolarity which dominates all international relationships…".[420]

NIC 2008: "By 2025, the international community will be composed of many actors in addition to nation-states and will lack an overarching approach to global governance. The 'system' will be multipolar with many clusters of both state and nonstate actors. Multipolar international systems—like the Concert of Europe—have existed in the past, but the one that is emerging is unprecedented because it is global and encompasses a mix of state and nonstate actors that are not grouped into rival camps of roughly equal weight. **The most salient characteristics of the 'new order' will be the shift from a unipolar world dominated by the United States to a relatively unstructured hierarchy of old powers and rising nations**, and the diffusion of power from state to nonstate actors."[421]

Ten years later, the Department of Defense in its 2018 National Defense Strategy names the great-power competition with China and Russia, not terrorism, as the number one challenge to US security.[422]

This assertion can expanded upon by empire expert Michael Doyle: "Next to the domestic political society of the periphery as a classic determinant of the mode of empire is the structure of the of the international system. Multipolar systems tend to formalize or require formal institutions of imperial rule; bipolar systems tend to informalize or permit informal arrangements. A bipolar system tends to internationalize domestic politics in a transnational extension of ideological conflict and factionalism. Bipolar informality is rooted in the clear symmetry achieved when each pole of a bipolar system becomes aligned with a particular faction within the peripheral regime. Since the periphery is ruled by either on domestic faction or the other, associated with one pole or the other, clear international alignments are expressed by domestic political arrangements. Thus stable collaboration is doubly reinforced – domestically and internationally – in a bipolar system, without the formal imposition of metropolitan rule."[423]

---

[420] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 417.
[421] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 1.
[422] https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[423] Doyle, Michael W. *Empires.* Ithaca, NY: Cornell University Press. 1986, p. 136.

On cyber politics: "Regardless of the truth to the outstanding questions of American decline, one cannot contest that relative decline is in effect, due to the rise of multipolarity in the global system. Several events have occurred in the early twenty-first century that have, if not compromised, then certainly tarnished elements of America's status as the sole hyper power… the tarnishing of moral authority after 9/11; the resulting military campaigns following the attacks… Second, the economic collapse of 2008 seemed to have fractured the superiority of the liberal economic order based on capitalism."[424] [MOVE?]

The statement of global multipolarity and the attribution of US decline to it indicates that there was at an earlier stage a unified global system of US dominance or a bipolar global system of dominance. In the context of cyber politics this is the of course cyberspace, alternatively called at varying points in its lifetime, the "Satellite Empire", nuclear technology, the global telecommunications grid, etc. This system constitutes the periphery of the US empire.

If there were at any point a true bipolarity in this global empire, it would have existed between the US and Russia during the Cold War, with the US domination of telecommunications and the Internet signaling the consolidation of this power, as argued by Herman Kahn in 1959.[425] This is attested to in many instances. Most recently, in the US Defense Department's declaration that space is the new priority arena to be dominated, and in its attempt to create a separate Space Force, admittedly, in order to streamline the sale of electronic weaponry rather than increase operational efficiency. Secondly, the decades old declaration of a Cold War and space race between the US and the Soviet Union. Thirdly, the current Russian government's impression that the Internet is little more than "a CIA project". [426] Fourthly, the US's wholesale rejection of other nation's attempts to construct an Internet system independent of the US's system. Fifthly, NATO's insistence that it reserves the right to employ means of cyberwarfare "however and whenever we choose".[427] [REWRITE - confusing]

+ADD Current events proof of an extant 'Satellite Empire': +ADD on Nuclear combat through cyberarms and cyberspace. Nuclear combat is real phenomenon, aka "cyberwarfare"
https://www.dailymail.co.uk/news/article-3495301/China-Russia-planning-military-satellites-missiles-spacecraft-lasers-Air-Force-general-warns.html ; https://www.ibtimes.com/mysterious-russian-spacecraft-stalking-us-spy-satellite-space-force-expresses-concern-2919595 ; https://www.space.com/hackers-could-turn-satellites-into-weapons.html ; https://www.reuters.com/article/us-india-satellite-idUSKCN1R80IA ; https://principia-scientific.org/breaking-us-military-suddenly-blocks-uk-from-all-spy-satellite-access/ ; https://www.nydailynews.com/news/world/ny-iran-nuclear-scientist-assassinated-20201130-xytqopog4bhcbi3nzylnkofmmy-story.html
"Two Presidential Valets Who Carry Nuclear Launch Codes Test Positive for Coronavirus"
https://www.democracynow.org/2020/10/7/headlines/two_presidential_valets_who_carry_nuclear_launch_codes_test_positive_for_coronavirus ;

[424] Steed, p. 33-34.
[425] Kahn, P. 417
[426] Steed, p. 24.
[427] O'Neill, Patrick Howell. "NATO will establish new cyber command centers". *Cyber Scoop*. 9 November 2017.

"France Runs Satellite War Game in European First" AFP 3/12/2021: "France on Friday prepared to simulate an attack by a hostile power on one of its satellites in a war game scenario the government said is less outlandishly futuristic than it may seem. President Emmanuel Macron was to watch onsite as his military chiefs started to play out a four-day sequence in which an unnamed space-capable power attacks a nation allied to France, and tries to take out a French communications satellite. Germany, Italy, and the US are participating in the AsterX space war game at France's national space agency CNES in Toulouse, the first such exercise in France or in Europe. It is an opportunity to simulate modifying the flight path of satellites, sending backup satellites to fix a breakdown, monitoring the transmission of sensitive data, and scrambling transmissions by hostile satellites temporarily or even shutting them down completely."[428]

+ADD "A multipolar system, by contrast, creates incentives for formal rule… one straightforward reason can be found in the wider choice a multipolar system offers the peripheral regime – a choice among metropoles and thus a wider opportunity to bargain for some measure of independence. **A metropole, then, if it is to exercise control to further strategic or transnational aims, must establish full and formal control over the periphery, over its day-to-day administration as well as over the general direction of its political evolution**."[429]

The RAND Corporation writes on cyberspace as political sphere: "This report begins with the premise that cyberspace as a domain is not fundamentally different than other domains when it comes to international relations. By this, we mean that states will seek to use cyber operations as one tool of statecraft, just as they seek to use tools to further their interests such as military force, economic power, or social and humanitarian influence. The same principle applies to the use of cyber operations as a way to exert influence or pressure on others to shape behavior, deter adverse actions, and compel an actor to act (either another state, a multinational organization, or even a single individual)."[430]

Lindsay Gorman and Laura Rosenberger, formerly of the State Department and National Security Council, write:

> To the extent that the United States and its democratic peers have recognized the contest unfolding within and over the information environment, they have largely approached it in one of three ways: first, as a traditional question of public diplomacy and strategic communication…; second, as an ancillary to kinetic warfare or other military operations …; or third, as an economic or security challenge arising from technological competition… While these three approaches are necessary, each one focuses on a different aspect of the challenge in isolation—public diplomacy, the nexus to kinetic warfare, or technological competition—and none is sufficient. Instead, an effective strategy recognizes that the

---

[428] https://www.thedefensepost.com/2021/03/12/france-satellite-war-game/

[429] Doyle, Michael W. *Empires.* Ithaca, NY: Cornell University Press. 1986, p. 136.

[430] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 5.

> information arena has emerged as a domain of sustained and permanent competition that touches on all traditional aspects of national power.[431]

In this section, I suggest that confining the view of information warfare to preexisting concepts of nation-state power neglects the actual draw of power to information warfare, - that of a being hegemon over a global 'satellite empire', literal and figurative. Literally because it is controlled via satellites, and figuratively, because other nations become satellite nations of the US empire. The resistance to recognize this reality is likely a mis/disinformation operation itself. Depending on how far this (self-)deception reaches into strategic thinking, this lack of realism contributes to the decline of US hegemony.

The nature of the 'Satellite Empire' at war is best contained in the definition of information operations provided by the US Congressional Research Service and Department of Defense:

> While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations… which include computer network attack, computer network defense, and computer network exploitation; psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC).[432]

The role of cyberweaponry is most saliently concealed in hackers' wars because information operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not "considered an armed attack under international law" or "an act of war". [REWORD] The *IO Defense Primer* goes on to state:

> Information Operations as an Act of War? Some have questioned whether tampering with, interfering with, or otherwise influencing a sovereign nation's democratic processes in an IW campaign is an act of war that could trigger a military response, and not necessarily in cyberspace. A similar question is whether **a cyberattack that falls below the threshold of damage and destruction that a kinetic event would impart** could be considered an armed attack under international law. **U.S. policy suggests that these types of operations fall below the threshold of armed conflict**.[433]

+ADD Lindsay Gorman and Laura Rosenberger, formerly of the State Department and National Security Council write of information operations:

> **Authoritarian regimes**… **engage in censorship, surveillance, and propaganda, using the media and other tools to control and manipulate information on behalf of the state**. Put simply, in democratic philosophy, information rests with citizens; in the autocratic vision, it rests with those in power… **Authoritarian regimes like Russia and China see information and cyber warfare as** integrated domains of asymmetric conflict **distinct from kinetic operations**.[434]

---

[431] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 76.

[432] Theohary, Catherine A. *Defense Primer: Information Operations*. Congressional Research Service. 14 January 2020, p. 1.

[433] Theohary, Catherine A. *Defense Primer: Information Operations*. Congressional Research Service. 14 January 2020, p. 2.

[434] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 75-76.

The Balance of Terror

The radiation from fallout has curious and frightening effects. Most people know, or will know in a postattack world, that if you get a fatal dose of radiation the sequence of events is about like this: first you become nauseated, then sick; you seem to recover, then in two or three weeks you really get sick and die.

Now just imagine yourself in the post war situation. Everybody will have been subjected to extremes of anxiety, unfamiliar environment, strange foods, minimum toilet facilities, inadequate shelters, and the like. Under those conditions some high percentage of the population is going to become nauseated, and nausea is very catching. If one man vomits, everybody vomits. It would not be surprising if almost everybody vomits. Almost everyone is likely to think he has received too much radiation. Morale may be so affected that many survivors may refuse to participate in constructive activities, but would content themselves with sitting down and waiting to die – some may even become violent and destructive.

However, the situation would be quite different if radiation meters were distributed. Assume now that a man gets sick from a cause other than radiation. Not believing this, his morale begins to drop. You look at this meter and say, 'You have received only ten roentgens, why are you vomiting? Pull yourself together and get to work.'

This view is in accord with experience in peacetime disasters that have been complicated by epidemics.[435]

Herman Kahn, *On Thermonuclear War: Will the Survivors Envy the Dead?*

Pax Global

Changes in the nuclear détente of geopolitical order, the 'delicate balance of terror', owed to cyberarms race practices and capabilities which have gone ignored for decades have possibly invalidated strategic concepts of deterrence, proliferation, and disarmament. Realities may have even nullified the very concept of *strategic* nuclear weapons. The geopolitical implications of the exploitation of these ambiguities and the increased exercise of that weapons system is presented as a major geopolitical threat.

+ADD on Nuclear combat through cyberarms and cyberspace. Nuclear combat is real phenomenon, aka "cyberwarfare"

+ADD "In general the most remarkable achievement of the strategic intellectuals was that they were able to update Clausewitz and to persuade themselves and their governmental clients that **even nuclear war can be correctly viewed as the 'continuation of policy by other means.'** At any rate, they contended, prudence requires us to live with the fact that the Communist powers will be **disposed to play the Clausewitzian game with post-Clausewitzian weapons**."[436]
+ADD "But two parties, at least, are **engaged in such deadly games; and because of this the 'delicate balance of terror' cannot be long stabilized**. Instead, with each side falling back upon 'prudential' analysis each is always running scared and thereby scaring it potential

[435] P. 85-86

[436] Rosenberg, Milton J. (ed.). *Beyond Conflict and Containment: Critical Studies of Military and Foreign Policy.* Transaction Books. 1972, p. 9-10.

opponent. The 'action-reaction cycle,' as George Rathjens calls it, spirals on, spinning off more and more dysfunctional consequences with every revolution. Most obvious of all these injurious consequences is the gigantic cost of new strategic weapons and 'defensive' systems, a cost which inevitably depletes national wealth and fosters inattention to other basic domestic needs. Even more disturbing to scholars and investigative journalists who have peered closely at the modern **military** is their occasionally **visible restiveness over the restricted utility of nuclear weapons**. **So vast an investment** in a special and highly potent technology of destruction must, inevitably, breed the temptation **to get some international political return from it**."[437]

+ADD (current Vice Chairman of the Joint Chiefs of Staff) Gen. John E. Hyten, Commander, United States Strategic Command in 2018: **"There is no such thing as a tactical nuclear weapon** in my opinion. There is no such thing as a conventional nuclear weapon. **All nuclear weapons are strategic**, but you need different kinds to respond to different threats."[438]

This statement of Gen. Hyten is reinforced by understanding the strategic bombing of civilians as a create a strategy to create resistance fighters and irregular warfare situations. This entails facilitating the proliferation of weapons to be used tactically and precluding strategic aims to end combat, thereby creating 'forever' wars, or 'career-long wars', as the case may be. In *Bombing Civilians: A Twentieth-Century History*, Yuki Tanaka and Marilyn B. Young detail this strategy:

> Due to the widespread use of depleted-uranium weapons in both Gulf Wars and the **increasing possibility that tactical nuclear arms may be used, as well as the availability of super-large daisy-cutter bombs and mother bombs, the distinction between conventional and nuclear weapons is rapidly disappearing**… The majority of victims of strategic bombing are civilians – in particular, women and children. In plain language, 'strategic bombing' of civilians is an act of terrorism. Is there any moral **justification for killing tens of thousands of noncombatants under the rationale that it will force a swift surrender**? It is important to remember that no war has ever been brought to an end by bombing civilians. Indeed, **such a strategy typically strengthens resistance**.[439]

+ADD "Ultimately, the argument of Mearshimer should be a clear focal point in conditioning liberal views to a realistic proposition, when he argues that powerful states can only pursue hegemony in a unipolar moment. '**When the world is bipolar or multipolar,** on the other hand, **great powers have little choice but to act according to realist dictates**, because of the presence of rival powers.'… A sensible strategy for pursuing the liberal vision must accept and account for the very real challenge it now faces, and own up to its false assumption that the Internet was an inherently liberal technology**; achieving such an accommodation of political**

---

[437] Rosenberg, Milton J. (ed.). *Beyond Conflict and Containment: Critical Studies of Military and Foreign Policy.* Transaction Books. 1972, p. 11-12.

[438] U.S. Senate Committee on Armed Service. COMMITTEE ON ARMED SERVICES UNITED STATES SENATE HEARING TO RECEIVE TESTIMONY ON UNITED STATES STRATEGIC COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2019 AND THE FUTURE YEARS DEFENSE PROGRAM. Tuesday, March 20, 2018. https://www.armed-services.senate.gov/imo/media/doc/18-28_03-20-18.pdf p. 23

[439] Tanaka, Yuki, and Marilyn B. Young (eds.). *Bombing Civilians: A Twentieth-Century History.* The New Press. 2009, p. 6.

diversity 'will take a surge of strategic imagination' that has been lacking and is sorely needed…"[440]

"The difficulty of and lags in attribution, the relatively low barriers to entry, and the potential for deep psychological (if not physical) impacts make cyberspace an attractive method of exerting pressure on states when compared with other means that require greater technical and capital investments. One way that states may choose to use cyber operations, in between espionage and outright conflict, is by bringing pressure to bear that influences another state's decisionmaking."[441]

"this condition of nuclear survivability is thought to create a stable balance of terror, where no rational aggressor would attempt such folly. In short, conventional wisdom holds that strategic deterrence is robust – and highly recalcitrant to technological change. The **core assumptions about nuclear survivability and deterrence were forged decades ago, in an analog world that is long gone**… Cold War conventional wisdom is being turned on its head, with far-reaching and potentially alarming consequences for strategic balances, nuclear stability, deterrence, and escalation control. The current gap between dominant assumptions about nuclear weapons and the technological realities of deterrence has never been greater."[442]

+ADD https://www.rand.org/pubs/papers/P1472.html The Delicate Balance of Terror by Albert Wohlstetter ; https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror The Eroding Balance of Terror The Decline of Deterrence By Andrew F. Krepinevich Jr. January/February 2019
+ADD [move to Cyber Realism?] "Making a Better Russian Mousetrap: Many Third World nations initially sought and stockpiled Russian arms, and then, disenchanted with the political strings attached, broke their close links with Russia. This left a lot of orphaned Russian equipment, too expensive to replace but in need of spare parts and upgrades. **Western companies** came to the rescue, **reverse-engineering the Russian systems** and providing replacement components that were usually superior to the original."[443]

"During the THAAD dispute [of 2017], as part of its campaign to coerce South Korea into shifting its stance on the missile defense system, China utilized not only political and economic levers but also appeared to leverage cyber intrusions. U.S.–based cybersecurity firm FireEye alleged that cyberespionage groups linked to Chinese military and intelligence agencies launched multiple attacks on South Korean government and commercial entities in response to Seoul's decision to deploy THAAD. While Chinese hackers have long targeted South Korea, security experts tracked a discernable uptick in the number and intensity of cyber operations in the weeks following Seoul's confirmation of deployment of the missile defense system, suggesting, in the words of FireEye executive and former U.S. Indo-Pacific Command commander ADM Patrick

---

[440] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 81.
[441] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 2.
[442] Saltzman Institute of War and Peace Studies. "Disruptive Technologies, Strategic Vulnerability, and the Future of Deterrence". *Columbia University Arnold A. Saltzman Institute of War and Peace Studies webpage*. Accessed 20 August 2020.
[443] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 339.

Walsh, a 'clear correlation' between cyber operations and THAAD deployment. In response to FireEye's allegations, Beijing issued a blanket denial. The Chinese Ministry of National Defense declared that Beijing consistently opposed hacking, while maintaining that China was a longtime victim of cyberattacks. The aim of these operations may have been to signal Chinese displeasure with the decision and to exert pressure to coerce the South to reverse the decision, but it is unlikely these operations were significant factors in the South Korean government's decisionmaking."[444]

"FireEye's director of cyberespionage analysis, John Hultquist, told the publication that normal Chinese hacking of South Korean targets increased in number and intensity in recent weeks after the South Korean government said it would deploy the Terminal High Altitude Area Defense (THAAD). **The U.S. military is in the process of fielding** a **THAAD** battery with South Korea **in response to North Korea's missile and nuclear weapons developments**… The company believes **the other hacker group, called APT (Advanced Persistent Threat) 10 may be linked to other Chinese intelligence or military units**, according to the report. Hultquist said the **hackers gained access to target systems using web-based intrusions and by tempting personnel to click on malicious email attachments or compromised websites, a tactic known as phishing**. He also said that an error in one of the hacker group's operational security provided FireEye **analysts with new information about their origins**. In March South Korea's Ministry of Foreign Affairs said in a press briefing it was **the target of several distributed denial-of-service (DDOS) cyber attacks following the deployment of THAAD**, according to South Korea's state-funded Yonhap News Agency… The report also said Russia's Kaspersky Lab observed a wave of attacks on South Korean targets starting in February using malicious software that seems to have been developed by Chinese speakers."[445]

With Chinese efforts of cyber coercion failed militarily in the THAAD dispute, it is important to note that US military objectives were summarily achieved in the situation. It becomes necessary to consider the following questions posed by the RAND Corporation regarding cyber operations, as the nature of cyber coercion "cases indicate how the threat, threat actor, and the desired change in behavior is often unclear or ambiguous".[446]

Cyber coercion questions on the THAAD dispute (2017)

Was there an explicit or implied threat aimed at another actor to coerce a change in behavior?	Yes, cyberattacks from outside South Korea intended to control South Korean military policy on new US missile deployment. The cyberattack resulted in US military objectives being achieved in South Korea.
What were the broader political and economic circumstances surrounding the threatened action, and do these circumstances	Policy tensions between China and the US placed South Korean military policy at the center of a proxy dispute over US weapons

[444] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 21.
[445] https://www.defensedaily.com/report-fireeye-says-chinese-hackers-attacking-south-korea-thaad-deployment-3/uncategorized/
[446] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. vii-viii.

provide clues concerning potential coercive action?	deployment. The coercive action resulted in US military objectives being obtained and a degradation of political-economic relations between China and South Korea. A private Russian cybersecurity company also reported attacks on South Korean targets.
Were the cyber operations intended primarily to threaten or impose pain to motivate a change in behavior or for some such other purpose as espionage or retaliation?	The attack, if from China, was intended to prevent a change in South Korean military policy. The attack, in effect, motivated a change in policy in South Korea toward the deployment of a new US missile system.

Questions in italics from Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.*

For these reasons, the cyberattacks surrounding the THAAD deployment indicate that the US is likely behind the 2016 cyber coercion tactics. As one of two primary nations implicated in the proxy conflict, accepting the ambiguous origin of the attacks, and noting the change spurred by the attacks - the success (or failure) of the coercive tactics benefiting US policy objectives, - all single out the US as very likely being responsible for the 2016 cyber coercion attacks on South Korea.

+ADD "Stuxnet is a computer worm discovered in June 2010. It initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment. While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit. In May 2011, the PBS program *Need To Know* cited a statement by **Gary Samore, White House Coordinator for Arms Control and Weapons of Mass Destruction, in which he said, "we're glad they [the Iranians] are having trouble with their centrifuge machine and that we – the US and its allies – are doing everything we can to make sure that we complicate matters for them", offering "winking acknowledgement" of US involvement in Stuxnet.** According to the British *Daily Telegraph*, a showreel that was played at a retirement party for the **head of the Israel Defense Forces (IDF), Gabi Ashkenazi, included references to Stuxnet as one of his operational successes as the IDF chief of staff.**"[447]

In the case of THAAD, major political economic implications result from whether one analyzes the cyber coercion as active coercion (compellence) or passive coercion (deterrence). While intent and origin are often ambiguous in cyber coercion, and cyber-realist proof often access-prohibitive, the damages suffered and the success or failure of coercion is generally clear.

An unfortunate starting point of this paper has been the need to argue that the Arab Spring was decidedly damaging to the Arab countries involved, and the democratic reforms – if they really were ever attempted - were abject failures followed by unimaginable human tragedy.

[447] https://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html ; https://www.pbs.org/wnet/need-to-know/security/video-cracking-the-code-defending-against-the-superweapons-of-the-21st-century-cyberwar/9456/

Because the real-life consequences can be so compelling, politicking our understanding of cyber coercions, whether owed to loyalties or fears, can be self-defeating.

Cyber-ops strictly implies war crimes. The RAND Corporation on nature of cyber-ops as irregular warfare constituting war crimes as cyber-ops implicitly involve and target civilian populations: "Unlike more-traditional concepts of warfare, this is a testament to the expansiveness of cyberspace as a domain; military and civilian actors will engage in cyber competition and conflict, and this will likely spill into the civilian domain."[448]

[TOPIC – Balance of Terror in transition to The Hacker's Arsenal]

"This combination – of revolutionary and increasingly clandestine technologies – means that neither non-governmental analysts (who are generally unaware of the changes) nor government officials (whose work on strategic systems is highly classified and compartmentalized) have adequately explored the military and political implications of the new era of strategic vulnerability.

To be clear, not all nuclear arsenals have suddenly become vulnerable. But every arsenal today is less secure than it was before the computer revolution, and those countries that face stronger, richer, and more technologically sophisticated opponents will find it increasingly hard to keep their nuclear deterrents secure. The age of easy survivability is over. The age of vulnerability has begun.

The project aims to bridge the gap between old intellectual assumptions and new strategic realities. The project has four main analytic components: (1) highlight the principal technological changes endangering the foundations of nuclear deterrence; (2) assess how those changes impact force survivability across salient geopolitical fault lines; (3) investigate how these fluid and less transparent nuclear balances are complicating strategies of deterrence, reassurance, and escalation control; and (4) identify options for mitigating these and other growing policy challenges."[449]

[TOPIC - transition to The Hacker's Arsenal]

"The final factor behind the U.S. nuclear command-and-control system rests with the fact that nuclear weapons, ever since their development, have also always been considered unique, not like any other military weapon. Starting under President Truman, the point was made crystal clear that the White House was in charge of the atomic bomb and its uses, not the military.", **[President Truman said:] "You have got to understand that this isn't a military weapon. It is used to wipe out women and children and unarmed people, and not for military uses.** So we have got to treat this differently from rifles and cannon and ordinary things like that."[450]

GENERAL C. ROBERT KEHLER, U.S. AIR FORCE, RETIRED, FORMER COMMANDER, UNITED STATES STRATEGIC COMMAND: "**U.S. nuclear weapons prevent the coercive or actual use of these weapons against us and our allies, which is their primary purpose, constrain the scope and scale of conflict, compel adversaries to ponder the consequences of**

---

[448] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 17.

[449] Saltzman Institute of War and Peace Studies. "Disruptive Technologies, Strategic Vulnerability, and the Future of Deterrence". *Columbia University Arnold A. Saltzman Institute of War and Peace Studies webpage*. Accessed 20 August 2020.

[450] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 3.

their actions before they act, and obviate the need for additional allies to acquire their own. No other weapon can replace the deterrent value of nuclear wea pons. And the ability to command and control our nuclear forces under all conditions of crisis and conflict remains central to the credibility of the deterrent… **This is a system controlled by human beings**. Nothing happens automatically. That system is designed to do two very important things. First, it is designed to enable the authorized use of nuclear weapons while preventing the unauthorized use or the accidental use or the inadvertent use of them; and two, to do so in the face of a wide variety of scenarios, including a nuclear attack."[451]

"**the decision to employ nuclear weapons** is a political decision requiring an explicit order from the President. The process **includes 'assessment, review, and consolation via secure phone and video conferencing to enable the President to consult with his senior advisors**, including the Secretary of Defense and other military commanders.' Once a decision is reached, **the order is prepared and transmitted to the forces using 'procedures, equipment, and communications** that ensure the President's nuclear control orders are received and properly implemented."[452]

"Military members are bound by the Uniform Code of Military Justice (UCML) to follow orders provided they are legal and come from appropriate command authority. **They are equally bound to question (and ultimately refuse) illegal orders or those that do not come from appropriate authority.**"[453]

PETER D. FEAVER, PH.D., PROFESSOR OF POLITICAL SCIENCE AND PUBLIC POLICY, DUKE UNIVERSITY: "First, at the heart of nuclear command and control is what might be called **the always-never dilemma**. **For nuclear deterrence to work, we must have a high assurance** that the country will always be able to present a credible nuclear strike **capability** to our adversaries even in the most dire scenarios. However, **because even a single nuclear detonation** would be so consequential and **might trigger an escalatory spiral** that would lead to civilization-threatening outcomes, we **must also have a high assurance** that there will **never be an accidental or unauthorized [use] of nuclear weapons**… **Pre-delegating the authority to use nuclear weapons and spreading that capability to do so to lower echelons may thwart an enemy's first-strike** planning, for example, but it would **increase the risk that a weapon might be used in an unauthorized fashion** or by someone confused in the fog of battle. The history of nuclear command and control is a history of civilian and military leaders debating the proper balance between 'always' and 'never.'"[454]

"In the past, reviews of the command and control system uncovered hardware flaws that needed to be corrected - for instance, **gaps in communications** that could be fixed with more modern technology. But **more often reviews identified software and wetware problems** - for instance, discovering that rules were interpreted in a way that produced unintended effects or discovering that bureaucracies had resorted to understandable **'work-arounds' to get around cumbersome procedures, and, in the process, introduced uncertainties** that were not properly understood by higher authorities. This latter process has been called the 'paradox of control': the more the

---

[451] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 5.
[452] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 7.
[453] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 8.
[454] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 8.

higher levels of command seek to assert restrictive control of subordinate element even at the risk of making those subordinate elements incapable of doing their jobs, the greater is the incentive of those subordinate elements to establish 'workarounds' that the higher authorities may not be aware of or if they are, may not fully comprehend… **measures aimed at providing radical solutions at the hardware level risk being undone by workarounds at the software or wetware levels."**[455]

The Hacker's Arsenal

I don't think anybody anticipated the breach of the levees.
George W. Bush on Hurricane Katrina, 2005

The lesser-known capabilities of cyberarms, the risks inherent in these weapons systems technological and social vulnerabilities, and the crimes committed by authorized and ostensibly unauthorized users of cyberwarfare systems is exposed in this section.

+ADD "The **global Non-Lethal Weapons market is expected to grow** at a CAGR [compound annual growth rate] of around **9% during 2016-2021. The factors driving the demand are growing civilian & political unrest, and police militarization**, thus resulting in the procurement of advanced weapon systems. As per the MRFR [Market Research Future Report] analysis, the factor restraining the market growth is the concern raised by civilian over the usage of these weapons and regulatory issues would hinder the market growth in the forecast period."[456]
+ADD "Non-lethal weapons (also termed as less lethal weapons) are used by both the military and the law enforcement forces. Unlike lethal weapons, that can cause casualties, the non-lethal weapons are used to reduce the fatalities to a large extent**. These weapons are specifically designed to cause temporary harm or injury to a person. Non-lethal weapons are mainly used for crowd dispersion, controlling civil wars, and controlling illegal protests against governments in order to maintain law and order. Factors such as increasing political disputes and civil unrest and militarization of law enforcement agencies are positively impacting the non-lethal weapons market**… The global Non-Lethal Weapons market is expected to witness a **CAGR of approximately 8% during the period 2018 to 2023**. The market is segmented by type, disabling mechanism, end-user, and region. Based on type, the non-lethal weapons market is divided into **direct contact non-lethal weapons [and] directed energy non-lethal weapons**. During the forecast period, the **direct energy segment is likely to witness the highest CAGR as it is more efficient in riot control operations**. Based on disabling mechanism, the non-lethal weapons market is divided into **impact, irritant chemicals, and intense sound/light.** In Furthermore, based on end-user, the non-lethal weapons market is divided into law enforcement and military. **In 2017, the law enforcement segment accounted for the largest market share as these organizations mostly are ordered to restrain, subdue or incapacitate** the threat rather than neutralizing. "[457]

---

[455] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 11-12.
[456] https://marketersmedia.com/global-non-lethal-weapons-market-is-expected-to-grow-at-a-cagr-of-around-9-during-2016-2021/212829
[457] https://www.marketresearchfuture.com/reports/non-lethal-weapons-market-1353

+ADD “The "enemies" will have fictional names, but when hundreds of US military personnel around the globe log on to their computers later this summer for a highly classified war game, it will be clear what a major focus of the scenarios will be -- how the US should respond to aggressive action and unexpected moves by China and Russia. Several defense officials tell CNN that the war game is a top priority for the chairman of the Joint Chiefs of Staff, Mark Milley, who will lead the exercise. Defense Secretary Lloyd Austin will be briefed as it plays out. The war game is designed to equip the US military's top leaders to deal with a fictional global crisis erupting on multiple fronts and players will have to deal with constantly changing scenarios and compete for military assets like aircraft carriers and bombers. They will take place at a crucial time for the Pentagon just months into Joe Biden's presidency. The military budget is being set and major decisions on troop levels and priorities are being made so it's hoped the war game will help prepare the military to face the challenges of the next few years… The scenarios covered in the game this summer will reflect real life possibilities. Those could include major cyber attacks, a Russian advance in the Baltics, further militarization of the Arctic by Moscow or China flexing its muscles in the South China Sea or even invading Taiwan… Top commanders are increasingly blunt about both countries, especially on nuclear modernization. Russia is upgrading bombers, intercontinental ballistic missiles, submarine launched ballistic missiles and warning systems, ‘in short, its entire strategic force structure,’ wrote Admiral Charles Richard, head of the US Strategic Command in a recent article in the Proceedings of the US Naval Institute journal. Moscow is also building hypersonic weapons that travel more than five times the speed of sound, and nuclear-powered torpedoes, capable of reaching US shores quickly. Richard warned that China is about to become a nation with a full nuclear triad, with an inventory of nuclear capable missiles, submarines and soon a long-range bomber. "While the PRC has maintained a "No First Use" policy since the 1960s—contending it will never use a nuclear weapon first—its buildup of advanced capabilities should give us pause. This policy could change in the blink of an eye. Beijing is pursuing capabilities and operating in a manner inconsistent with a minimum deterrent strategy, giving it a full range of options, including limited use and a first-strike capability," he wrote. The US military is doing substantive planning for the challenge from Russia and China, with billions of dollars of spending planned on modernization in both the nuclear and non-nuclear arena if its wins Congressional approval.”[458]

+ADD “In 1997, 31 members of the Mexican army’s elite airborne special forces group defected and formed the core enforcement arm for the Gulf Cartel (Cártel del Golfo). This group later split from the Gulf Cartel to form The Z’s (Los Zetas) and demonstrated sophisticated tactics by integrating intelligence operations with deliberate mission planning to conduct attacks using state-of-the-art weaponry and communication systems to rival the capabilities of Mexican security forces.”[459]

In fact, the cartel’s name, *Zetas* (the name of the letter z in Spanish), is a reference to “radio Z code”, a radio telegraphy code developed by NATO for intra-military and military-

[458] https://www.cnn.com/2021/03/27/politics/us-war-game-russia-china/index.html

[459] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 6.

police communication.[460] Significant to defected counterintelligence, Z radio codes relate mostly to frequency-based communication interception and interference directives.[461]
+ADD "There was another factor in that optimism as well, one that sounds very familiar today amid tech buzzwords thrown around in the promise of transformative initiatives. In a 2017 paper in **Genocide Studies and Prevention, Raymond and co-author Kristin Bergtora Sandvik call this 'technology optimism,' an often implicit belief that the use of information and communication technologies has 'an inherently Ambient Protective Effect (APE); i.e. casually transforming the threat matrix of a particular atrocity producing environment in a way that improves the human security status of targeted populations.'** As with surveillance cameras in public areas, there is an assumption among some sectors of the population that they will make the situation better by their mere existence, that the act of surveilling itself will prevent bad things from happening**. In fact, the reverse can happen. In a 2016 dissertation paper studying Amnesty International's Eyes on Darfur project, Grant Gordon found that 'Amnesty's advocacy effort was associated with between a 15 and 20 percentage point increase in violence in monitored areas.**'"[462]

[TOPIC – nullification of nuclear policy due to hacking, nullification of concept of *strategic* nuclear weapon]
Michael J. Mazarr writes in *Understanding Deterrence*:

> If deterrent threats come to be perceived as a general policy of hostility, they may lose their ability to be applied to deter… By its nature, deterrence is a demand that another state refrain from doing something. The more ambiguous the demand is, the more chance there is for failure in the deterrent policy. Not only must the deterring state be precise in its commitments, but its target must understand them clearly. A key challenge of deterrent threats is to ensure that a potential aggressor perceives the message "through the din and noise" of world politics. This demands both public and private efforts to communicate an unambiguous message. It also points to the danger of statements or actions that seemingly throw into doubt the sincerity of the commitment.[463]

+ADD "As the military field-tests **multiple types of directed energy weapons**, it's running into some **surprising real-world problems – like the dust from Cheetos**. When you put cutting-edge tech into the less-than-pristine hands of actual teenaged and twenty-something troops, you get unique feedback you'd never get in the lab, said Donald Schiffler, chief directed energy scientist at the Air Force Research Laboratory. For a **drone-busting high-powered microwave called THOR**, "we thought, well, we should have **everything touchscreen-operated**… like on your iPhone," Schiffler told a Booz Allen Hamilton webcast this morning. "That sounds great — except you find out **that that doesn't work for warfighters who are pulling a long shift, because they do things like eat Cheetos while they're sitting there working, and then the touchscreen does not work**."[464]

---

[460] https://www.aljazeera.com/features/2010/11/3/us-trained-cartel-terrorises-mexico
[461] https://www.pwcares.org/doc/Z-Signals.pdf
[462] https://foreignpolicy.com/2020/01/21/sudan-clooney-satellite-surveillance-can-trace-atrocities-but-not-stop-them/
[463] https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf P. 9
[464] https://breakingdefense.com/2020/07/a-golden-age-for-collaboration-on-lasers-microwaves-but-watch-the-cheetos/

[RE: War College PAL terrorist organization] "Some [**nuclear command and control** improvements], like **permissive action links, PALs**, which are **coded locks that block detonation of a weapon without inserting the PIN code**, and were pressed by far-seeing congressional advocates, these improvements may have helped forestall disaster. This brings me to my second major point. We must be willing to invest the requisite funds to keep our technology up to date. But in the nuclear command and control business, hardware is trumped by software, and software is trumped by wetware. Hardware refers to the technologies like the PALs I just mentioned. Software refers to the rules and procedures that govern how the hardware is used; for instance, the code management system that determines **who has the PAL codes and who is authorized to release them. Wetware refers to the human element**, the reliability of people involved in enforcing the rules, and the civil-military relations that form the political context in which the software and hardware operate."[465]

"weapon system that strikes the atmosphere with a focused electromagnetic beam may cause global warming, the [Indian] government said today and acknowledged that climate change is likely to reduce the yield of major crops like wheat and maize in India...HAARP is an advanced model of a super powerful ionospheric heater which may cause the globe to warm and have global warming effect."[466]

+ADD "**One of the best ways to secure American military technology is to steal it**. There is a proven technique for this. First, you monitor all U.S. military and scientific publications. All but a few top-secret U.S. military R&D projects are discussed in some detail in the open press. For this you will get a good idea of what's coming and when. At this point, you also alert your spies to look for American R&D people who can be bribed, blackmailed, or otherwise persuaded to deliver secret documents and components to your scientists. In many cases, you will string these people along until the project is near completion…. Since U.S. military R&D projects take about fifteen years to complete, you can afford to watch and wait. Besides, developing illegal contacts within these projects takes time… You save 10 to 50 percent of your development costs because of your espionage efforts."[467] [Re: social engineering hacking]

+ADD "The latest thing [as of 1990] in **tactical radio are 'frequency hoppers'** that evade jamming and are more secure from overhearing. They do this by switching frequencies so quickly that no jamming equipment can keep up with it. Enemy monitors cannot follow conversations because they cannot switch frequencies quickly either. The two frequency-hopping radios synchronize their hopping so they can understand each other. As these radios came into use, an unpleasant side effect was discovered: The radios sometimes touch upon a frequency combination that jams other friendly radios."[468]

+ADD "The numerous electronic components (commonly packed in **black boxes) filling modern aircraft usually have to do with electronic warfare. These devices either detect enemy radar and transmissions, or jam and deceive them.** …Testing is complicated by the presence of a dozen of mor sensors in the aircraft that are capable of dealing with thousands of different frequencies and many more combinations. …In addition to possible electronic failures,

---

[465] 115th Congress. "Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons". United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019, p. 9.

[466] "US-developed weapon system may cause global warming: govt". *The Times of India*. 18 July 2016.

[467] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 240.

[468] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 244.

any defects in the wiring can have catastrophic effects on system performance. Ultimately, any **failures in the electronic-warfare systems** would only be known when enemy systems were encountered under actual combat conditions."[469]

+ADD "**Mexican drug cartels are using weaponized consumer drones** in their latest gang war, according to reports in El Universal and other local news media. A citizens' militia group in Tepalcatepec, Michoacán, formed to protect farmers from the cartel, found two drones in a car used by gunmen belonging to the Jalisco New Generation Cartel (CJNG), a group estimated to control a third of the drugs consumed in the U.S. The drones had plastic containers taped to them filled with C4 explosive and ball bearing shrapnel. The militias say that they have heard explosions, and believe that the drones are the latest weapons an ongoing gang war**. The CJNG has been involved with such devices since late 2017 in various regions of Mexico**,' says analyst Dr. Robert J. Bunker, Director of Research and Analysis at C/O Futures, LLC. **'This cartel is well on its way to institutionalizing the use of weaponized drones.** None of the other cartels appear to presently even be experimenting with the weaponization of these devices.'**… In 2018 an armed drone attacked the residence of a senior official in Baja, California.** The official was not at home, and the attack seems to have been intended as a warning. **Three CNJG drones with explosive were recovered this year, part of an arsenal for use against the rival Rosa de Lima cartel… The Mexican drones appeared to be wired for remote detonation** in kamikaze attacks. They are similar to the jury-rigged quadcopters used in an unsuccessful assassination attempt against President Maduro of Venezuela in 2018. **They are less sophisticated than the bomber drones used by ISIS and other groups in the Middle East since 2016 which drop modified 40mm grenades with great precision, used with deadly effect against Iraqi government forces. Such drones are now widespread in the Middle East. Their absence in Mexico is may be because the cartels do not have access to munitions which can easily be modified for drone use. The U.S. military makes extensive use of portable kamikaze drones**, which it terms 'loitering munitions,' in particular the SwitchBlade made by Californian company AeroVironment AVAV -1.6%. This has night vision, the ability to lock on to a target and a silent attack mode, as well as an advanced precision warhead. 'Improvised drone bomb designs for terrorist and criminal organizations are still relatively unsophisticated from a nation-state and future potentials perspective,' says Bunker. **'This is due to both the lack of technical sophistication of their bomb makers and the lack of computer, data/signals, and command and control expertise of their pilots.'**"[470]

+ADD "The world's major armed forces currently possess hundreds of thousands of laser devices. Most are used for range finding, target designation, and fire control. **Humans can be temporarily or permanently blinded by most lasers, and battlefield accidents are expected.** They have already occurred in peacetime. The Russians are suspected of staging such accidents to test the possibility of using lasers in wartime to blind enemy pilots. They have already temporarily blinded several American pilots with their high-powered shipboard lasers. Iraq is believed to have tested such a device in combat against Iran, leaving thousands with severe eye

---

[469] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 248.

[470] https://www.forbes.com/sites/davidhambling/2020/08/24/mexican-drug-cartel-carries-out-drone-strikes-in-gang-war/?sh=496b29ae9432

injuries. Other nations are building weapons that will blind enemy troops and/or instruments with lasers. **The next war may be quite a light show**, though few who see it may be able to do so more than once."[471] … "With all the talk of **electronics and sensors**, we tend to forget that all these goodies **are only as good as the human senses** of sight, hearing, and touch **are in coping with them**. … Tests have been made placing electric devices on pilot's forearms and chest, which would enable the pilot to feel changes in status of systems. This could give new meaning to the **terms *heart-burn* (fuel-pump failure), *foot's asleep* (landing gear inoperable), and *pain in the ass* (afterburner malfunction).** However, this **sensory approach** could make an unexpected itch in the wrong place a **potentially fatal event**."[472]
+ADD quote "'If you load a mud foot down with a lot of gadgets that he has to watch, somebody a lot more simply equipped – say with a stone ax – will sneak up and bash his head in while he is trying to read a vernier.'" [473] Robert A. Heinlen, American science fiction novelist
+ADD quote "As General John Vessey, Chairman of the Joint Chiefs of Staff in the early eighties, once remarked regarding high-tech communications equipment, 'In the next war we will still have to use runners' to deliver messages when the radios and telephones fail."[474]

+ADD *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All* Arthur Holland Michel
+ADD "experience as the methods of disintegration, torture and destruction from the worst systems that humanity has ever produced like the East German Stasi and the Nazi's Gestapo in WW2 Germany are applied to the victim"[475]
The RAND Corporation defines cyber-ops in terms of threatening, inflicting pain and causing physical damage: "*Coercion in theory* requires one actor to make explicit demands of another which are tied to clear consequences for noncompliance. Coercion in theory can include inflicting pain or punishment to demonstrate commitment and signal that worse is to come if the threatened state or actor does not accede to the coercer's demands. *In practice*, however, a coercing state may only make vague threats or even seek to covertly act to inflict some pain with the intent of motivating the coerced state to change its behavior. The specific desired behavior may not be clearly stated either. Observed practice is not always entirely ambiguous: It could involve a clear demand, but an ill-defined threat. For this report, we define *cyber coercion* as the threat (implied or explicit) or limited use of cyber operations to motivate a change in behavior by another actor that may involve cyber operations on their own or in conjunction with other coercive actions… Our assessment of these cases indicates how the threat, threat actor, and the desired change in behavior is often unclear or ambiguous, though this ambiguity does not appear to prevent countries from pursuing these coercive campaigns… What motivates these attacks can vary from the misguided—'can I hack into this network?'—to the truly malicious—'can we cause physical destruction through cyberspace?'… several scholars have already addressed the seemingly low rate of success for cyber coercion.[12] Successful cyber coercion results from either

[471] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 239.
[472] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 261-62.
[473] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 261.
[474] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 262.
[475] https://jointinvestigation.files.wordpress.com/2018/08/jit-guide_jit-20180830-005-kh-v1_first-aid1.pdf

the credible threat or some elements of a successful cyber operation with a change in behavior. Even in cases where the operation itself achieves its proximate aims (e.g., limited damage to critical infrastructure), it appears that behavioral changes are few, whether because the actor carrying out the operation overestimated the likely impact or because it underestimated the capacity of the adversary to withstand pain. Despite this poor track record, however, states persist in developing cyber capabilities and appear to believe, rightly or wrongly, that there is promise in cyber coercion. Therefore, we can expect states to continue to pursue coercive actions through cyberspace, and even increasingly turn to cyber operations to coerce."[476]
The RAND Corporation wants people to know that, actually, cyber coercion in international politics isn't totally like kidnapping: "Coercion in international relations is not the same as kidnapping, though some of the academic literature uses formulations that more closely resemble kidnapping than the dynamics of interstate relations. This difference is important for two reasons: 1) context is critical to understanding whether coercion is occurring; and 2) the potential for miscommunication between coercer and coerced can be significant, even if there is a longstanding relationship between states, as we shall see in some of the case studies in this report. In a kidnapping, there is usually an explicit demand, whether it is money or some other outcome, such as the release of political prisoners."[477]
International definitions of cyber-ops include mass psy-ops and electronic warfare, referred to as "comprehensive coercion": "Russia's approach to countering this state of affairs is to conceive of cyber operations as a subelement of broader information warfare, combining elements of psychological operations, electronic warfare, and network attack. Russian military thinking speaks of information warfare as encompassing actions that can impact information systems (i.e., information technology [IT] networks), but with the ultimate aim of undermining those systems or 'producing mass psychological effects with the aim of destabilizing society and the state or coercing the state to make decisions in the interests of the opposing side." The RAND Corporation and "Russian doctrine and security policies therefore recognize the potential to coerce with cyber operations." [478] ; **China:** "In the words of Ye Zheng, an expert in information warfare at AMS [former director of the Informationized Operations Research Office at the Academy of Military Science Operational Theory and Regulations Department in Beijing, China], "the strategic game in the cyberspace is not limited by time and space, does not distinguish between peace and war, and has no frontline and homefront."[479]

+ADD "At the time of writing, **all members of the Joint Investigation Team** [Dr. Katherine Horton, Switzerland Founder and Leader of the Joint Investigation Team **High Energy Physicist and Expert on Complex Human Systems**; Karen Melton Stewart, USA Investigator and Intelligence Analyst for the Joint Investigation Team ret. **NSA Intelligence Analyst, Expert on Weapons Development & Proliferation**; Dr. Millicent Black, USA Investigator and Welfare Officer for the Joint Investigation Team **Expert on Violence against Women and Military**

[476] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. vii-viii, x, 1, 8.
[477] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 6.
[478] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 10.
[479] Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019, p. 16.

Neuro/Biotechnology; Ramola Dharmaraj, USA Investigator and Press Officer for the Joint Investigation Team Investigative **Journalist and Expert on Secret Service Criminality**; Melanie Vritschan, Belgium Investigator and Events Manager for the Joint Investigation Team Founder of ICATOR, **Expert on Civil Rights & Military Neuro/Biotechnology[480]] are themselves continuously physically assaulted with modern military weaponry**, receive regular death threats and suffer repeated assassination attempts. Each of the investigators has been denied assistance and remedy by their respective police services, judicial offices and legislature to this day."[481]

+ADD "By 2020 or thereafter - such a complex techno-system is unlikely to respect schedules - this triple canopy should be able to atomise a single "terrorist" with a missile strike after tracking his eyeball, facial image, or heat signature for hundreds of miles through field and favela, or blind an entire army by knocking out all ground communications, avionics and naval navigation."[482] Compare this to claims made in 2020 by Hollywood movie star and spouse of alleged international human rights lawyer representing both Arab Spring journalists and ISIS sex slave victims. "Satellite Surveillance Can Trace Atrocities but Not Stop Them: George Clooney's pioneering data project documented horrors in Sudan, but that wasn't enough" "SSP went a step further than previous efforts to document mass killings, seeking to identify the indicators needed to predict them so that information could be shared before they happened. As Raymond told me by phone, "We went into SSP believing we could standardize the observable patterns that would happen in certain kinds of atrocities and create a new forensics." This is possible because, as Raymond explained, "there's a logistical ground pattern required to kill a lot of people." It was a chilling reminder of just how systematic such atrocities are. And in today's world, the prepositioning of troops and equipment necessary for a massacre is not only predictable; it's also "entirely visible from space.'…

+ADD Syrian representative in leaked discussion with John Kerry ~"atrocities in Syria well documented by drones, satellites, cameras, etc, no more proof needed"[483]

In a 2016 dissertation paper studying Amnesty International's Eyes on Darfur project, Grant Gordon found that "Amnesty's advocacy effort was associated with between a 15 and 20 percentage point increase in violence in monitored areas." [484]

On pandemic response increased surveillance and contact tracing: "On Monday, the F.B.I. released preliminary statistics showing a major increase in murder last year [2020]… cities of all sizes reported increases of greater than 20 percent… Although it's not clear what has caused the spike in murder, some possibilities are the various stresses of the pandemic".[485]

---

[480] https://jointinvestigation.files.wordpress.com/2017/06/jit-2017-06-26_001-kh-v1_who-is-who1.pdf
[481] https://jointinvestigation.files.wordpress.com/2018/08/jit-guide_jit-20180830-005-kh-v1_first-aid1.pdf
[482] https://www.aljazeera.com/indepth/opinion/2012/11/201211912435170883.html
[483] https://www.youtube.com/watch?v=e4phB-_pXDM&feature=youtu.be ~9:00
[484] https://foreignpolicy.com/2020/01/21/sudan-clooney-satellite-surveillance-can-trace-atrocities-but-not-stop-them/
[485] Asher, Jeff. "US Murder Rate Remains Elevated as New Reporting System Begins". *The New York Times*. 16 March 2021.

More on the self-referential impotence of the surveillance industry in the section titled Research and Arrested Development.

+ADD https://www.reuters.com/article/us-usa-defense-cybersecurity/pentagon-to-treat-cyberspace-as-operational-domain-idUSTRE76D5FA20110714 (9 years ago

[TOPIC – Extrajudicial stalking and murder by electronic weaponry operated on nanosecond basis by the US government]

+ADD find magazine article (new yorker, time?) 2017-early 2018 ISIS sex slave returned home, within days suffers from sudden loss of ability to speak, stand, collapses, loses consciousness. Electronic weaponry stalking and torture of freed sex slaves.

+ADD "Plan for Hunting Terrorists signals U.S. to intends to keep adding names to kill lists" by Greg Miller, 8/23/2012 [486]

It is argued that **"**Social media cannot conduct the attacks and sabotage, establish the administrations and organizations, or advance the social and economic development that is crucial to the latter phases of an insurgency. As Barrie Axford says in 'Talk About a Social Revolution: Social Media and the MENA Uprisings,' '[t]he digital public sphere, if such it is, may increase the number and range of participants but, in terms of outcomes, it could still be argued that bombs, guns, and Apache attack helicopters tip insurrections and win revolutions.'"[487] This argument is not factually accurate and is not an actionable understanding in the case of the most likely course of coup in highly connected 'democracies'. The so-called Satellite Empire is highly prone to be the battlefield and weapon of choice within modernized nations.

This is not only because the focus of this work is cyberrealism. Social scientists interested in urban planning have long commented on the inability for street protests to evolve into revolution in most American regions due to the cities' lack of central gathering places, such as town squares or plazas. This leaves cyber coordination for revolutionary protests without ubiquitous places of physical manifestation in the US. This would seem to indicate alternate courses would be taken to effect 'tipping insurrections'. How this occurs and why it occurs within the 'Satellite Empire' is discussed in this section, with the focus being on the Arab Spring as an American product.

I take 'Satellite Empire' from Herman Kahn's *On Thermonuclear War* section titled Hypothetical Past: World War III [check subtitle]. Because he does not elaborate on the term but to mention it in the context of the emergence of the Cold War in the late 1940s, I take the term to indicate his recognition of a non-traditional empire that emerged out of nuclear wartime advancement mid-century. I use the term to encompass a warfaring organizational structure existing just beyond our grasp that is made possible through nuclear technologies. The term also denotes the client states of an empire. In terms of warfare, this includes fields as abstracted as psychological/information warfare to the most kinetic fields like satellite engineering.

+ADD sections chapters 9 & 10 Click Here To Kill Everybody

"Right now, they [governments] prioritize maintaining the ability to use the Internet for offensive purposes… But if we are ever going to make any progress on security, the need to switch their thinking and start to prioritize defense. Governments should support what Jason

[486] https://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html

[487] Lindsey, Richard A.

Healey calls a 'defense dominant' strategy. Yes, offense is essential to defense. Intelligence and law enforcement agencies in liberal democracies have legitimate needs to monitor hostile governments, surveil terrorist organizations, and investigate criminals. They use the insecurities in the Internet to do all of those things, and they make legitimate claims about the security benefits that result. They don't characterize themselves as being anti-security. In fact, their rhetoric is very pro-security. But their actions undermine the security of the Internet… We all use the same Internet hardware and software. There is simply no way to secure US networks while at the same time leaving foreign networks open to eavesdropping and attack. There's no way to secure our phones and computers from criminals and terrorists without also securing phones and computers of those criminals and terrorists. On the generalized worldwide network that is the Internet, anything we do to secure its hardware and software secures it everywhere in the world. And everything we do to keep it insecure similarly affects the entire world."[488]

Despite the military-intelligence industries rush into the fray of purchasing, selling and using electronic weaponry, the National Intelligence Council itself predicts the failure of the triple canopy of electronic weaponry to stave of domestic attacks in *Global Trends 2025: A Transformed World. (find cite)*

"Examples as disparate as Sweden and Rwanda indicate that countries with relatively large numbers of politically active women place greater importance on societal issues such as healthcare, the environment, and economic development. If this trend [women's political involvement] continues over the next 15-20 years, as is likely, an increasing number of countries could favor social programs over military ones."[489] The continued exclusion of women from military, security and intelligence decision-making, along with their increased inclusion in more traditional women's fields like economy and human relations, absolutely ensures that military will become more remote from decisionmakers' considerations, less funded, and placed on a back burner.

This however indicates that whoever is in power will favor their own field of expertise and experience. It also serves as a prime example to illustrate how the US military-intelligence-security industries contribute to their own defeat while having foreknowledge of the problem and end-to-end control of the remedy. As the previous section Out of the Blue introduced, these industries constantly serve as their own worst enemy, and usually as their only enemy. As Durant argued, the internal makeup of the society changes and the old empire is essentially consumed from within, especially when it cannot cross the Augustan threshold, which particularly devastates the military and intelligence classes of empire.

"The Pensioner Boom: Challenges of Aging Populations": "The cost of trying to maintain pensions and health coverage will squeeze out expenditures on other priorities, such as defense."[490]

---

[488] Click here p. 160-161.

[489] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 16.

[490] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 21.

+ADD [MOVE to other section?] In time of armed conflict, the traditional power dynamics are more susceptible to reconfiguration. Law and order has broken down, the balance of power is in the process of being reshaped and there may be room for movement within the pre-existing social hierarchies. As rape and other forms of sexual violence are about maintaining and restoring certain power balances, sexual violence will likely be committed in time of potential imbalance. Indeed, it has been noted that, ' [a] comparison of low-rape and rape-prone societies reveals that the occurrence of rape is particularly high where male power has become unstable '. But why then the high incidence of male sexual violence? It has been posited, persuasively, that sexual violence against men in war occurs for much the same reason as sexual violence against women striving for equality and independence in male-dominated societies, namely that in both situations, there is an attempt to suppress challenges to the social status of the dominant group."[491]

This is an aspect of the decline of military and intelligence dominance that those same industries recognize and predict to become more severe. What those groups do not acknowledge is that the emergence of the information age represents the replacement of one type of civilization with another type. These industries' bumbling physical violence into the age of information warfare, making obvious physical substitutions like employing electronic lasers in place of igniting gunpowder, along with practicing anti-informationism and anti-intellectualism, displays their complete inability to make the changes needed to cross their Augustan threshold into the age of information warfare as the force of the empire.

It's likely that the rise of fascism in the 20th century until now is the deadly reaction of old civilization's strong arm of empire to the new longer arm of empire in the Information Age. The strong have become the weak in power, and in their last throes of power, they barely embrace the new identities of power just enough to malign that power (information), name the changed elements of their civilization as invasive, attack and disable that power, and so destroy the entire population and territory of that nation. As is discussed in the section 'The Bomb and the GDP', the US is a civilization of GDP calculations dependent on auto manufacturers-turned-warfare producers, soldiers that fight, and civilians that thrive working on the assembly line.

The US cannot conceive of itself or any of its social classes outside of this paradigm, and it definitely cannot predict that whatever nation or group that holds another paradigm will succeed the US as world power. And so it continues watching for new smart weaponry, launching satellites, manipulating radio waves, and measuring the fighting capabilities of other nations by GDP-to-weaponry arsenals calculations. The anxious attempts to emphasize cyber simulators and video gameplay in wargaming discussed above in the section Out of the Blue is an example of their attempts to define 'information' narrowly as 'information technology' - something any analytic group can buy, sell, and deploy, no matter how unenlightened or uneducated they may be.

As Herman Kahn wrote in *Ten Common Pitfalls*,

> Probably no applied professional group is so intensely and continuously concerned with methodological and philosophical questions as Operations Analysts and Systems Analysts. Partly this occurs because it is important to be clear on methodological points and partly it is

[491] Sexual Violence against males in conflict P. 267-268

> undoubtedly just the normal introspection to be expected in any new field. However it is hard to avoid the feeling that much of this self-questioning is caused by a sort of mass inferiority complex or at least a general sense of insecurity. Assuming that this insecurity exists we would conjecture that it is due to at least two causes:
> 1. The somewhat nebulous and unspecialized nature of most of the work makes it hard for practitioners to obtain automatic deference and acknowledgement…
> 2. A correct (if sometimes subconscious) recognition that an extraordinarily high percent of the work done in this field is somehow not quite passable.[492]

They do not even realize that that end is now nearly worthless and irrelevant even if it is achieved. When knowledge and information is the end itself, *how* informedness is achieved is information itself. If it is done badly, the goal-info is unusable, or the illegal means become information used against the government which gatherers it. If the intelligence forces play at zero sum tactics, - if their means are not informed but anti-informationist, - it creates a net-zero gain.

The US military-intelligence industry would balk at the mention of paradigms as dangerous for national security, and then attempt to figure out how to monopolize that new paradigm or neutralize the threat of the paradigm – maybe by thought-control, or a disinformation campaign? The concept that means *create* the desired end is nonsense to regimes that justify grotesque levels of brutality to achieve rather petty ends. In fact, they are too occupied eliminating competition in their new role as information providers that they cannot dedicate any resources or personnel to adapting to that new legitimate role themselves.

The following examples from the National Intelligence Council demonstrate the barbed wire fence the security-intel industries find themselves straddling, caught between their state function as brutalist deceivers and their new role as information providers. One can almost perceive their desperate attempts to perpetuate a violent circle of return business in which they invent poor information or illegally access information, then create panicky chaos when they transfer blame or leak breeches as government crimes or vulnerabilities in order to maintain the demand for brutal deceiver tactics, which are their only real talents and the sole State role that they alone monopolize. As the CIA recently lamented on Twitter, dead drops are themselves dead in the age of nanosurveillance, and exist now only as museum pieces.

Unfortunately for global security, this is viewed as a threat to a way of life within intel-security industries. As many reasonable (and unreasonable people) familiar with those industries have warned, the intelligence-security sectors of the world have become the most conspiratorial, threatening and dangerous industries on Earth. Then, policymakers turn to those same industries for review of the warnings issued against those industries, which creates the conditions for secret prisons, assassinations, and extrajudicial killings. Most intellectuals doubt this cycle is unconscious for either party due the public existence of above-top secret classification levels and official secret courts.

---

[492] Kahn, Herman and Irwin Mann. *Ten Common Pitfalls.* The RAND Corporation, Santa Monica, California. 17 July 1957, p. vii.

The National Intelligence Council predicted in 2009 that the world would make a "rapid" transition away from fossil fuels between 2020 to 2025 due to negative effects on the climate (that will remain unsolved despite the abandonment of fossil fuels). This is bound to cause major disruptions geopolitically. The report illustrates that this change would devastate oil producing nations, and could reduce economic growth for low-efficiency nations like China. It also claims that climate change "could lead to increasingly heated interstate recriminations and possibly to low-level armed conflicts."[493]

The Intelligence report overlooks that the disappearance of oil trade would completely undercut US currency which is based on the strength of the trading petrol-dollar. The report does, however, imagine a gigantic hurricane caused by climate change destroying the New York Stock Exchange, causing it and entire parts of East Coast cities to be relocated elsewhere.[494] This allegedly is unrelated to another Intelligence observation made in the report that, "In the West, the biggest change—not anticipated before the [2008 financial] crisis—is the increase in state power. Western governments now own large swaths of their financial sectors and must manage them, potentially politicizing markets."[495]

The report also glosses over the fact that a major contributing factor to climate change is electronic weaponry, which strikes the ionosphere, creating ozone or O3. It remains unexplained why Intelligence does not emphasize electronic weaponry/surveillance as a major cause of climate change, as a type of non-particulate pollution that must be eliminated to prevent climate change. This is not even recognized in the report despite Intelligence anticipating that eliminating fossil fuel use *will not* improve climate change. In fact, the report even allows for *increased* directed energy weapons proliferation in the hands of states and terroristic actors, and the 'warming up' of countries to warhead-type nuclear weapons use via the increased use of directed energy weapons.[496]

2020 Pandemic, atmospheric holes forming above the Artic in the spring of 2011, coinciding with the Arab Spring movement.[497] [REWORD – repeated]

This is not only an example - within one report - of the absolutely nefarious deceptions committed by Intelligence and wargamers, but succinctly reveals those policy communities' intentional staging of policy failures and disasters. The simple incriminating question is: when such possibilities are anticipated and outlined in a mere 120 pages ten years ahead of time, why would Intelligence hasten those failures and disasters and not assume the position of preventing them? Such reports should serve as preventative policy guides, not dark prophecy that must be carried out. When these disasters and failures are predicted in government publications, and yet

---

[493] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 66

[494] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 57, 82, 29, 39; 4.

[495] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 10.

[496] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 57-59; 67, 70-71.

[497] Harvey, Fiona. "Record-size hole opens in ozone layer above the Arctic". *The Guardian*. 7 April 2020.

not prevented, or recognized by representatives as known issues when crisis breaks out, then what purpose is Intelligence and the House Intelligence Committee serving?

Perhaps they are satisfied in their own coy sense of knowing rather than acting on the knowledge for others' benefit. As Max Weber writes in *Politics as a Vocation*, "first of all the career of politics grants a feeling of power. The knowledge of influencing men, of participating in power of them, and above all, the feeling of holding in one's hands a nerve fiber of historically important events…With this we enter the field of ethical questions, for that is where the problem belongs: What kind of a man must one be if he is to be allowed to put his hand on the wheel of history? One can say that three pre-eminent qualities are decisive for the politician: passion, a feeling of responsibility, and a sense of proportion."[498] This is discusses in this chapter's section A Kafkaesque Answer to an Orwellian Problem.

+ADD "In a nuclear world the 'small powers' would have vis-à-vis one another: 1. greater opportunities for blackmail and mischief-making; 2. greater accident proneness; 3. an increased capability for 'local' Munichs, Pearl Harbors, and blitzkriegs; 4. pressures to pre-empt because of point 1, 2, and 3 above; 5. a tendency to neglect conventional capabilities because of an over-reliance on nuclear capabilities; 6. internal (civil war, *coup d'état*, irresponsibility, etc.) and external (arms race, fear of fear, etc.) political problems; 7. the creation of a situation in which the diffusion of nuclear weapons to really irresponsible organizations is facilitated. Nuclear diffusion would also: 8. complicate future problems of control, by making such control involve the small powers having to accept an obvious reduction in their sovereignty (i.e., they give something up rather than simply abstain); 9.give the Soviet Union or other large power many opportunities to act as agent-provocateur; and 10. create the capabilities and therefore the pressure for many nations to make a crisis serious or to exploit an on-going crisis (catalytic war or escalation)."[499]

Clearly lacking in a sense of responsibility and proportion, maybe the most appalling of the National Intelligence Council's 2025 policy scenarios predicts failure to create a vaccine against a pandemic disease in which "tens to hundreds of millions of Americans within the US Homeland would become ill and deaths would mount into the tens of millions. Outside the US, critical infrastructure degradation and economic loss on a global scale would result as approximately a third of the worldwide population became ill and hundreds of millions died."[500]

The genre of much of the *Global Trends 2025* report indicates that Intelligence seems to relish vicariously living out of those disasters in writing bizarre diary entries in the voice of a non-existent US president, pretending to be Russian diplomats in an imaginary memo out of the Shanghai Cooperation Organization, and penning fake news articles about unreal events. The tone of the report is one of creative outlet and perverse enjoyment, not analytical assessment and

---

[498] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 115.

[499] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 492-493.

[500] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 75.

sober warning. Why it should come as a surprise that wargamers take security policy to be a game must be too abstract for my reasoning.

At the same time, the report claims that the US will find its increased layering of satellite directed energy surveillance futile in maintaining global security, which will move away from US dominance. +FIND in report

Put this subsection before?

"Warfare in 2025 is likely to be characterized by the following strategic trends:
The Increasing Importance of Information. Advances in information technologies are enabling new warfighting synergies through combinations of advanced precision weaponry, improving target and surveillance capabilities, enhanced command and control, and the expanding use of artificial intelligence and robotics. Future proliferation of long-range precision weapons will permit a growing number of states to threaten rapid destruction of an adversary's critical economic, energy, political, and military and information infrastructures. The growing importance of information technologies as an enabler of modern warfighting capabilities will make information itself a primary target in future conflicts. By 2025 some states probably will deploy weapons designed to destroy or disable information, sensor, and communication networks and systems including anti-satellite, radiofrequency, and laser weapons.

The Evolution of Irregular Warfare Capabilities. The adoption of irregular warfare tactics by both state and nonstate actors as a primary warfighting approach in countering advanced militaries will be a key characteristic of conflicts in 2025. The spread of light weaponry, including precision tactical and man-portable weapon systems, and information and communication technologies will significantly increase the threat posed by irregular forms of warfare over the next 15-20 years. Modern communication technologies such as satellite and cellular phones, the Internet, and commercial encryption, combined with hand-held navigation devices and high-capacity information systems that can contain large amounts of text, maps, and digital images and videos will greatly enable future irregular forces to organize, coordinate, and execute dispersed operations…
The Expansion and Escalation of Conflicts Beyond the Traditional Battlefield. Containing the expansion and escalation of conflicts will become more problematic in the future. The advancement of weapons capabilities such as long-range precision weapons, the continued proliferation of weapons of mass destruction, and the employment of new forms of warfare such as cyber and space warfare are providing state militaries and nonstate groups the means to escalate and expand future conflicts beyond the traditional battlefield."[501]

When arguing that hacker groups like Anonymous and tech corporations like Facebook are given license by the State to work on behalf of the State in foreign policy and defense measures, it becomes important to qualify what hacking and cybercrime entails at such a level.

[501] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 71.

Not only would such individuals, against whom citizens would have no recourse, have access to data about private persons such as can be accessed through computers, this includes the ability to crash cars, airplanes, and disable anything from medical devices like pacemakers to power plants.[502]

But hackers and tech administrators would, and do, have access to what are known varyingly as electronic weaponry, Tesla technologies, Active Denial Systems, broad and directed microwaves technologies, High Frequency Active Auroral Research Program (HAARP), satellite surveillance and communication systems, geographic information systems (GIS), location based systems (LIS), and a host of other incarnations of espionage and human tracking systems. Electronic weaponry can also be used to stage physical attacks on electronics specifically using LOICs.[503] Hackers have even been able to gain access to servers hosting CERN, the European Organization for Nuclear Research that holds the Large Hadron Collider particle accelerator in Switzerland, and NASA websites.[504] + Interesting to note, p 111-125 *Doomsday Scenarios* ch "large hadron collider doomsday fears can help scientists prepare for real dangers/are unfounded".[505] In some very extreme cases, electronic weaponry can even be used to create hurricanes, control weather patterns, divert the Gulf Current, and melt polar ice caps.[506] +Anti-trust accusations and human brain/knowledge as 'competition' for computers/information technology as logical endgame and extreme negative outcome of incentives for EW use. Non-consensual BCI and illegal mergers/cooperation of ICT companies.

Directed energy weapons are atomic energy weapons that produce movement of electrons guided by magnetism to effect radiation. Paradoxically, electronic weaponry has been used to effectively deactivate atomic warheads and nuclear missiles (find cite). From a cyber-realist viewpoint, this makes electronic weaponry more powerful than traditional nuclear warheads.

National Intelligence Council explains the further paradoxical role of limited nuclear weaponry in expanding the use or 'breaking the ice' in using nuclear weapons in Global Trends 2025: "In such cases, the defending power might try to limit the potential for escalation by employing a nuclear weapon test to signal resolve and deter aggression or by confining the use of nuclear weapons to the defense of its own territory. Options for limited physical destruction attacks such as those that use very low-yield weapons or high-altitude nuclear blasts designed to disrupt an enemy's information networks and systems via an electromagnetic pulse effect could further erode the taboo against nuclear weapon use and prompt reassessments of the vulnerabilities of modern conventional military forces. If nuclear weapons are used destructively

---

[502] Schneier, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. W.W. Norton & Company. 2018, p. 9.

[503] See: Olsen. *We Are Anonymous*, p. 478: "LOIC (low orbit ion cannon): Originally created as a stress-testing tool for servers, this open-source Web application has become popular among supporters of Anonymous as a digital weapon that, if used by enough people, can be used to carry out a DDoS attack on a website."

[504] Olsen. *We Are Anonymous*, p. 132; 207.

[505] Bertalsky, Noah (ed.). *Doomsday Scenarios*. Greenhaven Press. 2011. PAGES

[506] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 483-484.

in the next 15-20 years, the international system will be shocked as it experiences immediate humanitarian, economic, and political-military repercussions."[507]

"Psychological Warfare, Information War, and mind control may seem to be exotic topics, but the impact of these technologies and techniques is profound. Our minds are being impacted through a longstanding series of programs aimed at manipulating public opinion through intelligence agencies, think tanks, corporate media and a host of non-governmental organizations designed to engender fear, division and uncertainty in the public. Media manipulation involving the artificial framing of our collective reality is often a hit or miss proposition, but psychological operations have been carried out in the past, and are being carried out even today, through the practices of 'Information Warfare,' directed at enemies abroad and at the American people. According to Mary C. FitzGerald of the Hudson Institute, "New-concept weapons, such as laser, electromagnetic, plasma, climatic, genetic and biotechnological are the central principle driving the modernization of national defense."[508]

+ADD National Cancer Institute:

> Workplace exposures to ELF radiation: Several studies conducted in the 1980s and early 1990s reported that people who worked in some electrical occupations that exposed them to ELF radiation (such as power station operators and telephone line workers) had higher-than-expected rates of some types of cancer, particularly leukemia, brain tumors, and male breast cancer… Workplace exposures to radiofrequency radiation: A case-control study among U.S. Air Force personnel found the suggestion of an increased risk of brain cancer among personnel who maintained or repaired radiofrequency or microwave-emitting equipment. A case-control study found the suggestion of an increased risk of death from brain cancer among men occupationally exposed to microwave and/or radiofrequency radiation, with all of the excess risk among workers in electrical and electronics jobs involving design, manufacture, repair, or installation of electrical or electronics equipment.[509]

While the National Cancer Institute claims that the findings showing that significant cellular and other neurological changes occur under exposure radiation are in the minority, this is simply not true in relevant literature. +ADD W.H.O. article

As results show that populations simply under radar surveillance experience a 20% increase in violent behavior, those closely operating the radar equipment are likely to show an increased rate of violence on par with their increased level of radiation exposure. Behavioral science would also suggest that the violent and senseless actions taken by the intel-surveillance state confirm those findings.

+*Gentlemen: You are mad!* Lewis Mumford, 1946.[510] And while it may not have been their intended meaning, the fanciful term some of these industries have given to electromagnetic

---

[507] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 67.

[508] Phillips, Peter, Lew Brown and Bridget Thornton. *US Electromagnetic Weapons and Human Rights: A Study of the History of US Intelligence Community Human Rights Violations and Continuing Research in Electromagnetic Weapons*. Rohnert Park, CA: Sonoma State University Media Freedom Foundation. December 2006, p. 9.

[509] https://www.cancer.gov/about-cancer/causes-prevention/risk/radiation/electromagnetic-fields-fact-sheet

[510] https://fossilfreeri.org/2018/08/09/people-we-are-absolutely-stark-raving-mad/ ??USE?

experimentation topographical zones, "Wonderland",[511] from Lewis Carroll's *Alice's Adventures in Wonderland* & *Through the Looking Glass*, may have more connotations than Mad-Hatters would like to admit. These programmers choice of literary reference to Lewis Carroll's (real name: Charles Dodgson, a logician and mathematician) literary nonsense work on formal logic for their 'excessively rational to the point of absurdity' uses of quantum topographical programming is another obvious indicator. The quip more appropriate to describe today's lackluster gentlemen's merchants as 'Mad as a Surveillor'. Later on, I will address literal madness as a model of violent political philosophies. [REWORD]

Cyber realism should denote quantum realism, especially where human innovation and human intervention are concerned. Encounters with phenomena that defy causality, such as in the nuclear fields, has led to rejection of Aristotelian naturalism, the philosophy underpinning the scientific method.[512] The rejection of Aristotelian naturalism diminishes the role of epistemology, ontology and mereology in inquiry, and teleology alone supervenes. This reduction is referred to as quietism in the field of physics.[513]

Due to the importance of physicists' input in policy and security concerns, this abstract philosophical or methodological difference in the field of nuclear physics has been misappropriated to fields of policy decisionmaking.
+ADD teleology of war "a necessary function in the perfection of the state… war has a teleological and beneficial impact on the internal workings of the state and the creation of universal history.", from classic political philosophy, eg. Hegel[514]

The result has given relevant experts a propensity to deny Newtonian physics where it does apply (as if familiarity with *defying* causality is precursory to *denying* causality); "In other words, Einstein's theory was very clear on just where Newton's principles ended and where his own theory began. In contrast, crank theories 'usually start and end in mid-air. They do not connect in any way with things that are known'."[515]

This is not an abstract argument, as it applies to the epistemology used by nuclear experts and quantum mechanists, some of whom are high-level decisionmakers on security policy. The result is a widespread and long-term lack of causal knowledge, "that is, knowledge of the relevant or appropriate causes," of any phenomenon or reality.[516]

In the 9th century at the height of Greek revivalism in science, al-Fārābī defined astronomy from astrology, noting that astronomy concerns itself with the measurement and movements of the celestial spheres. Meanwhile, astrology concerns itself with the measurement

---

[511] Find IBM quantum computing video
[512] Marzūqī, Abū Ya´rub. *Mafhūm al-sababīyyah 'ind al-Ghazālī.* Bouslama. Tunis. 1978, p. iv.
[513] https://plato.stanford.edu/entries/realism/
[514] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 96.
[515] Goode, Erich. *Paranormal Beliefs: A Sociological Introduction.* Waveland Press. Illinois. 2000, p. 83.
[516] https://plato.stanford.edu/entries/aristotle-causality/

and movements of the celestial spheres as they relate to the rise and fall of kings, and other "effects of the planets on the sublunary world".[517]

The fact that modern nuclear space science dedicates only 1% of observation satellites to observing outer space, while 99% of observation satellites are dedicated to observing Earth.[518] With space sciences predominately serving security purposes to guard national regimes, all suggests that modern space science is astrology rather than astronomy. Hence, the very unscientific teleological thinking, usually codified in grant proposals for research and development, that has developed in the modern scientific fields that make up the 'astrology' industries.

That top-level security advisors do not 'believe' in cause-and-effect and astrologists' dependence on defense funding, I argue, is partially what leads such industries to adhere to (anti-realist) wargaming as their sole real-world epistemology. Where experiments of observable phenomena are a requirement for planning nuclear security, it has led to unnecessary and infinitely repeated intentional 'controlled' exposures. The policy thought is that such events are 'unavoidable' if we are to know anything about what would result. Even consistent results from multiple repetitions of damaging nuclear experiments are not, under misappropriated quantum anti-realist thought, definitive in nature.

This is an unacceptable risk we live with owed to sloppy philosophical confusion experienced by numericists – for example, the equation of causality with consequences, i.e. there will be no effect to their causing nuclear exposure. While this may be a practical theory in nuclear labs (despite the very physical measures such laboratorians must take to remain safe), it comes across as pestilent irresponsibility and a misappropriation of scientific concepts to policy discussions.

Considering the veil of secrecy and strong arms of intimidation these industries employ to ensure such sloppy misunderstandings persist, I conjecture the confusion or "paradox" is intentional policy subversion. As I discuss in the section A Kafkaesque Answer to an Orwellian Problem, many aspiring or pseudo-scientific types in policy circles are likely to be enticed by the secrecy and the (pseudo-)scientific jargon which justifies such irresponsible policy measures. "…Most crank theories 'aren't even wrong.' Says physicist Jeremy Berstein, 'I have never yet seen a crank physics theory that offered novel quantitative prediction that could be either verified or falsified.'"[519] Classification and secrecy, which apply across the board to nuclear fields and their resultant policy contributions, are conducive to risky bogus scientific claims due to lack of falsifiability.

The mixing of policymaking with nuclear planning lends itself to the narrow predominance of teleology. That is, a narrow focus on justification and intent behind nuclear planning – "it must serve an ultimate end". Nuclear planning based on terms of ultimate purpose alone lead to fatalistic doomsday scenario-making and result in reckless endangerment of entire

---

[517] Janos, Damien. "Al-Fārābī on the Method of Astronomy." *Early Science and Medicine*, vol. 15, no. 3, 2010, pp. 237–265. *JSTOR*, www.jstor.org/stable/20750216. Accessed 8 Apr. 2020.
[518] https://www.sia.org/wp-content/uploads/2017/07/SIA-SSIR-2017.pdf
[519] Goode, Erich. *Paranormal Beliefs: A Sociological Introduction.* Waveland Press. Illinois. 2000, p. 83.

populations. Scientific attention to realistic nuclear uses and the ramifications of exposure or detonation do not exist in 'astrology' industry teleology.

The anti-realism embraced, understandably, by many nuclear experts and quantum mechanists can tend towards an embrace of *superstitious* (although sometimes secular) belief systems. Superstition, as belief system or psychological operation, in the decisionmaking nuclear fields is referenced in RAND's Robert Specht's 1957 essay *War Games* on "writers of science fiction" preferring "the [war] game played on a high-speed computer,"[520] the Pentagon's advertisement of UFOs, and magical jargon like "cloak of invisibility"[521] or "Jedi" used to explain the operators of electromagnetism.

Erich Goode, sociologist specialized in deviance, imaginary deviance (reactions to non-existent phenomena), and moral panic, writes:

> Jean Piaget, a Swiss psychologist (1896-1980), found that teleological thinking is characteristic of children's thinking. For instance, children below a certain age say that the purpose of clouds is to bring rain, the purpose of rain is to water plants, the purpose of plants is to feed humans and animals. One child Piaget interviewed said that, of the two mountains that loomed over Geneva, the higher one was for adults to climb and the lower one was for children to climb. Small children believe that inanimate objects and natural phenomena think and act as human do – that they reason, have goals, and act to achieve those goals.[522]

Chalmers Johnson writes similarly on the impact that the nuclear fields' lack of empiricism has had on US foreign policy:

> Much of RAND's work was always ideological, designed to support the American values of individualism and personal gratification as well as to counter Marxism, but its ideological bent was disguised in statistics and equations, which allegedly made its analyses 'rational' and 'scientific.' Alex Abella writes [in *Soldiers of Reason*]: 'If a subject could not be measured, ranged, or classified, it was of little consequence in systems analysis, for it was not rational. Numbers were all — the human factor was a mere adjunct to the empirical.' In my opinion, Abella here confuses numerical with empirical. Most RAND analyses were formal, deductive, and mathematical but rarely based on concrete research into actually functioning societies. RAND never devoted itself to the ethnographic and linguistic knowledge necessary to do truly empirical research on societies that its administrators and researchers, in any case, thought they already understood.
>
> For example, RAND's research conclusions on the Third World, limited war, and counterinsurgency during the Vietnam War were notably wrong-headed. It argued that the United States should support 'military modernization' in underdeveloped countries, that military takeovers and military rule were good things, that we could work with military officers in other countries, where democracy was best honored in the breach. The result was that virtually every government in East Asia during the 1960s and 1970s was a U.S.-backed military dictatorship, including South Vietnam, South Korea, Thailand, the Philippines, Indonesia, and Taiwan.[523]

---

[520] Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957.
[521] https://globalnews.ca/news/4302166/invisibility-cloak-technology/
[522] Goode, Erich. *Paranormal Beliefs: A Sociological Introduction.* Waveland Press. Illinois. 2000, p. 65.
[523] Johnson, Chalmers. "A Litany of Horrors: America's University of Imperialism". *Tomgram: Chalmers Johnson, Teaching Imperialism 101.* TomDispatch. 29 April 2008.

Quantum realism, as it applies to human innovation and intervention in policy and research and development, being a facet of cyber-realism, is increasing important due to the increasing influence of quantum computers and nuclear physics on human telecommunications and policy decisionmaking. I discuss the political importance of this cyber-reality in my Arab Spring analysis in the section titled Proxy Wars and 'Going Native': Internet Backbone Providers, with reference made to quantum computer surveillance and encrypted Internet traffic in cyber-revolutions. In the present section, The Hacker's Arsenal, the Internet as nuclear engineering and nuclear surveillance/targeting weaponry are the principle topics looked at under cyber or quantum realism.

Simply considering average concepts of hacking one must, Bruce Schneier writes in *Click Here to Kill Everybody*:

> start with the IoT [Internet of Things] or, more generally, cyberphysical systems. Add the miniaturization of sensors, controllers, and transmitters. Then add autonomous algorithms, machine learning, and artificial intelligence. Toss in some cloud computing, with corresponding increases in capabilities for storage and processing. Don't forget to include Internet penetration, pervasive computing, and the widespread availability of high-speed wireless connectivity. And finally, mix in some robotics. What you get is a single global Internet that affects the world in a direct physical manner.[524]

+ADD "NEWS FROM ITEC: Army's 'Google Earth on Steroids' to Include Inside of Buildings" *National Defense* 5/17/2019 [525]

+ADD Game of Drones Microsoft article here

The author adds that when it comes to the operating systems and their updates or "patches", which the downloading of software, "owners have no control over the patching process, and usually have no idea that their devices have even been patched."[526] +ADD https://www.forbes.com/sites/daveywinder/2019/08/24/windows-users-warned-to-update-now-as-complete-control-hack-attack-confirmed/#3eaa636c5bdb

Quote "Your problem is to allocate from day to day your resources of atomic weapons and conventional sorties to the targets of enemy troops, interdiction targets, and airfields, this is the face of the enemy's actions against you. In addition you move your ground troops into the combat zone, supporting them by your logistics network, and exposing them to atomic fire, in an attempt to defeat the enemy forces."[527]
+ADD [TOPIC - SIMILAR TO JOINT INVESTIGATION TEAM] https://www.geneva-academy.ch/joomlatools-files/docman-files/Non-Kinetic-Energy%20Weapons.pdf "The

---

[524] Schneier, Bruce. *Click Here to Kill Everybody*, p. 7.
[525] https://www.nationaldefensemagazine.org/articles/2019/5/17/news-from-itec-armys-google-earth-on-steroids-to-include-inside-of-buildings
[526] Schneier, Bruce. *Click Here to Kill Everybody*, p. 38.
[527] Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957.

paper has been drafted on the basis of discussions at a meeting of experts convened at the Geneva Academy [Geneva Academy of International Humanitarian Law and Human Rights] on 17–19 May 2010 (hereinafter, the 'May 2010 Meeting of Experts') and supporting research.": "A kinetic-energy weapon is one that threatens or inflicts harm to a person through the application to the human body of the energy that a bullet, fragment, or other projectile possesses due to its mass and motion," or formulaically as KE = mv^2/2.[528]
+ADD 12 articles 1 video here or to Radio-logical Warfare:
https://www.washingtonpost.com/local/was-a-spys-parkinsons-disease-caused-by-a-secret-microwave-weapon-attack/2017/11/26/d5d530e0-c3f5-11e7-afe9-4f60b5a6c4a0_story.html
https://edition.cnn.com/2013/09/25/us/washington-navy-yard-investigation/ ;
https://slate.com/news-and-politics/2013/09/aaron-alexis-elf-waves-fbi-says-navy-yard-shooter-may-have-thought-he-was-controlled-by-electromagnetic-waves.html
http://www.i-sis.org.uk/BW.php
https://www.wired.com/2009/07/court-to-defendant-stop-blasting-that-mans-mind/
https://organised-crime-of-covert-electronic-assault-nz.com/wp-content/uploads/2019/09/james_wolbert_protection_against_electronic_harassment_court_order_document_december_20082.pdf
https://www.wired.com/2008/05/army-removes-pa/
https://www.wired.com/2008/12/un-investigates/
https://www.wired.com/story/mind-games-the-tortured-lives-of-targeted-individuals/
https://www.nytimes.com/2016/06/11/health/gang-stalking-targeted-individuals.html?_r=0
https://www.nytimes.com/2008/11/13/fashion/13psych.html?pagewanted=all
https://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399_pf.html
https://www.youtube.com/watch?v=364txWWlS4A John Hall - Satellite Terrorism, Surveillance Technology - 1 April 2010

The use of these technologies to track, harm, stalk, identify, continuously surveil, torture and kill people has been construed by members of the US-Europe Joint Investigation Team, a small group of experts in physics and surveillance, to apply to Article 7 of *The Rome Statue of the International Criminal Court*, an international court dedicated entirely to prosecuting crimes of genocide and crimes against humanity, in the following ways:
1. *Enslavement*—in this case, Electronic Enslavement, by virtue of Continuous Clandestine Tracking and Locating via Non-consensually implanted tracking Microchips, Bio-MEMs, Nanochips, or/and Brain Prints or Brain Bio-Resonance Frequencies, and GPS/GIS tracking satellites; Continuous "Electronic Surveillance" or Assault with Electromagnetic Radiation; Punitive Physical and Neural Assault with Electronic Weapons; Continuous Audio and Video Surveillance with planted bugs and recording and tracking devices in homes and vehicles (Article 7, (c));

[528] Casey-Maslen, Stuart. *Non-kinetic-energy weapons termed 'non-lethal' A Preliminary Assessment under International Humanitarian Law and International Human Rights Law*. Geneva Academy of International Humanitarian Law and Human Rights. October 2010, p. 4.

2. *Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law*—in this case, Electronic Imprisonment, by virtue of severe encroachment and criminal trespass into homes and onto bodies and brains with the use of electromagnetic radiation/sonics, continually or periodically applied (Article 7, (e));
3. *Torture* –in this case, Electronic Torture, by virtue of assault, remote bodily access and manipulation, regular sleep-deprivation, injection of synthetic dreams, images, voices, sensations, remote electro-shocking, remote electrical vibrations, remote neuro-takeover, biohacking and bio-robotizing, all induced with electromagnetic weapons, sonic weapons, neuroweapons, bio-communications devices such as implants and transponders, BCI systems (Brain Computer Interface), and other weapons facilitating covert or clandestine assault (Article 7, f)
4. *Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity*—in this case, Electronic Rape, Electronic Sex Trafficking, Electronic Sexual Slavery, Electronic Sexual Violence, and Electronic Enforced Sterilization, by virtue of sexual assault and violence aimed at the private reproductory and urino-genital systems of women, young girls, men, and young boys, conducted remotely, at a distance, using radiation weapons, sonic weapons, and nonconsensually implanted microchips, neurostimulators, transponders, and Wireless Body Area Networks (Article 7, g).
5. *Persecution...on other grounds universally recognized as impermissible under International Law*—in this case, 1) Electronic Persecution, by virtue of continuous assault & torture with electromagnetic weapons, remote bodily manipulation, remote brain and bodily control, remote EEG cloning and heterodyning (imposing others' Brain Frequencies on one, permitting partial or full-body neuro-takeover), remote cerebral trauma, all induced with the weapons named above; 2) Psychological Persecution, by virtue of subjecting individuals to non-stop electromagnetic tracking and assault, non-stop physical stress creation, non-stop sensory stimulation, forced disruption of activities, non-stop sleep-deprivation, and non-stop COINTELPRO stalking, swarming, interrogation, vandalism, break-ins, gaslighting, employment sabotage, character ruination, social isolation, slander and defamation, public mockery and street theater (Article 7, h).
6. *Enforced Disappearance of Persons*—in this case, Sabotage and Ruination of individuals' Business, Reputation, and Character Assassination, by virtue of dissemination of lies, slander, libelous and defamatory statements about individuals within their own neighborhoods, work and life communities, areas and cities of residence and employment, often rendering individuals homeless, jobless, blacklisted, and unemployable (Article 7, i).
7. *Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health*—in this case, Remote Body and Brain Access, Manipulation, and Assault using the electronic weapons described above, and effecting:

- **Bio/Neuro-Hacking and the Theft of Personal Intellectual Property** (one's brainwaves—whether thought, emotion, sensation, memory, intention, cogitation, mentation, inner voice, or any other);
- **Bio-Robotizing**—which is essentially the neural takeover of a person's brain and manipulating a person's limbs, organs, joints, and entire body from outside;
- **Continuous Psychological, Mental, and Internal Torture** via Voice to Skull and Synthetic Telepathy running abusive monologues inside individuals' brains, an intrinsic aspect of Trauma-Based Mind Control, and prelude to bio-robotizing;

- **Continuous Psychological and Social Trauma** caused by non-stop assault of individuals with Psy Ops-defined inputs related to the individual's life, picked up by intensive surveillance, including neuro-surveillance;
- and the very act of **Trauma-Based Mind Control**, which is the effecting of remote control of people's brains and bodily movements and behaviors by inflicting physical and psychological trauma on them (Article 7, k)."[529]

The United States does not recognize the ICC or its statutes. This has been most fervently expressed in former National Security Advisor and interim US Ambassador to the UN John Bolton's statement that he "will let the ICC die on its own."[530] Bolton's quote was featured in an article favorably shared by President Trump on his Twitter account.[531] It should be noted that in 2016 the US State Department also cut off contact with the UN Human Rights Commission.[532] It also has refused to render US military personnel for prosecution in the ICC for crimes of torture against Afghan citizens - accusations which the US Senate Select Committee on Intelligence confirmed as characteristic of US Intel activities and topic of perjury.

+ADD "By transmitting channels of disinformation from hidden locations, clandestine PsyOp radio shares ideological trajectories with the ultrasonic beam technology. It is in their scope that they differ. Whereas the radio focuses upon creating multiple mass deceptions of the social body, the HSS targets the individuated body and endeavours to alienate and isolate it from the enveloping social networks it is a part of. The convergences of these technologies can easily be registered again however, in their dislocative schema. Both the radio's and the HSS's capacity to achieve 'multi-channelled states' in or around their targeted listeners is reliant upon the inability of those who hear, to locate the source of the transmission (a schizophonic or acousmatic (see glossary) state). For now, we will be further exploring the term schizophonia as it more precisely articulates the military's waveformed agenda to cause a multiplicity of psychological maladies in its targets, including those of confusion, disorientation, and alienation."[533]

LOIC (Low Orbit Ion Cannon) is a common tool used by hackers in DDOS (Distributed Denial of Service) attacks that utilizes physics rather than social engineering to attack. …+more "That day, nine hundred people suddenly jumped into #operationpayback, the main public chat room on AnonOps IRC, which had been quiet for months. About five hundred of these people had volunteered their computers to connect to the LOIC 'hive.' By now LOIC had an automatic

---

[529] US-Europe Joint Investigation Team. "Notice of Crimes Against Humanity Using Energy & Neuro/Bio Weapons, Notice of Criminal Trespass, Notice of Theft of Intellectual Property, Notice of Impending Criminal Charges". *The Everyday Concerned Citizen*. 28 August 2017.

[530] Crabtree, Susan. "On Trump's ICC Win, Dems and Republicans See Eye to Eye". *Real Clear Politics.* 15 April 2019.

[531] https://twitter.com/realdonaldtrump/status/1118370255091507201?lang=en

[532] https://usun.usmission.gov/remarks-on-u-s-withdrawal-from-human-rights-council-impact-and-next-steps-at-the-heritage-foundation/

[533] Heys, Toby. *SONIC, INFRASONIC, AND ULTRASONIC FREQUENCIES: The Utilisation of Waveforms as Weapons, Apparatus for Psychological Manipulation, and as Instruments of Physiological Influence by Industrial, Entertainment, and Military Organisations*. March 2011 http://researchonline.ljmu.ac.uk/id/eprint/6092/1/543845.pdf

function; you only needed to set it to hive mode and someone in #command would set the target and time. They would type simple instructions into their configured IRC channel - 'lazor start' and 'lazor stop.' Normal users didn't have to know who the target was or when you were supposed to fire. They could just run the program in the background."[534] During this 'operation' concerning Wikileaks, this weapon was directed at "the main site of Senator Joseph Lieberman, the chairman of the U.S. Senate Homeland Security and Governmental Affairs Committee, which had first pushed Amazon to stop hosting WikiLeaks."[535]
"Most countries don't have either the budget or the expertise to develop this caliber of surveillance and hacking tools. Instead, they buy surveillance and hacking tools from cyberweapons manufacturers. These are companies like FinFisher's seller Gamma Group (Germany and the UK), HackingTeam (Italy), VASTech (South Africa), Cyberbit (Israel), and NSO Group (also Israel)."[536]

On third party hardware and software - laptops and servers
https://www.army.mil/article/199368/raven_claw_augments_battle_management_for_electronic_warfare_operations

https://www.raytheon.com/news/feature/electronic-warfare-laptop
https://www.dote.osd.mil/pub/reports/FY2018/pdf/army/2018ewpmt.pdf

+ADD Dissertation, p. 146-219 "CHAPTER 3 The Inverted Eschatology of Black Ecstasy: When Music Becomes Painful in Guantanamo Bay" *SONIC, INFRASONIC, AND ULTRASONIC FREQUENCIES: The Utilisation of Waveforms as Weapons, Apparatus for Psychological Manipulation, and as Instruments of Physiological Influence by Industrial, Entertainment, and Military Organisations*. By TOBY HEYS 2011http://researchonline.ljmu.ac.uk/id/eprint/6092/1/543845.pdf From abstract: "In chapter one it is argued that since the inception of wired radio speaker systems into U.S. industrial factories in 1922, the development of sonic strategies based primarily on the scoring of architectonic spatiality, cycles of repetition, and the enveloping dynamics of surround sound can be traced to the sonic torture occurring in Guantanamo Bay during the first decade of the twenty-first century. Exploring the use of surround sound speaker techniques by the FBI during the Waco Siege in Texas, this argument is developed in chapter two. In chapter three it is further contended that the acoustic techniques utilised in the Guantanamo torture cells represent the final modality and the logical conclusion of these strategies that have evolved between civilian and military contexts over the past 80 years. In chapter four, the speaker system instrumentality of the HSS ultrasonic beam - occurring post Guantanamo - comes to symbolise an epistemic shift in the application of waveformed pressure; the dynamics of directional ultrasound technology signalling the orchestration of a new set of frequency-based relations between the transmitter and the receiver, the speaker system and architectural context, and the civilian and war torn environment."
[TOPIC – power theory on electronic weaponry]

---

[534] Olsen. *We Are Anonymous*, p. 111.
[535] Olsen. *We Are Anonymous*, p. 111-112.
[536] Schneier, Bruce. *Click Here to Kill Everybody*, 65.

"Existing in a web of power relations, this vacillating subjectivity transmits, mutates, and receives information according to the micro-sound politics, noise, and collective harmonies emitted from the network of surrounding embodied speakers that it finds itself within. It is in this distributed system of social influence that we are able to monitor the ongoing spatial negotiations, methods of psychological alienation, and strategies of physiological manipulation that simultaneously locates and displaces our missing waveformed body of knowledge. Now that we have heard about the capacity of our muted subjectivity and its possible whereabouts, we can say that this is the body that will be investigated, spatialised, historicised and ultimately fleshed out through the study. We can also name it. It is the antenna body. The antenna body speaks to us about being-in-the-world-of-waveforms… Our line-up of previous somatic modalities of waveformed thought has told us much about where we need to search for our missing waveformed body of knowledge in order to perceive, spatialise, and socio-politically register it. We now need to explore new philosophical terrains and parameters in order to flesh out the movements of the antenna body and the martial, industrial and civic networks it exists within. A new set of questions need to be forwarded in order to locate its agency, potential, and socio-political register; enquiries that engender asking - Who develops frequency-based technologies in order to capture, index, and harness imperceptible frequencies and how are they utilised to shape social, temporary, and private space? How do we define the behaviours of, the fleshy interface of, and the extension of the body in a vibrational field of relations? How do we name, record, and traverse the thresholds between sound and silence, between presence and absence? Only when we have answered these questions will we able to say that we have started mapping the sensorial topologies of the antenna body; a cartography of influence, manipulation, and torture that will enable us to better articulate its movements and transgressions and our own sense of space and orientation in relation to it."[537]

Matossian "Poisons of the Past: Molds, Epidemics, and History" summary
https://www.journals.uchicago.edu/doi/abs/10.1086/355568 [move?]

Radio-logical Warfare
Sometimes I think evil is a tangible thing - with wave lengths, just as sound and light have.
Richard Connell, *The Most Dangerous Game* (1924)

The purpose of delineating this section from the previous section The Hacker's Arsenal, which focused on the technical capabilities of cyberwarfare, is to highlight the Janus-faced nature of weapons systems. Rarely are technological weapons discussed in one venue as both weapons of physical destruction and societal destruction. Each and every technological weapon has a double-life, so to speak, between weapons program briefs and psychological strategy boards.

+ADD Operation Just Cause/Nifty Package Dec. 20, 1989 – Jan. 3, 1990: "'But what we could not plan for was an **aerial bombardment**, which is exactly what happened,' Noriega later

[537] Heys, Toby. *SONIC, INFRASONIC, AND ULTRASONIC FREQUENCIES: The Utilisation of Waveforms as Weapons, Apparatus for Psychological Manipulation, and as Instruments of Physiological Influence by Industrial, Entertainment, and Military Organisations*. March 2011 http://researchonline.ljmu.ac.uk/id/eprint/6092/1/543845.pdf P. 13-14; 21.

lamented. The U.S. Air Force dropped 422 bombs on Panama in 13 hours, destroying the PDF [Panamanian Defense Forces] by **disconnecting its principal lines of communication**… Eventually Noriega escaped the U.S. manhunt by seeking refuge in the residence of Monsignor Sebastian Laboa, the papal nuncio to Panama… For the next two weeks U.S. troops circled the embassy, blaring Guns and Roses' 'Eye of Destruction' and other noisy **rock songs from giant speakers in a peculiar attempt to unnerve Noriega through questionable art. 'It was a low moment in U.S. Army history,' Scowcroft later admitted. Blasting rock music was silly, childish, reproachable, 'undignified.' But in some strange, postmodern way it worked. CNN broadcast the United States versus Noriega showdown continuously**, as Panama's 'Maximum Leader' was transformed into 'Hunted Fugitive,' a corrupt drug dealer who had thwarted the will of the Panamanian people and was now hiding in a papal basement. Hunkered down in a dirty T-shirt, baggy Bermuda shorts, and a baseball cap pulled low over his face, forced to listen to American rock and roll, Noriega had become **an international joke overnight**…. [January 3, 1990] Monsignor **Laboa consulted with U.S. major general Wayne Dowling** about what to do. **After the meeting the monsignor found his resolve and asked Noriega to evacuate his residence**; within a few hours Noriega, afraid of being lynched, walked out of the nunciature and surrendered to American forces. He was place on a helicopter to Howard Air Force Base and delivered to the custody of the U.S. Drug Enforcement Agency."[538]

+ADD Adam Scott Wandt, an assistant professor of public policy at the John Jay College of Criminal Justice, said the LRAD can be a weapon in addition to a communication tool.
"**Adam Scott Wandt, an assistant professor of public policy at the John Jay College of Criminal Justice, said the LRAD can be a weapon in addition to a communication tool**. An LRAD [long range acoustical device], which looks like a large black speaker, can function as a public-address system, giving police a way to communicate with a large crowd, Wandt said. Activate what is called the 'area-denial function' on the device and it becomes a 'sonic weapon,' he said. On the model purchased by the NYPD, the control panel warns in all capital letters, 'Do not enter within 10 meters during continuous operation' when the LRAD is employing the area-denial function, court documents said. 'Making someone feel pain and discomfort is a use of force,' Wandt said. LRAD Corp., which makes the device, did not respond to NBC News' repeated requests for comment. 'The officers that used this technology knew or should have known it would cause pain in the protesters that they are using it on,' Wandt said, 'The government has very well documented ... that damage could occur with sounds over 100-120 decibels. This product clearly exceeds those limits.' In the case of a violent protest, Wandt said he understands why police might want to use LRADs in place of potentially lethal force. But, he said, 'When **law enforcement adopts new technologies, they have a responsibility to understand how they work, especially before they use them on a civilian population** that is nonviolent,' like at the protest [Anika] Edrei attended in 2014. Edrei hopes the suit will lead to others **being protected from the sonic device's harmful effects and lead to policy change**."[539]

+ADD [Female interviewee] On ISIS in Mosul "They understood how to attack us mentally before they attacked us with weapons. They made us fear them." [@1h:28m]

---

[538] Bose, Meena and Rosanna Perotti. *From Cold War to New World Order: The Foreign Policy of George H.W. Bush*. Hofstra University Contributions in Political Science, No. 393. Greenwood Press. 2002, p. 180-181.
[539] https://www.nbcnews.com/news/us-news/plug-your-ears-run-nypd-s-use-sound-cannons-challenged-n1008916

[Female interviewee 2] June 5-11, 2014 In Mosul, one day after departure of regular US troops: "I remember at dawn, I heard the sound of megaphones. 'We are the Islamic State in Iraq and the Levant.' [I said] 'What Islamic State? What does this mean?'.
[Male interviewee] "'We drove through the city. The army that used to insult the people on a daily basis in the checkpoints have disappeared. They collapsed. We thought the security forces would come back, fight back, the terrorists would leave. But then, when I saw the weapons, the new cars, they were almost all in one uniform, I became totally sure that ISIS is here to stay.'… What we used to see as the police was now the Islamic police. What used to be the Iraq flag is now the black flag of ISIS. From day one, you would see in the street what they called the media outlet putting on the TV monitor ISIS videos, showing their propaganda… I saw, myself, children between twelve to fifteen years old joining ISIS just after watching a video.'
[Interviewer] 'Would ISIS have existed if America had stayed?'
[Male interviewee 2] 'I don't think so, no. The Americans would have stopped that. The USA committed two major bad things in Iraq. First was invasion, and the second was withdrawing from Iraq.'"[540]
On US Special Forces presence in Iraq throughout ISIS occupation, dispatched to Northern Iraq June 15, 2014: https://en.wikipedia.org/wiki/American-led_intervention_in_Iraq_(2014%E2%80%93present) ; +ADD "The 90 Special Forces troops were joining 40 troops pulled from assignments at the U.S. Embassy in Baghdad to set up a Joint Operations Center with the Iraqi military. An additional 50 Special Forces troops were expected to arrive in Baghdad in the next several days, said Rear Adm. John Kirby, the Pentagon press secretary. President Obama has authorized up to 300 Special Forces troops from U.S. Central Command deploy to Iraq to aid the crumbling Iraqi military fighting the advancing forces of the Islamic State of Iraq and the Levant. Kirby stressed that the Special Forces troops would be working with the Iraqis at the headquarters and brigade levels."[541]

+ADD "Porter's early dispatches from Saigon include a host of new initiatives for closer cooperation with the VIS. In mid-October he reported a surge in *Chieu Hoi* returnees, **citing leaflets and loudspeakers as the reason for their defection.** On 23 October 1965, the South Vietnamese, with U.S. help, launched a major initiative in the Mekong Delta based on a claim of 'inevitable victory.' Forces deployed included four million air-dropped leaflets, twenty-three loudspeaker aircraft, and loudspeakers mounted on a fleet of three-wheeled Lambretta scooters. Meanwhile, in the center of the country, **JUSPAO [Joint United States Public Affairs Office] unveiled its so-called 'spirit record,' a ghostly mixture of traditional Vietnamese funeral music, unnerving sound effects, and the grotesquely amplified sound of weeping women or a child crying, 'Daddy! Daddy! Come home…'** The breakthrough lay in effective cooperation with the South Vietnamese."[542]
+ADD "'Voice of God' weapon being used in Iraq"
https://www.dailykos.com/stories/2007/12/23/425814/- ;
"The Voice of God Weapon Returns" https://www.wired.com/2007/12/the-voice-of-go/ ;

---

[540] *Once Upon a Time in Iraq.* 14 July 2020. https://www.pbs.org/wgbh/frontline/film/once-upon-a-time-in-iraq/
[541] https://www.military.com/daily-news/2014/06/24/90-us-special-forces-troops-arrive-in-baghdad.html
[542] Cull, Nicholas J. *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989.* Cambridge University Press. 2008, p. 270.

"HOMEMADE MICROWAVE WEAPONS"
https://globalguerrillas.typepad.com/globalguerrillas/2004/05/journal_homemad.html
"'Heat Ray' And 'The Voice Of God': My Experience With The Nonlethal Weapons Eyed For Use In D.C. Protests" https://www.forbes.com/sites/markcancian/2020/09/18/will-dod-deploy-a--heat-ray-and-the-voice-of-god-against-demonstrators/?sh=5861c4bf7add [move to urban warfare planning?]
"voice of God weapon used in Iraq Medusa v2k"
https://www.youtube.com/watch?v=hPQ6pr9yh14
"LRAD's CEO Woody Norris Describes His Company's " Voice of God" Sonic Weapon"
https://www.youtube.com/watch?v=1pefJgkG0lw

On Army electronic warfare in Cold War operations: "But while high-bandwidth national networks rely on fiber-optic landlines and undersea cables, tactical networks have to work on the move, which means they're wireless. So tactical cyber warfare depends on *electronic* warfare, the use of radio waves to detect, disrupt, and deceive the enemy's transmissions while protecting your own. Unfortunately, the Army disbanded its electronic warfare corps after the Cold War."[543] [REPEATED in Proxy Wars]

"Between 2005 and 2010, the State Department funneled $12 million to opposition groups opposed to Assad. The US also financed Syrian exiles in Britain to start an anti-government cable TV channel they beamed into Syria."[544]

During the Soviet invasion of Afghanistan, the US sought to counter Soviet media efforts by broadcasting the US sponsored RadioFree Afghanistan station in 1985.[545]
-document from National Security Archives 1985 on Pakistani Intelligence aircraft broadcasting RadioFree Afghanistan[546]
-Reauthorized Radio Free Afghanistan in 2001[547] broadcast fr Oom Kuwait by then-Senator Joe Biden for $17 million in 2001 alone
-Al-Hurra television before US invasion of Iraq (already cited?)
http://eds.a.ebscohost.com.ezproxy.shsu.edu/eds/results?vid=0&sid=24164ff2-5bf5-489d-b18b-644f70abe70d%40sdc-v-sessmgr03&bquery=al-hurra&bdata=JmNsaTA9RlQxJmNsdjA9WSZ0eXBlPTEmc2VhcmNoTW9kZT1TdGFuZGFyZCZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d
-RadioFree Europe and Radio Liberty: 26 languages, available across social media platforms[548]

---

[543] Freedberg, Sydney J., Jr. "Can Army Afford The Electronic Warfare Force It Wants?". *Breaking Defense.* 19 November 2018.
[544] Bramhall, Stuart Jeanne. "The Arab Spring: Made in the USA: Review of Ahmed Bensada's Book". *Global Research.* 22 March 2018. Electronic resource. < https://www.globalresearch.ca/the-arab-spring-made-in-the-usa/5484950>. [previously published https://dissidentvoice.org/2015/10/the-arab-spring-made-in-the-usa/]
[545] Clarity, James F. "BREIFING; Come In, Afghanistan". *The New York Times.* 1 October 1985.
[546] [PRINTED]
[547] 107th Congress. "S. Rept. 107-125 - AUTHORIZATION OF 'RADIO FREE AFGHANISTAN'". Senate Report: Foreign Relations. US Congress. 14 December 2001.
[548] https://pressroom.rferl.org/about-us

- https://www.globalresearch.ca/us-grant-35-million-promote-fake-news-bubble-syria-control-local-media/5701830

Audio radio and radar weaponry, although used for distinct purposes in war, have the combined effect to increase nuclear biological damage on a population. From the point of view of physics, the difference between radio and radar-enabled weaponry is in levels of directed radiation intensity. From the point of view of war weaponry strategy, any reason to increase exposure in a population serves as a weapon. It is not only the audible transmission of audible radio, the words and ideas, that are strategy of war, but the pretext for higher transmission of radiation directed at a population is also part of the war strategy. Both the intellectual and physiological are considered psychological war strategy.

Broadcasting stations also make an ideal cover for radar weaponry control stations. As Biden's December 2001 bill stated, despite *Voice of America* radio already broadcasting successfully in Afghanistan in 2001 with "a substantial audience inside the country", $9 million, - "the capital funding authorized in the bill [that] contemplates construction of a new shortwave transmitter in Kuwait," - gave legal authority to exceed fiscal year 2002 Congressional budget in order to provide grant money for the sole purpose of funding Radio Free Afghanistan.

The bill also repealed "a permanent ban on construction of a U.S. shortwave radio transmitter in Kuwait. The ban was enacted in 1994, at a time of serious budget stringency and in the aftermath of the cancellation of a major transmitter project in Israel." It also designated the facility "to use U.S.-owned transmitters in Kuwait for broadcast of *Radio Free Iraq* or RFE/RL's Persian Service."[549]

This Janus-faced use of media in war is apparent when considering the purpose of broadcasting audiovisual messages to a population, allegedly as information propaganda, while simultaneously destroying the electric grid that that population would need in order to consume that propaganda.

In his 1996 article "The Story Behind Finnish Telecommunications Industry: Military Radio Systems and Electronic Warfare in Finland during World War II", research technologist Pekka Eskeline writes:

> Late summer 1941, when the Finnish forces had already done a re-entry to the city of Viipuri, which was lost to Russia in March 1940, a couple of **radio-controlled mines** were found beside a bridge. Also, sudden explosions were heard in areas which should have been under Finnish control. Rapidly, it turned out, **that the whole city seemed to be covered with such radio mines and Finnish specialists suggested a jamming action to be carried out on a frequency, which could be defined from the previously found mine. A popular Finnish folk song "Sakkijarven polkka" was played day after day through a powerful conventional AM transmitter.** The choice of the record was not based on its popularity, but **this particular piece of music (actually not a very nice one) happens to be practically continuous with no silent spots. Several triggering attempts by an audio triad could be heard on the band, but the music covered it until the batteries of the mines were**

[549] 107th Congress. "S. Rept. 107-125 - AUTHORIZATION OF 'RADIO FREE AFGHANISTAN'". Senate Report: Foreign Relations. US Congress. 14 December 2001.

> **exhausted**. The action probably not only minimized the destruction of the city but also saved the castle of Viipuri for the coming generations… There exists a direct, though long relationship between the Radio Workshop of the Armed Forces, which produced the transmitters for Finnish guerilla troops; the State Electrical Workshop, which was responsible for many Air Force radios; and the present Nokia Telecommunications, the well-known supplier of both microwave equipment, cellular radio systems and - not too astonishingly - modern military communication infrastructure.[550]

Not all music used in radio warfare is audible songs familiar to listeners, however. Radio may broadcast music which is inaudible to the unaided human ear. **For an example of (ELF) extremely low frequency music used in warfare,** I highly recommend the (audible frequency) song titled "The Sun's Gone Dim and the Sky's Turned Black" composed by Icelandic composer Jóhann Jóhannsson (1969-2018), son of IBM software engineer, in his album *IBM 1401, A User's Manual.* The vocals of the track are imitative of ELF transmissions used in radio-enabled psychological warfare. Just like with any music, the transmission's effect on its environment, including the human mind and body, is housed within worded lyrics, tones/frequencies, durations and repetitions.

In *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* de Goede, Bosma and Pallister-Wilkins write on techwarfare's unstated role in wargaming: "Whereas Straube and Bosma mainly focus on digital security technologies, Sarah Hughes and Philip Garnett in Chapter 12 develop a broader understanding of 'technology' as a mode of governing that includes 'multiple technologies by which state actors work to influence a narrative surrounding an event or process."[551] [ADD from Chapter 12]

Anais, Seantel. 2013. "Objects of Security/Objects of Research. Analyzing Non-lethal Weapons" pp. 195-198 Research Methods in Critical Security Methods. Routledge. [the designation 'non-lethal' can equate to implements of torture]

From *On Thermonuclear War*: "Offhand, it might not seem reasonable that bacteriological and chemical weapons might be acceptable when nuclear neutron weapons are not, but this might be true of specialized bacteriological or chemical weapons that could be used to enfeeble temporarily or otherwise impair the efficiency of the enemy's civilians or soldiers. The classical use of tear gas in civilian disturbances has exactly this character of being a much more acceptable weapon than ordinary bullets. In fact, it is conceivable that one might develop an effective capability of just having psychological effects on the enemy. For example, if one gave tranquilizers to the enemy soldiers in large amounts they might become unfit for military duty."[552]

---

[550] Eskeline, Pekka."The Story Behind Finnish Telecommunications Industry: Military Radio Systems and Electronic Warfare in Finland during World War I1 (1939-1945)". *IEEE AES Systems Magazine*, August 1996, p. 6-7.

[551] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 16.

[552] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 486.

[Re: connection to wargames/continuous simulated warfare as continuous psychological warfare]

From *On Thermonuclear War*: "Warning systems against ballistic missile attacks may depend not only on radar but may also use infrared, various types of electrical signals, acoustical noise, or optical observation."[553] [justifications used in Biden legislation in Kuwait pre Iraq War, Radio Free]

[TOPIC – US patent for bio-electronic weaponry programmable through social media analytics and alterable through Internet-hosted music files]

+ADD "System and method of generating high voltage variable frequency electromagnetic radiation" US Patent 10,252,072 Advanced Biotechnologies, LLC. April 9, 2019: "**In a high voltage, variable frequency radiation generation system**, a carrier signal supplied to a primary coil of a transformer is varied, e.g., turned ON and OFF at variable frequencies. The ON duration and/or the average amplitude of the carrier signal may also be varied. Moreover, the carrier signal may be modulated using an audio signal. The parameters to control the variation of the carrier can be provided as a recipe via a software application. A server can provide different types of apps providing different control features. **The server may also collect user characteristic data and recipe usage data, and may facilitate exchange of these data and may recommend recipes based on a particular user characteristic**… According to various studies, the body of a living being has the inherent **ability to selectively absorb the needed frequencies through cells of the skin, nerves, muscles, connective tissues, and organs**. As such, **controlled electromagnetic pulses may provide** a jump-start to dysfunctional cell-level electrical systems, e.g., those experiencing **significant impedance to proper signal flow and thereby adversely affecting function of such systems.** Exposing the body to controlled electromagnetic radiation, therefore, can help in improving wellness… **The usage data corresponding to one or more users may receive from a social medium account (e.g., Facebook.TM., Twitter.TM., or WhatsApp.TM. account) of the user. Alternatively or in addition, the usage data corresponding to one or more users may be received from a resonant electromagnetic radiation device, where the user has been exposed to radiation from that device. The usage data corresponding to one or more users may be received via a network, e.g., the Internet. One or more user characteristics of one or more users may include user's temperature, pulse rate, respiration rate, blood pressure, and/or electroencephalogram (EEG).** The indication of usage may include a frequency of usage and/or an effectiveness measure… **the method also includes selecting a user characteristic from the recipe database that matches with the user characteristic received separately, and transmitting to a destination at least one recipe from the set of recipes corresponding to or correlating with the selected user characteristic. The destination can be a social medium account of a user and/or a controller of a resonant electromagnetic radiation device… One or more usage data elements corresponding to a user may be received, via a network, from a social medium account of the user and/or a controller of an resonant electromagnetic radiation device used by the user.** The modulation style may include audio modulation, and **the recipe may further include an audio file identifier, such as a reference to a memory location in storage, a link to a song file on the Internet, a home network, etc.** In some embodiments, the modulation style **includes frequency sweep**… In one embodiment, the output voltage of the power supply 108 can be adjusted to any value **within the range of 50-300V DC**. Additionally or in the

[553] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 480.

alternative, **the processor 126 can provide a stored audio signal (e.g., a song), via a selector/mixer 128, to control the output DC voltage** supplied by the variable DC-DC power supply 108 at the output 110. Specifically, the output voltage can be varied according to instantaneous frequencies of the stored audio signal. As the output voltage is used to generate the carrier frequency, the amplitude of the carrier can also vary according to the instantaneous frequencies of the audio signal, thereby resulting amplitude modulation of the carrier. In some embodiments, alternatively or in addition, **an audio signal can be received from an external source (e.g., a smart phone, CD player, etc.) at an audio input port 130, and can be used to modulate the carrier in a manner similar to amplitude modulation** using the stored audio signal. **The audio signal may be received or streamed via a network (such as the Internet, a user's home network, etc.)**, as well."[554] [120 Volts AC standard in US home electrical outlets]

J.E. Dobson, professor and former Department of State Senior Scientist in the Office of the Geographer and Global Issues, and P.F Fisher, professor of geographical information, describe electronic weaponry in their article "Geoslavery", which appeared in *IEEE Technology and Society Magazine* in 2013, in the following passage:

> Geoslavery is defined here as a practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave. Inherent in this concept is the potential for a master to routinely control time, location, speed, and direction for each and every movement of the slave or, indeed, of many slaves simultaneously. Enhanced surveillance and control may be attained through complementary monitoring of functional indicators such as body temperature, heart rate, and perspiration. It is possible to monitor people and exert behavioral control manually, as slavemasters have done for centuries. The key to widespread adoption, universal coverage, and exceptional precision, today, lies in recent advances of electronic information systems. Human tracking systems, currently sold commercially without restriction, already empower those who would be masters, and safeguards have not yet evolved to protect those destined to become slaves. Current products freely exploit the GPS and other digital information offered as a public good, but no government has yet established any specific statutes or regulations restricting their use… Inexpensive human tracking systems that combine these three technologies are now commercially available and widely marketed. Individual units currently sell for less than $300...Anyone monitoring the tracking system can exert control over the person being tracked by reprimanding or otherwise punishing the person in near real time or retrospectively at the end of each day, week, or year. Only one other technology is necessary to enforce real-time control. Simply add a transponder that receives a radio command from the master and instantaneously shocks, stings, burns, or otherwise punishes the slave. The technical feasibility of two-way LBS has been proven. One human-tracking device comes with a remote-control lock, and another commercial product (not advertised for human tracking) comes with a GPS receiver and two-way radio combined in a single hand-held unit... If the slave were to transgress, a command could be transmitted instantaneously to the transponder, which would administer punishment. The result would be an electronic form of geoslavery... A master can prescribe a route and force a slave to follow it to a precision measured in centimeters. Or, a master may grant a slave free rein except for certain areas

---

[554] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10,252,072.PN.&OS=PN/10,252,072&RS=PN/10,252,072

> defined as taboo. Or, a master may limit a slave's visits to specified places, times, and durations. Or, a master may prohibit intersections between a slave's track and that of any other specified slave or group of slaves...Such systems are already in use to incarcerate convicted criminals in Britain and the U.S. Prisoners are allowed to be in certain places at certain times, and not to range outside a prescribed polygon. These people have been found guilty in a recognized judicial system and are having their liberty curtailed as part of the criminal justice system. Others, however, may be subject to the same technology without due process. ...Tyrants who choose to dominate their subjects, husbands and wives who choose to dominate their spouses, and employers who choose to dominate their employees now may do so in the extreme... In 1967, for example, during early development of GIS to support computerization of the 1970 census, a Yale University administrator declared the efforts a threat to individual privacy and closed the project's computer accounts ... In the current War on Terrorism, strong positions have been expressed on both sides regarding increased U. S. government access to information about personal transactions (including their geographic coordinates) following the terrorist attack of September 11, 2001. In the climate of fear that currently exists around the globe, one might readily imagine the citizens of any nation demanding that all suspicious foreigners be tagged with human-tracking devices for the duration of their stay. Or, they might take it further and demand that all foreigners be tagged. Or, they might include their fellow citizens as well... Being digital, LBS can be programmed so that it watches each and every subject, evaluates myriad pathways based on models or sets of rules, and automatically issues instructions and punishments... With LBS, one human operator could monitor 1,000. . .10,000. . .100,000. . .1,000,000 fellow humans and yet know if any one of them steps off the path by more than a few centimeters.'[555]

+ADD **State surveillance may meet the standard of political imprisonment**:
1) deprivation of liberty including the impossibility of leaving a certain place at will [on surveillance – it is impossible to leave global or localized tracking-enabled surveillance, it is possible to prevent movement with punitive energy weapons and electronic barriers], being under guard, made vulnerable to severe punishment, held in a place in which access is prohibited or restricted, denial to any trial or fair trial in which state surveillance is imposed after sentencing, proven necessary, or illegal;
2) political motivation by authorities, explicit (such as public campaign of pre-election, anti-corruption, or anti-terrorism) or by hidden causes of actions or omissions by authorities.[556]

With this approach, it is possible to interpret every person on the planet as a political prisoner or potential political prisoner. The actions taken during the COVID-19 pandemic by global, national and local state entities, including lockdowns and contract tracing, have proven this approach legitimate in international and human security research.

This is not the only example of governments systematizing irradiation as a means of social control. In a document used by the prosecution of Nazi war criminals during the Nuremberg trials titled "Covering Letter from Brack to Himmler, 28 March 1941, with Report on Experiments Concerning Sterilization and Castration by X-Rays" classified "Top Secret" reads:

Dear Reich Leader:

---

[555] Dobson, J.E, and P.F Fisher. "Geoslavery." *IEEE Technology and Society Magazine*, Vol. 22, No.1. 2013, p. 47-52.

[556] https://memohrc.org/en/specials/guidelines-definition-political-prisoner

> Enclosed herewith for your information is the result of the investigations into the possibility of sterilization or castration, respectively, by means of X-rays... high X-ray dosages destroy the internal secretion of the ovary, or of the testicles, respectively. Lower dosages would temporarily paralyze the procreative capacity...
> The actual dosage can be given in various ways, and the irradiation can take place quite imperceptibly. The necessary local dosage for men is 500-600r [rotengen], for women 300-350r. In general, an irradiation period of 2 minutes for men, 3 minutes for women, with the highest voltage, a thin filter and at a short distance, ought to be sufficient. There is, however, a disadvantage that has to be put up with: as it is impossible to noticeably cover the rest of the body with lead, the other tissues of the body will be injured, and radiological malaise, the so-called 'Roentgenkater', will ensue. If the X-ray intensity is too high, those parts of the skin which the rays have reached will exhibit symptoms of burns...
> One practical way of proceeding would be, for instance, to let the persons to be treated approach a counter, where they could be asked to answer some questions or to fill in forms, which would take them 2 or 3 minutes. The official sitting behind the counter could operate the installation in such a way as to turn a switch which would activate the two valves simultaneously (since the irradiation has to operate from both sides.) With a two valves installation about 150-200 persons could then be sterilized per day, and therefore, with 20 usch installations as many as 3000-4000 persons per day.
> In summary, it may be said that, having regard to the present state of radiological technique and research, mass sterilization by means of X-ray can be carried out without difficulty. However, it seems to be impossible to do this in such a way that the persons concerned do not sooner or later realize with certainty that they have been sterilized or castrated by X-rays. [Signed] Brack.[557]

Ironically, the simultaneous technology innovated for translation at the Nuremberg Trials, used to convict Nazi war criminals for such crimes as inducing radiological malaise and sterilization, resembles the advantages touted today by those in favor of using radiation surveillance to prosecute war criminals:

> Anyone in the courtroom with a headset could listen to the language of his or her choosing. Whitney Harris, a member of the American prosecution staff, describing the new 'instantaneous translation' system [said], 'Whatever was said on an incoming line was instantaneously translated into the other languages by wonderfully skilled interpreters. The interpretations then went into every chair in the courtroom by other telephonic wires, to be picked up through headphones for which a switch was provided to enable the listener to select the preferred language. It was the first time in history that such a system had been used in a judicial proceeding or, for that matter, in any hearing of such length and complexity. After the trial began, Reich Marshal Hermann Göring—who spoke English as well as German—exclaimed, 'This system is very efficient, but it will also shorten my life!''[558]
> [MOVE?]

Many devices have special capabilities that just so happen to double as surveillance capacities. For example, the "gyroscope on your iPhone, put there to detect motion and

---

[557] *Trials of War Criminals: Before the Nuremberg Military Tribunals under Control Council Law, No. 10. Vol. I, The Medical Case.* U.S. Government Printing Office. 1946-49, p. 719-20.
[558] "Hitler and the Birth of Modern Interpreting" 29 August 2016 https://www.executivelinguist.com/hitler-and-the-birth-of-modern-interpreting/

orientation, is sensitive enough to pick up acoustic vibrations and therefore can eavesdrop on conversations."[559]

Tech companies and research institutes Google, Samsung, Sony, University of Michigan, University of Wisconsin, Johnson & Johnson, HP, Inc. and international start-ups have been granted patents by the US Patent Office for both contact lens and intra-ocular surgically implanted lens devices that can perform a variety of surveillance and human tracking functions. The functions of these devices include "communicating with computers and mobile devices", "collecting biological data such as internal body temperature and blood-alcohol content", "glucose-sensing and monitoring", auto-focusing "built-in cameras... to capture photos with winking", lenses that can "store data without the need for a smartphone", "antennae that transmit and receive data as well as supply and receive electric power", lenses that allow users to "view augmented reality with a small display unit in the center of the lens that can sync up to smartphones wirelessly via the antenna", "motion sensors in the lenses" including "piezoelectric sensor (example of pressure sensor), an infrared sensor, an acceleration sensor, a gyro sensor (example of tilt sensor)", "an ocular potential measurement unit that converts eye movement into electrical power to control the smaller versions of part of a modern digital camera embedded in the lens", and "features such as autofocus, automatic exposure adjustment, aperture controls, adjustable zoom, and playback."[560] Histories of such devices and implants being placed on and inside individuals without their consent have been recorded for decades. (find citation)

Ali A. Zainalabdeen, medical doctor and Ph.D. in neurology, represented the Turkmen Rescue Foundation (TRF) at a 2016 State Department conference on the threats to religious and ethnic minorities under the Islamic State where he spoke briefly about widespread undiagnosed pulmonary and neurological conditions suffered by patients in Iraq under the Islamic State.[561] In my own research over a decade, I have heard many accounts from Iraqi refugees attesting to similar conditions, including sudden total paralyses that were experienced in Iraq under US occupation pre-ISIS.

Yale University researchers reported in *The Guardian* in a 2014 article titled "Female Refugees from Syria 'Blighted by Gynaecological Illness and Stress'" that:

> [One interviewee said] **'Anger has spread** …I feel like I need a psychiatrist. I've been beating my child abnormally, and when he sleeps I regret it and cry, yet the next day I get tense and beat him again.'... **These women often reported gynecological problems, including severe pelvic pain and menstrual irregularity** among those who were not pregnant... Seventy-three women had been pregnant at some point during the conflict and **just under half had delivered**, the study says. **Among the completed pregnancies, just under a quarter (23.7%) had been pre-term births, four had been miscarriages or induced abortions (10.5%) and one baby died. There were complications in over a third (36.8%), of which the most common was hemorrhage. Of those currently pregnant,**

---

[559] Schneier, Bruce. *Click Here to Kill Everybody*, 29.

[560] Guzman, Genevieve de. ""Smart" Contact Lenses: Spy Gadget or Formidable Threat to Privacy?". *The Richmond Journal of Law and Technology.* University of Richmond School of Law. 16 January 2017.

[561] Berkeley Center for Religion, Peace & World Affairs. "Threats to Religious and Ethnic Minorities under the Islamic State". Conference held at Georgetown University. 28 July 2016.

> **over a third (39.5%) of them reported problems such as abnormal weakness and tiredness, severe abdominal pain, bleeding and fever**.[562] ; "In addition to poor reproductive health outcomes, many women rated their health as poor and this was statistically significantly associated with exposure to violence when mediated by stress. Many reported having chronic illnesses, including anemia and hypertension, which may be related to complications surrounding pregnancy and delivery. Food insecurity, identified among more than half of respondents, may be contributing to menstrual irregularity or to increased anemia… Multivariate analyses revealed significant positive associations between exposure to conflict violence and gynecologic conditions (menstrual irregularity, severe pelvic pain, and RTIs [reproductive tract infections]), which is consistent with existing literature in both refugee and non-refugee populations… Many women reported health conditions potentially related to stress, including: nerve issues, depression, unusual pain and fatigue, loss of appetite or sleep, repeated vomiting, and migraines."[563]

The Atlantic staff writer Joe Pinsker notes similar effects on reproduction that the COVID-19 pandemic has had in the US in less than nine months:

> **These missing births, which could end up numbering in the hundreds of thousands in the U.S., will make up what's been called the 'COVID baby bust.'** One would think that a **baby bust would take at least nine months to reveal itself, but traces of one seem to have already appeared.** As Philip Cohen, a sociologist at the University of Maryland, has noted, **births started to decline in California and Florida during the summer**. **That'd be too soon, though, to reflect a drop in conceptions during the pandemic, or a rise in abortions or miscarriages (which tend to happen earlier on in pregnancy).** Three possible explanations, Cohen told me, are errors or lags in states' data on births, large numbers of pregnant people moving during the pandemic and giving birth in another state, or a large, unexpected drop-off in births that was already going to happen regardless of the pandemic. The first is probably incorrect—California's public-health department told me that it wasn't aware of any delays in reporting data (and Florida's didn't respond). The second is possible, but a little hard to believe. Cohen thinks the third is likeliest. 'It might actually be that we were already heading for a record drop in births this year,' he said. **'If that's the case, then birth rates in 2021 are probably going to be even more shockingly low.'** … The resulting decline in births, whenever it kicks in, could be quite large. In June, the economists Melissa Kearney and Phillip Levine **projected that 300,000 to 500,000 fewer babies might be born in 2021 than there would have been otherwise.** 'We see no reason to think that our estimate was too large at this point,' Kearney told me five months after the analysis was published. 'In fact, **given the ongoing stress for current parents associated with school closures, the effect might even be larger than what we predicted**.' Kearney and Levine's estimate is based in part on the declines in birth rates that occurred as a result of past crises, such as the 1918–19 influenza pandemic and, more recently, the Great Recession. But as the two economists note, the coronavirus pandemic is a departure from historical precedents. The influenza pandemic wasn't an economic crisis and the Great Recession wasn't a public-health crisis, so it might be difficult to accurately predict the effects of a

---

[562] Boseley, Sarah. "Female refugees from Syria 'blighted by gynaecological illness and stress'". *The Guardian*. 19 February 2014.

[563] Reese Masterson, A., Usta, J., Gupta, J. et al. "Assessment of reproductive health and violence against women among displaced Syrians in Lebanon". *BMC Women's Health 14, 25* (2014). https://doi.org/10.1186/1472-6874-14-25.

> disaster that mixes elements of both… **It's not just that fewer babies will be born—it's also that different babies will likely be born, to different parents**. As I wrote in July, **white parents and parents with more resources might be better able** to go through with their pre-pandemic childbirth plans **than parents of color and parents with fewer resources**, such as those who have lost earnings or jobs during the pandemic.[564]

Sociologist and research fellow Malka Older writes in "Satellite Surveillance Can Trace Atrocities but Not Stop Them" on the divisive issue of SAR use in human rights applications:

> I reached out to Nathaniel Raymond, the director of operations of the initiative mentioned in those articles, the Satellite Sentinel Project (SSP). A collaboration among a number of organizations and housed at the Harvard Humanitarian Initiative, SSP was largely funded by Not on Our Watch, the organization started by Clooney along with some of his *Ocean's Eleven* co-stars. SSP has now closed, and the Clooneys have shifted focus to the Sentry project, which follows money rather than armed movement in satellite photos, but Raymond believes that in today's data-intensive world, the work of SSP is more relevant than ever. SSP went a step further than previous efforts to document mass killings, seeking to identify the indicators needed to predict them so that information could be shared before they happened. As Raymond told me by phone, "We went into SSP believing we could standardize the observable patterns that would happen in certain kinds of atrocities and create a new forensics." This is possible because, as Raymond explained, "there's a logistical ground pattern required to kill a lot of people." It was a chilling reminder of just how systematic such atrocities are. And in today's world, the prepositioning of troops and equipment necessary **for a massacre is not only predictable; it's also "entirely visible from space."** SSP was largely successful in its predictive goals. The Harvard Humanitarian Initiative's report on the pilot phase of the project makes for grim but impressive reading about large-scale violence that was predicted before it happened, recorded in almost real time as it occurred, and further documented as the perpetrators, to varying degrees, attempted to conceal it. The analysis was accurate and prescient enough that the report quotes Rebecca Hamilton, a former special correspondent for the *Washington Post* in Sudan and a fellow at the Pulitzer Center on Crisis Reporting, as calling the attack on Abyei 'perhaps the most clearly forecast crisis in history.'… In a 2016 dissertation paper studying Amnesty International's Eyes on Darfur project, Grant Gordon found that "**Amnesty's advocacy effort was associated with between a 15 and 20 percentage point increase in violence in monitored areas.""**[565]

In *Violence and Intervention,* dissertation by Grant Gordon, Gordon writes: "the most violent conflicts in Africa, I show that regime elites withhold payments in order to distinguish loyalty and evidence that this screening strategy drives high levels of civilian abuse. In the second essay, I assess the impact of "Eyes on Darfur", **the first-ever satellite intervention implemented by Amnesty International USA amidst a brutal genocide with the objective of reducing violence. Using a high-frequency, sub-national dataset on genocidal violence, I show that this intervention resulted in pernicious and persistent effects: monitored areas experienced**

---

[564] Pinsker, Joe. "Here Come the COVID-19 Baby Bust". *The Atlantic*. 24 November 2020.
[565] https://foreignpolicy.com/2020/01/21/sudan-clooney-satellite-surveillance-can-trace-atrocities-but-not-stop-them/

increases in violence during the program as well as in subsequent years, as did neighboring areas."(p 1)]

On pandemic response increased surveillance and contact tracing: "On Monday, the F.B.I. released preliminary statistics showing a major increase in murder last year [2020]… cities of all sizes reported increases of greater than 20 percent… Although it's not clear what has caused the spike in murder, some possibilities are the various stresses of the pandemic".[566]

[re: radiation illness and radiation 'madness' from electronic weaponry, re: **Nasser** quote from **Tahrir Square in 1953** that, "The enemy is now fighting us with money, **hostile propaganda and the agitation of minds**."[567]]

+ADD Syrian representative in leaked discussion with John Kerry ~"atrocities in Syria well documented by drones, satellites, cameras, etc, no more proof needed"[568]

Matossian article: "Known as *la Grande Peu*, this episode might have been forgotten had it not been an important precipitating event in the French Revolution… in what one contemporary observer called a strange state of 'patriotic drunkenness'…The clues are buried in eighteenth-century French provincial records, which show that many French citizens suffered from a form of poisoning in 1789, the result of eating bad bread. The same records also mention that in the region… many women miscarried… one Dr. Geoffrey chronicled a marked deterioration in public health in the second half of July 1789, reporting that jaundice, diarrhea, and nervous attacks were common, especially among women… Geoffrey attributed all of these symptoms to the consumption of 'bad flour' and reported that all were relieved by a change to 'better bread'. Two Paris physicians also chronicled an increase in illness, especially nervous diseases in the second half of July. When their patients many of the pregnant women, suffered 'apoplexies, paralysis, anxiety, fear, visceral upset, depression, slow fevers, and erysipelas,' these doctors, like Geoffrey, suspected that 'bad bread' might be to blame… in July 1789 the rye crop was 'prodigiously' affected by ergot, the sclerotium, or hard phase, in the life cycle of a fungus… During the Middle Ages, writers described dozens of epidemics of what they generally called 'holy fire,' now believed to be ergot poisoning… it appears then, that the role of ergot was to create a suggestible state of mind and to distort perceptions in its victims, while political and cultural factors determined the precise nature of the interpretations that victims places upon their symptoms."[569]

"'I want to rape his anus,' Topiary replied. 'Raping' servers was a typical way to describe a hack into its network," writes Olson.[570] But this is not necessarily the only interpretation of this phrase in cyber technology. With access to directed energy weapons, hackers can very well cause damage to internal organs and bodily members of targeted victims. These physiological assaults

---

[566] Asher, Jeff. "US Murder Rate Remains Elevated as New Reporting System Begins". *The New York Times*. 16 March 2021.
[567] James, Laura. "Whose Voice? Nasser, the Arabs, and 'Sawt al-Arab' Radio". *Arab Media and Society.* Kamal Adham Center for Television and Digital Journalism of The American University in Cairo. 1 June 2006.
[568] https://www.youtube.com/watch?v=e4phB-_pXDM&feature=youtu.be ~9:00
[569] Matossian, Mary Kilbourne. "The Time of the Great Fear". *Sciences,* 38-41. New York Academy of Sciences. 1984, p. 39-41.
[570] Olsen. *We Are Anonymous,* p. 17.

are described by US-Europe Joint Investigation Team members in the interpretation of Rome Statue Article 7, g, as previously detailed in section The Hacker's Arsenal.

The use of electronic weaponry by the US military throughout its occupations of Iraq and Afghanistan is confirmed in a *Breaking Defense* article which states that US Cyber Command is the center of electronic warfare capabilities, as "the Army disbanded its electronic warfare corps after the Cold War." The article goes on to confirm that the Army "recreated some EW capability for Afghanistan and Iraq" which it says was "narrowly focused on jamming radio-controlled roadside bombs (RCIEDS), was chronically undermanned and overstressed and got cut back after the Iraq pullout."[571]

ISIS, another organized crime group led publicly by released prisoners of the US, who recruit online, gained access to US weaponry in Iraq. (ADD NIC prediction about profliferation of EW to terrorists and attack on CENTCOM, IEDs as ecoterrorism tool)

Many of these capabilities resemble traditional ideas of possession in which a person's senses are overpowered by another. This is likely the reason behind Anonymous' choice of slogan "We are Legion" (a biblical reference to the name given by demons possessing a man in the *Book of Matthew*), an indication that the online group was founded to be equipped with neuro-electronic weaponry.

By General Raymond Thomas', commander of U.S. Special Operations Command (USSOCOM), own confession, warfare in Syria and Iraq is of an electronic nature:

> Right now in Syria we are operating in the most aggressive EW environment on the planet from our adversaries… They are testing us every day, knocking our communications down, disabling our EC-130s, etcetera.

He did not specify which country was responsible for the aggressive use of electronic weaponry.[572]

Daniel Steed in *The Politics and Technology of Cyberspace* writes: "As a result of the inability to resolve the Russian intervention on any side, the stalemate in Ukraine has actually provided Russia with a more valuable use for such an ambiguous situation, 'using the country as a cyberwar testing ground – a laboratory for perfecting new forms of global online combat… The ability to be able to carry out such an e

xtended campaign of experimentation unchallenged also highlights a dual purpose that is rightly established by [Thomas] Rid; they are also testing the edges of what the international community will tolerate. 'Russian hackers are testing our red lines, what they can get away with… **You push and see if you're pushed back. If not, you try the next step.'** The push back did not come, and that next step was not slow in coming."[573] ; GREENBERG "How an Entire Nation Became Russia's Test Lab for Cyberwar" https://www.wired.com/story/russian-hackers-attack-ukraine/

---

[571] Freedberg, Sydney J., Jr. "Can Army Afford The Electronic Warfare Force It Wants?" *Breaking Defense*. 19 November 2018.

[572] Brimelow, Ben. "Syria Is Now 'The Most Aggressive Electronic Warfare Environment On The Planet,' SOCOM Says". *Task and Purpose.* 26 April 2018.

[573] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 44-45.

+ADD emailed articles on Orange Revolution

"In 2007, over the course of 22 days a Russian attack on Estonia took out commercial and government servers with distributed denial of service attacks; not just public websites but also what one report called 'more vital targets, such as online banking **and the Domain Name System,' without which people can't find or look up websites and online servers**."[574]

A Kafkaesque Answer To An Orwellian Problem

Withdrawing from the tragic spectacle, as they see it, of the Cosmic spheres.
Plotinus, *Enneads, II (The Case Against the Gnostics), 9, 13*

[SECTION TOPIC - The unincorporated Satellite Empire as cause of the end of US empire/global hegemon, and the United States becoming a failed state]

The natural solution to the existence of an essential but unincorporated warfaring 'satellite empire' to a centralized empire is twofold. First, low-level accountability and individual case resolution according to existing legal judgements would be necessary. Second, at the national level the centralized government would need to make necessary reforms to bureaucratize and administrate the 'satellite empire' - crossing the Augustan threshold by integrating the expanding periphery into the bureaucracy functions of the center. This has failed to occur on either level. Because of this, individual injustices continue to prevail, and the government's center ensures delegitimization and risks collapse.

+ADD "When utilising music for torture the legislative distance orchestrated by the U.S. military from its own country's legal system is instructive, as are the attempts to camouflage such procedural transgressions. From an interview conducted with a member of the U.S. military's sonic torture squads named C.J. Grisham, Jonathan Pieslak presents us with information pertaining to the notion that the American military respected the Geneva Conventions. He writes, "Grisham also said that he made a tape of babies crying; detainees usually answered questions after a half hour. He explained, however, that interrogators could not be reckless in their choice of sounds, because they were required by law to listen along with the detainee" (2009: 88). Later in the same passage the same soldier is quoted as saying "You are not allowed to do anything to the enemy, by law, that you wouldn't do yourself ... We can't treat them any worse than we treat ourselves ... We had to sit there for hours listening to babies crying, but we know what the purpose of this is, so it doesn't really get (on) our nerves as much and we can tune it out" (Pieslak, 2009: 88). **The suggestion that torture practices in Guantanamo abided by occidental mandates of legal procedure seems disingenuous and specious at best, and contemptuous and laughably cruel at worst.** Since Pieslak's book is written from the perspective of U.S. soldiers who served in Iraq and concerns their musical inclinations, rituals, and productions, it is not surprising that the overall tones of the text are defensive and sympathetic. As critically dubious as the aforementioned body of research sounds, it does inadvertently bring to the fore some interesting questions in relation to those who conduct sonic torture and how they themselves, listen. In the Guantanamo cells, a soldier's soundscape is composed of a mix of disconcerting tracks of anger, resentment, alienation, pain, and confusion. One would think that being enveloped in such sonic loops of recusant feedback would, over

[574] https://spectrum.ieee.org/podcast/telecom/security/is-cyberwar-war

time, have detrimental effects on those employed to exist within them. For army personnel, being informed as to how sound is to be harnessed, to what ends, and when transmissions will be activated and terminated is of no little significance. **Being in the receipt of such knowledge locates those amplifying sound in an acutely more cogent and authoritative position than that of the submissive detainee in relation to psychological trauma.** As further examined in the following pages, one listens, hears, and perceives differently when under intense duress as compared to another who is involved in similar activities of their own volition and with little external pressure to bear. Put simply, those at the controls of the sonic technologies (the soldiers) perceive in a privileged manner whilst they are part of a network of power relations that confirms their convictions, beliefs, and status. **There are, however, still questions pertaining to the waveformed repercussions upon those whom are sonically empowered.** One could not be human if one were not affected by what they perceive, particularly when that which they hear everyday, repetitiously consists of extreme and intense music, noise, and terror. This is not to say that we should have sympathy with those who conduct sonic torture, it **merely points to the idea that we have little conception of the oscillating potential of waveforms to inflict different degrees of damage upon both the receiver and the transmitter.** We exist within exponentially removed degrees of mixed waveforms all day, everyday, and we still only have notional ideas pertaining to the measurement of their affect; not only on humans, but also on the world we live in and everything that relates to it."[575]

As US Air Force Major Zachary Martin writes in *The Hydra: the strategic paradox of human security in Mexico* on narcotics-based clientelism, a security problem comparable to psychological and biological warfare:

"**the policy measures necessary to solve this human security problem introduce a strategic paradox that inhibits their adoption** in the US and Mexico**. Sweeping domestic policy reforms to legalize** narcotics within the US and Mexico **can end the illicit** narcotics **supply-demand dynamic fueling deficient human security.** Such reforms will **prove politically difficult to implement** within states, produce public health challenges, **and require multilateral cooperation.** More importantly, **a legalization strategy creates a duality of interests between the state and cartels over natural and man-made resources, which sets the conditions for widespread economic grievances that can stimulate an insurgency and transform a human security problem into a war.** The threat to both the US and Mexico consists of human insecurity, and the enemy consists of cartels exploiting this insecurity. Cartels exist at the substate level, primarily to maximize profits from the drug trade. They focus violence mostly against each other to expand control over a competitive illicit market and rely on corruption to undermine the state and preclude interference in their activities."[576]

+ADD *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* Marieke de Goede, Esmé Bosma, Polly Pallister-Wilkins: "Furthermore, it is well known that secrecy holds a certain allure or seduction. **It is often the researcher's expectation that there is a core of valuable truth** at the heart of the invisible or the forbidden. As Graham Jones has put it, it is **tempting to equate 'secrecy – and the difficulty of access – with the depth and authenticity of knowledge'** (2014: 61). Remote locations, shielded laboratories, concealed documents, are easily inscribed with a particular value. However, we must be mindful of what Jacques Derrida

[575] P 183-84 http://researchonline.ljmu.ac.uk/id/eprint/6092/1/543845.pdf

[576] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 2-3.

called the 'secrecy effect'. **As Derrida (1994: 254) notes, there is a certain 'value' to the secret, which he called a 'capital of the secret', that forms a basis for its authority**. In this sense, secrecy's value entails something like a 'magical reification' of the professional in possession of the secret. We now have a vibrant literature, sometimes called Secrecy Studies, which problematises the 'secrecy effect' and which shows that secrecy is more than a barrier to be overcome."[577] ;
Former CIA officers Marc Polymeropoulos and John Sipher in open letter to Biden: "Among them, **intelligence collectors face existential threats from ubiquitous surveillance. We need to devise ways to defeat 21st century technology** and allow officers to operate effectively around the world… **expect the IC to do its work in secret**. Leaks of sensitive information will not be tolerated, and **the IC should seek to stay out of the news.** Intelligence should be **a silent profession**… protecting the nation **in the shadows**, around the globe, 24/7".[578]

"Ethical dilemmas of security research are different than those in – for example – the observation of health practices or social movements. Questions of confidentiality, anonymisation and secrecy play out in difference ways in relation to qualitative immersion into security communities. As Fairlie Chappuis and Jana Krause show in this volume, the safety of researchers and their subjects requires special consideration, and has specific ethical implications."[579] ;
"Accordingly, the contributions to Part 1 probe the value of the secret itself. Studying secrecy is not strictly about uncovering the kernel of the hidden, but is about analysing the play of power and authority that secrecies enable and produce… Moreover, it is important, as researchers, to *resist* the 'magical reification' of the secret or the holder of secrets."[580] ;

"In addition, secrecy may arise less form a deliberate hiding or classification, and more from the need for specialised knowledge or expertise to decipher practices or discourses. Sometimes, the secret is kept in public. Michael Taussig coined the term 'public secret' to denote 'that which is generally known, but cannot be articulated. Often practices are not necessarily secret, but are not readily analysable for other reasons; they could be too overwhelming in volume, too distant, foreign, or too complicated to understand in the often limited time available for the research project. Accordingly, contributions to Part 2 of the book engage with the challenge of understanding the role and inner workings of complex security technologies. All kinds of security practices, from border security, to drone warfare, to 'securing with algorithms', are technology-led in ways that are opaque to researchers and practitioners alike. In what ways do technologies require specialised knowledge to design, implement, use, and understand them and what does this mean for our knowledge production about security decision-making and practices?"[581] ;

---

[577] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 5-6.
[578] "A Letter to President-elect Biden on Restoring Relations with the Intelligence Community" https://www.justsecurity.org/73287/a-letter-to-president-elect-biden-on-restoring-relations-with-the-intelligence-community/
[579] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 6.
[580] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 10.
[581] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 14.

"…'Reflexive methodologies', make dynamic encounters with secrecy a primary object of analysis. Rather than strictly seeking access… It is less focused on uncovering the kernel of the secret, than it is on analysing the mundane lifeworlds of security practices and practitioners that are powerfully structured through codes and rites of secrecy. "[582] [choppy quote – rework in paragraph]
"Researchers might experience different affective states **in relation to secrecy 'ranging from guilty excitement of penetration to intense paranoia** about the consequences of approaching or disclosing secrets'… A reflexive attitude generates awareness for the ways in which secrets shape our own knowledge production, and how out methods may affect our respondents."[583]
As profiled by Hazelwood, these varied reactions following exposure to 'secrets' (ostensibly state secrets which are done semi-illegally) fit the general profiles of the Organized Criminal and the Unorganized Criminal. The organized criminal is generally excited about even public coverage of his (or possibly, others') secret crimes, while the disorganized criminal character is prone to panic and paranoia when it comes to maintaining his (or others') secret crimes.

+ADD "And **Washington has filled this legal void with a secret executive matrix** - operated by the CIA and the clandestine Special Operations Command - that assigns names arbitrarily, without any judicial oversight, to a classified "kill list" that means silent, sudden death from the sky for terror suspects across the Muslim world. Although **US plans for space warfare remain highly classified,** it is possible to assemble the pieces of this aerospace puzzle by trawling the Pentagon's websites and finding many of the key components in technical descriptions at the Defence Advanced Research Projects Agency (DARPA)."[584]
+ADD "Satellite Surveillance Can Trace Atrocities but Not Stop Them: George Clooney's pioneering data project documented horrors in Sudan, but that wasn't enough" "But now it's 2020, and skepticism about surveillance and technology is the norm—especially in the **intersection of military intelligence and humanitarian aid.** So when I saw a tweet making the rounds—to the tune of 30,000 retweets—about **Clooney spending his hard-earned Nespresso dollars on a satellite to track Sudanese President Omar al-Bashir (now very deservedly deposed and an indicted war criminal),** I was curious to get a version of the story a little less starry-eyed than the gushy 2013 Huffington Post article screenshotted in the tweet—and to see what role this kind of outside surveillance had actually played. **In an age of ubiquitous cameras and big data, it turns out, documentation might be easy, but political action often remains as out of reach as ever… "[585]**

+ADD In my own attempts to contact CNN, their child company HLN, Amazon, Space X, Google and their child company YouTube, Twitter, Facebook, and MAXAR concerning a host of concerns about individual cyber privacy, the companies' political activities in the Arab Spring, and institutional practices concerning cyber privacy and surveillance, cyberstalking and electronic human trafficking and tracking, I have received responses from five companies:

---

[582] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 14.
[583] de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020, p. 14.
[584] https://www.aljazeera.com/indepth/opinion/2012/11/201211912435170883.html
[585] https://foreignpolicy.com/2020/01/21/sudan-clooney-satellite-surveillance-can-trace-atrocities-but-not-stop-them/

Amazon denied such activities were permissible under policy but conceded that their cloud computing service could be misused to invade another's privacy or suveil without Amazon's oversight or willingness to intervene; Google writes "to not expect a response beyond this email" to public inquiries if Google deems the one inquiring "not a member of the press"; YouTube refused to respond to an inquiry into legality from a non-litigator; Twitter does not respond to any emails and will only respond through their own platform; and Facebook refers those who "are not members of the press" to their troubleshooting links for profile accounts. Being new members of the press/media themselves, it is not only ironic that these companies adhere to a traditional definition of 'press', but limiting inquiries to members of the media eliminates all possibility of outside inquiry and research into the media.

Even in related queries to the press, I have received responses less responsive than those made to government departments known for secrecy. In a query made on a non-condemnatory *New York Times* seven year-old article on targeted assassinations of child "al-Qaeda terrorists" by the Obama Administration[586], I was told by *New York Times* correspondent Scott Shane that the identity of the Obama Administration officials that witnessed the approval of murders of Afghan and Pakistani children alleged to be al-Qaeda members would not be revealed upon request by *The New York Times* because it is, in his words, "classified stuff". Of course no one in the professional field of Middle East Studies is impressed by such a designation nor convinced that anyone at *The New York Times* constitutionally holds security clearance beyond an entrance pass to an official press room. This journalist followed up the request denial by sending an email seven hours later informing me that he would be retiring as correspondent from *The New York Times*.

I impress that the US media alleges it has and maintains classified US government secrets on the targeted murders of children abroad by the US government. Members of the US media refuse Ph.D. researchers in the field access to that information and, even more bizarrely, declare their official career retirement from journalism to inquirers within hours of receiving inquiries, despite that newspaper having revealed that information unsolicited almost ten years earlier.

Who, then, presses the press for answers? All considered, I can see how it would not be desirable to these companies to have their deeds questioned and detailed in another's work with no path of recourse if the perspective were not in their favor.

+ADD Contacted the toll-free Army Recruiting by phone. Asked for connecting number to Army Futures Command in Austin, Texas on LaVaca Street. When I called the number, I was connected to a city council office phone for the city of Port LaVaca, Texas. When I called Army Recruiting back, I was given a second number that connected me to an apartment leasing complex. In my third conversation with Army Recruiting, I was informed that I was contacting a contractor, not a military office. When I asked the name of the contractor, the employee hung up the phone before answering.

---

[586] https://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html

This piqued my interest, so I looked up the largest corporate military recruiting company I knew of, GoArmy.com, in Reuters company profiles. I found no listing. I also found no corporate page or corporate statement for the .com. I contacted GoArmy.com using their chat feature on the goarmy.com webpage. I was told by the correspondent that he/she was not aware of any other name the company used. He/she also recommended I contact the same Army Recruiting number which earlier connected me with the city council office and the apartment leasing complex.

+ADD Contacted Air Force by online platform and by email to IG. No responses. Called Public Inquiries line to Air Force. The caller is informed that they cannot leave a message and no call will be returned. The caller is redirected to the webpage (not of use in a computer hacking situation) and instructed to send an email.

I have contacted USCYBERCOM (US Cyber Command) by phone and described the effects of these electronic weapons, and inquired as to whether USCYBERCOM could trace or prevent the misuse of electronic weaponry within the United States by persons with clearances or who gain access to another's clearance. From the representative's response, I was able to confirm that the weapons can indeed be used in the United States against citizens. The only situation in which USCYBERCOM would intervene is if the misuser or hacker is military personnel who can be identified by name and branch of the Armed Forces by the person filing the complaint.

In reality, no one needs to be able to provide name and rank of misusers - a citizen target does not take soldiers as prisoners of war in reporting system abuses, and a victim cannot demand these answers from a remote attacker. These weapons and their deployments are extremely well tracked in what Raytheon, a major US cyber weapons manufacturer, advertises as "real time feeds" to commanders through software and servers recording the weapon operators' "digital footprint". The military and its contractors should already have very defined process for reporting such crimes; as Staff Sgt. David Delgado, a former electronic warfare technician with the U.S. Navy, said in 2018, "Electronic warfare isn't new."[587]

"The **Draft Protocol Concerning Non-Detectable Fragments**, initialed by 81 countries during the 1978-80 UN Disarmament Conference, is perhaps the shortest arms-control agreement ever concluded, reading, **'It is prohibited to use any weapon the primary effect of which is to injure by fragments which in the human body escape detection by X-rays.'**"[588]

+ ADD below quotes "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

---

[587] Higgins, John. "Raven Claw Augments Battle Management for Electronic Warfare Operations". *Army webpage*. 22 January 2018.

[588] Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 421.

> The question becomes more problematic when dealing with the conduct of a private entity, which is part of an industry that is heavily regulated by the government (Skinner v. Railway Labor Executives Association, 1989). Although the Fourth Amendment does not protect against a private party acting on its own initiative, it does protect against searches and seizures by industrial entities when they are acting as instruments or agents of the government. In determining whether an entity is acting as an agent of the federal government (thus bound by the Fourth Amendment), the Court considers the circumstances particular to the situation such as the degree of the government's regulation in the industry's activities. When government participation in the private industry is high, the Court considers the private entity to be an instrument of the government, and thus subject to the requirements of the Fourth Amendment. Railroads, for example, appear to be instruments of the government because they are heavily regulated. In *Skinner*, the Court held that railroads were in fact instruments of the government. In this case, a federal regulation required railroads to administer breath and urine tests to employees who violated particular safety rules. The Court concluded that when a railroad administers the tests in accordance with regulation, it does so "by compulsion of sovereign authority," namely as an agent of the government. Accordingly, the Court found that "the lawfulness of its [the railroad's] acts is controlled by the Fourth Amendment."[589]

"…surely the Government may not exceed the scope of the private search unless is has the right to make an independent search….A partial invasion of privacy cannot automatically justify a total invasion." P. 42

"In Katz v. United States (1967), federal agents placed a listening device on the outside wall of a public telephone booth to listen to the defendant's conversation. Following common law trespass doctrine, the Ninth Circuit held that because there was no actual penetration of the booth, there was no trespass, and therefore no search. The Court reversed, ruling that because the Fourth Amendment 'protects people, not places,' it no longer made sense to rely on the antiquated property law concept of trespass." P. 45

"…we are in the midst of a revolution in intellectual technology that is changing the way we think, communicate, do business, and live our private lives. In the span of three decades we have seen the invention of personal computers, the development of the internet, the routine use of e-mail, the proliferation of cell phones and personal data assistants, an explosion of audio and video technology, and a hundred other technologies undreamed of by our parents. These make the fourth amendment's reference to 'papers, and effects' seem quaint by comparison. Our spheres of private activity have spread outward in all directions. At the same time, law enforcement agencies have begun to employ these new tools and media. They no longer need to rely on the unaided human faculties of the peeping Tom and the eavesdropper. They are capable

---

[589] Bloom, Robert M. *Searches, Seizures, and Warrants: A Reference Guide to the United States Constitution.* Westport, Connecticut: Praeger, 2003, p. 41.

of spectacularly intrusive invasions…The third [reason] is the internationalization of public and private life that has come about in the same period of time and for some of the same reasons. To an unprecedented extent our ideas and culture, friends and business partners, cross borders and oceans." P. xiv

"In *Mapp v. Ohio*, 367 U.S. 643 (1961), the Supreme Court held that evidence seized by searches and seizures in violation of the fourth amendment is inadmissible in criminal trials in state courts." This also applies to derivative evidence, the "'fruit of the poisonous tree'. Derivative evidence may be admitted if it is sufficiently attenuated, if it has an independent source, if it would inevitably have been discovered, and so on." P. xv

"In *Kyllo* [v. United States, 2001], a case involving thermal imaging information emanating from a home, Scalia, writing for the majority, held that the applicability of the Fourth Amendment turned on what he perceived to be the original meaning of amendment, which drew a 'firm line at the entrance of the home' (Payton b. New York, 1980)… In a 5-4 decision written by Justice Scalia, the Court determined that there was indeed an expectation of privacy in the heat emanating from a home and the Fourth Amendment was therefore applicable. He characterized the issue in terms of the limits that should be place on emerging technology in order to preserve our privacy rights." P. 15, 52-53 – add UTILIZATION OF HISTORY IN RECENT CASES – ORIGINAL INTENT on same page to 'reasonableness' points

+ "More recently Justice Antonin Scalia observed [on the Fourth Amendment] 'inconsistent jurisprudence that has been with us for years' (California v. Acevedo, 1991)." P. 3

[RE-WORD] This is to say that the purposeful neglect of reporting security concerns and breaches constitutes criminal negligence by all involved in the electronic warfare operation industry. That these misusers are working under State regulation, the State is de facto willing to assume criminal liability for the misuse of electronic weaponry by refusing to take misconduct reports and prosecute breaches.

Despite the Pentagon's insistence on telling fairy tales to the public, aliens cannot assume criminal liability for the misuse of State regulated weaponry.[590] RAND's Robert Specht wrote an early indication that Air Force and RAND technicians planned by 1957 to cover their electronic weaponry operations with fictional narratives, saying, "Another type of war game – and one favored by writers of science fiction – is the game played on a high-speed computer."[591] The government giving credence to this public tale is disturbing within the context of past civilizations, which had despotic rulers who attempted to present themselves as otherworldly demigods with supernatural abilities, or as divinely ordained people with access to superhuman powers, in order to tyrannize their subjects.

"Some of the larger empires lasted a long time because, instead of disintegrating in civil wars, they crossed the Augustan threshold. Where the periphery was large relative to the resources of

[590] Watkins, Eli and Brian Todd. "Former Pentagon UFO official: 'We may not be alone'". *CNN*. 19 December 2017. https://www.cnn.com/2017/12/18/politics/luis-elizondo-ufo-pentagon/index.html

[591] Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957.

the metropole, empires persisted only if they were able to develop a polity that governed for the sake of the empire as a whole… Empire continues to attract as a road to peace, but imperialism holds a double tragedy. First, modern empires, resting upon metropolitan ethnic nationalism, may not be able to travel the whole way to integration. Second, any extensive empire, to survive long enough for integration to occur, must cross the Augustan threshold to imperial bureaucratic rule – and bureaucratizing the metropole destroys participatory government. Liberty and empire emerge, both analytically and historically, as opposites, for the periphery from the beginning and for the metropole in the end."[592]

The only way for the State to avoid eventual prosecution is to negate its own authority and dismantle its own processes - to cross the Augustan threshold in futility, - which policy-wise may explain the US' choice of extrajudicial methods of punishment, restating the need for the stateless measures all over again. These are extremely complex and nearly impossible policy and governance situations that are being determined and managed (and of course, worsened) by weapons technicians. The desperate policymakers whose hidden short-sighted policies bore this situation can only be described as self-serving saboteurs.

This is echoed in Vahakn Dadrian's book *Warrant for Genocide*: "the Ottoman Empire's notorious nationalities problem began to deteriorate and assume once more the general character of chronic nationality conflict. The 1912 Balkan War was the climax of a series of disasters that ensued the further aggravated the woes of the empire. The human, territorial, and materials losses, not to speak of the attendant massive trauma engulfing the Turkish nation and the Ittihadist rulers (party of the Young Turks), were phenomena that still haunt the memories of many Turks. Paradoxically, however, instead of undertaking policy modifications regarding the culminative grievances of the residual nationalities and minorities of the truncated empire, the Ittihadist rulers became even more hardened in this respect."[593]

As contingency planners, I would postulate that such minds and technicians have 'a separate peace' exit strategy which is also hidden from regular policy decision-making processes, which would have been heavily invested in financially and reputation-wise already, à la Herman Kahn's Cold War doomsday scenarios, furthering still the State's motives for taking stateless measures.

Genocides are by legal definition systematic. In the absence of a nation-state, where there is genocide occurring not attributed a state system, some system must be responsible for systematizing the events. In this essay, I have presented many facts that suggest that technology systems have regularly supplemented genocides by states in the past, and may be up to the 'auto-pilot' level of conducting genocides with relatively little apparent state involvement. I agree with author Dadrian that any such change is done to obfuscate reality of conspiracy to genocide between human planners and systematization. [REWORD, repeated – on Satellite Empire in genocidal designs, especially in failed states]

---

[592] Doyle, Michael W. *Empires.* Ithaca, NY: Cornell University Press. 1986, p. 137.
[593] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 2.

"The Intricate Relationship between Acts of Conspiracy and Genocidal Designs"
Warrant for Genocide by Dadrian:

> One of the "essential features in the conception, design, and implementation" of the Ittihadist Young Turk genocide of Armenians during World War I was "the maintenance of the utmost secrecy of the scheme, to be safeguarded by camouflage and deflection. In other words, the leadership of Ittihad is revealed here as having engaged in careful deliberations leading to the adoption of a radical policy for the resolution of a historically lingering nationality conflict."… "The picture that emerges from these party congress is the dual-track performance of Ittihad. On the one hand there is the formulation of a platform outlining a party program that is intended strictly for public consumption. On the other hand, there is the clandestine parring of a sketchy plan that is ominous and undoubtedly sinister in nature, and is, therefore, kept secret from the public, even from the regular organs of the government, and from the lower echelons of the party leadership and naturally from rank and file. The former act is belied by the latter as the main purpose of the duality of such role performance is to conceal and/or deflect from the essential and high priority objectives of the top leadership of the party. The principal aim is to confound the outsiders by surreptitiously combining overt and covert methods of operations.[594]
>
> Several Turkish authors, historians, political scientists, and biographers, did recognize this secretive modus operandi of Ittihad as its trademark, as far as the attainment of questionable goals and its reliance on lethal violence were concerned. Tevfik Cavdar, the biographer of Ittihad party boss Talat, explicitly admitted to 'the dual character of the organization' of Ittihad party whose 'secret nature was nurtured and explored through a separate organizational component. The entire body exactly resembled an iceberg comprising visible and invisible parts.'
>
> Speaking of Talat as the party boss, Cavdar declared that he knew how to exploit the potential of that secret component of the party by way of 'readily sliding in the position of man launching illegal undertakings.' Sina Askin, a historian and an expert on Ittihad, pointed out that the party's 'secrecy was meant to cover the discrepancy between its program of Ottomanization and its application of a program of Turkism. Moreover, the resort to secrecy was probably due to the mentality of an organization which did not recoil from murdering people in pursuit of its political goals. For his part Tarik Z. Tunaya, the late dean of Turkish political scientists, declared: 'Ittihad was a power-wielding monopolistic clique which issued orders from behind the curtains…the great Empire was in the hands of these eight individuals…operating secretly and in an organized way behind a mysterious curtain…a secret oligarchy which resorted to weapons whenever it could not silence ideas.'
>
> The most salient feature of this almost pervasive secretiveness of Ittihad was the extension of that secretiveness to the regular organs of the Ottoman state organization, organs which were not directly identified with the party apparatus and as such were treated as alien elements. This is exactly the modus operandi Talat had projected in the above mentioned pre-Congress conclave of top Ittihadist leaders in Saloniki in August 1910. He stated that the goals of the party, especially with respect to the provinces, could not be attained unless the provincial officials of the government were kept 'in ignorance'. This is an attitude in which lethal schemes of conspiracy can readily germinate, including the scheme of organizing the mass

[594] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 100.

murder of a targeted population group; the actualization of such a scheme all but may become contingent upon the onset of propitious opportunities.[595]

On the topic of electronic warfare, Herman Kahn wrote in his 1958 book *On Thermonuclear War* in the chapter titled "Stresses and Strains: Planning for a Complicated World" the following:

> Just because violations of certain kinds of bans can be detected does not mean that we could enter into such an agreement and then tailor our defense establishment around the existence of the ban. We must always ask, 'What would happen if it [a ban] is violated?' Would we then be in a position to take corrective action or to stand pat, or would we be completely defenseless (either at the time of the violation or later)? ...
> It would be rather easy in the case of a democratic society to enforce a ban on large-scale manufacture of new and complicated weapons. This would be especially true where the nation allowed free movement of inspectors and access to people and places. In the case of a totalitarian society, it is doubtful that such a ban could be enforced, unless clandestine intelligence came to the rescue. This would especially be true if the totalitarian government allowed only very limited inspection at fixed times and places and if in addition could discipline its own citizens. The official system could then only hope to control the rate at which these weapons entered service.
>
> The next area to consider is the deployment of weapons. If aerial or ground observation is allowed, an absolute ban should be relatively easy to police**. If an appreciable number of weapons are present it should be a relatively easy matter to find at least one of these weapons and, if a single weapon is found in the banned area, a violation has occurred. If the ban is not absolute, but on some quantity, it may be difficult to distinguish** whether there are *n* or *n* + *m* weapons in the area. However, **it is not essential to have an absolute ban if the Arms Control Commission is informed of the location and status of every weapon in the area, and if this information can be frequently and readily checked. In that case it would still be true, most of the time, that a single discovery of an unauthorized weapon meant a deliberate violation.**
>
> Control of the deployment of weapons is most likely to be useful in specialized circumstances, as a supplement or addition to existing defense arrangements. The deployment of weapons could be limited in order to reduce the possibility of surprise attack, false alarms, accidental war, creation of tense situations, and so forth.
>
> Control over the deployment of weapons is often advocated as a method of reducing international tension…[but] the 'reach' of modern weapons is such that withdrawals of from 50 to 100 miles, or even many hundreds of miles, can be meaningless from a tactical or strategic point of view. This meaninglessness is likely to be realized soon after the agreement is put into effect...
>
> ...Very closely related to the control of deployment would be limits on operational practices. These, too, can be relatively easily monitored if frequent inspection procedures are allowed, because the detection of a single aberration would mean a violation…
>
> **Some of the most useful arms control measures on operation and deployment are those designed to reduce the probability of accidental war, fatal human error, or**

[595] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 1; 100-101.

> **miscalculations. This could be done by not having forces on super-alert, by restricting operations on both sides to reduce the rate at which false alarms might be generated, by the banning of any peacetime practices that could be used to mask a surprise attack, and so on.[596]**
>
> Reference war games in 2020 and 2023 again[597]

It is unclear whether the job of US analyst attracts individuals with dissociative personality disorders or whether such conditions develop over time, but it is clear that these individuals are completely capable of calling such plots a game, conducting the actual wars, and excusing it to themselves and others as all just a scenario.. ; *Soldiers of Reason* game theory bookmarks - meant as elaborate lessons, Kahn states they are used to "mask a surprise attack".

+ADD Arms Trade figures article, Space Force bullshit:
[TOPIC – Arms trade, proxy wars as strategic economic decisions by RAND]
"For these reasons, we propose using an **alternative model** that more effectively explains the dynamism to Iranian strategy and **how it fosters nascent proxy relationships**. **A market entry and investment model** frames Iranian activity as if it were a firm seeking market expansion. **In applying this model, we treat countries as if they were potential markets,** where Iran explores opportunities, screens partners, and ultimately invests in relationships. In exploring markets, **relevant factors are the level of strategic value, the extent to which there are accessible or open conditions (such as a weak state with porous borders), and the degree of latent demand (such as a disgruntled Shia population)**… In Chapter Three we apply this theoretical framework to the case of Lebanon, Iraq, and the Persian Gulf in greater depth, describing Iran's **past efforts to cultivate proxies using the market entry and investment model.** Turning specifically to Yemen, **Stage 1 of the market entry and investment model is to explore opportunities. The proxy market in Yemen was opened wide after 2011, with the near collapse of the government** and **increased demand** by the Houthis' **rapid political and military expansion**. **Weak national control** and **robust smuggling routes** created permissive conditions for Iran to push materiel support into Yemen without high risk or cost. The appeal of this market also increased given heightened Iranian-Saudi tensions and with Saudi intervention in Yemen providing an opportunity for Iran to exact high costs on the Saudi military through proxy conflict with low risk of direct confrontation. Although the focus is often on Iranian support to the Houthis, Iran has **also looked to screen and select a number of proxies** in Yemen, **Stage 2 of the market entry and investment model.** There are natural impediments to the Houthi-Iran partnership, such as differences in the form of Shiism that they practice. Prior to 2014, Iran explored relationships with other potential partners, such as the southern secessionist movement, so as to diversify its portfolio of proxy reports."[598] ADD Houthi scenarios here?

---

[596] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 236-237.

[597] https://www.tomdispatch.com/blog/176429/tomgram%3A_nick_turse%2C_tomorrow%27s_terror_today/; https://theintercept.com/2017/10/22/the-u-s-will-invade-west-africa-in-2023-after-an-attack-in-new-york-according-to-pentagon-war-game/

[598] Johnston, Trevor, et al. *Could the Houthis Be the Next Hizballah? Iranian Proxy Development in Yemen and the Future of the Houthi Movement*. The RAND Corporation. 2020, p. ix-x.

"The last subject I have in Table 64 is Astronautics. From the military point of view, the importance of Space Warfare may have been overplayed. It is very easy to make the obvious Mahan analogy on 'control of the sea' and talk blithely and superficially of 'control of space.' The analogy was never really accurate even for control of the air, and at least in the sixties, it seems to be completely misleading for space… Unlike military programs, space programs are not psychological. If they do not work objectively, it is noticed. Therefore it is very likely that equipment developed for space will be reliable at least in peacetime. It is also worth saying that that despite many misleading remarks to the effect that powerful rockets are not useful for military purposes but only for space, there do seem to be many military advantages…".[599]

Holding in mind the capabilities of technology which are Clausewitz's "operational instruments" of war today, consider those realities in the context of the Information Age. A nebulus term, 'Information Age' is defined by Holocaust researcher Edwin Black when he says:

> I know there are people on the Internet right now that think they know what information technology is. And they think that the Information Age was born in Silicon Valley. Most people within listening range of my voice do *not* know what the Information Age is. *The Information Age is the individualization of statistics.* Not only can I count you as a member of the crowd, I can individualize the information I have about you. And the Information Age was invented not in Silicon Valley, but in Berlin in 1933. IBM came to the Third Reich, and said, 'We are the solutions company, and there's no solution we won't give you.' So, they said, 'I want to know where the Jews are. Who are the Jews?'[600]

To this effect, Richard A. Lindsey wrote that,

> What social media has done, or at least helped, is to weaponize information down to the individual level. Whether social media facilitates information as a weapon in the form of truth or propaganda for the revolutionary, or terrorist, again is subject to a combination of perspective and reality.[601]

When NATO stated in 2017 that, "For NATO, it is always our aim to use minimum force to achieve maximum effect and therefore cyber effects may be the best response,"[602] we should consider this in connection to the above wartime definition of the Information Age.

There are no longer justifications required for the waste of resources that would be required if traditional offensives were proposed to be taken against an individual or small group. The individualization of statistics increases the likelihood that warfare is taken against individuals and targeted populations of nearly petty proportions by major military organizations like NATO. In essence, any one antagonistic person or small group can be assessed by NATO as

---

[599] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 486.
[600] Black, Edwin. "IBM and the Holocaust". 26 February 2012. Presentation at Yeshiva University, New York, NY.
[601] Lindsey, Richard A. "What the Arab Spring Tells Us About the Future of Social Media in Revolutionary Movements". *Small Wars Journal,* 2013.
[602] O'Neill, Patrick Howell. "NATO will establish new cyber command centers". *Cyber Scoop.* 9 November 2017. Internet resource.

if they posed a threat high enough to justify NATO interest, as if any individual were a nuclear dictator to be taken out. The thought of deploying troops and military armored vehicles representing the most powerful governments in the world to confiscate a laptop or disconnect a small hacker group's server should be as embarrassing and horrifying to those organizations as it is ridiculous and terrorizing to those on the outside.

But NATO's "$3.4 billion IT and cybersecurity modernization program" along with even more budget allocated for IT administration by international troops and intelligence agents includes security measures taken against individuals and small groups. This inevitable realization brings up major international disputes on national sovereignties, legal jurisdictions, and appeals processes, just as it was vaguely 'predicted' in NIC's *Global Trends 2025*.

What is more, this trend poses an increasing threat to international security relations. As as the ability of States and non-state actors to take transborder 'kinetic' action becomes facilitated with EW and Internet proliferation, multinational policy rejoinders required in response to those transnational actions on sovereign territory have not become more facilitated. This severely diminishes governments' ability to respond and to appear reactive.

At best, NATO member countries' "however and whenever" nonchalant cyber action will result in enormous amounts of work in policy and legal responses, possibly backlogging entire government departments with documenting, classifying elements, justifying action, establishing policy positions, writing press releases, and filing and receiving complaints and lawsuits on the daily transborder military action that, under traditional capabilities, would occur once in a few years at most.

This could drive any nation into debt and governing paralysis. This includes those that choose to initiate the action and those that are repeatedly attacked. The possibility of this as an intended effect of cyber transgression should be seriously considered when choosing how to respond to unusual volumes of cyberattacks, especially under unusual circumstances.

At the individual level, citizens may recognize already that international relations change on a daily basis due to these actions and the reactions. This could prove to be devastating to the dollar economy which relies on global perception of a stable US economy with predictable government relations. The decline of the dollar was also vaguely 'predicted' in NIC's *Global Trends 2025*.

The instability that could result long term would be devastating to the US's dominance of Internet infrastructure and Internet trade, which relies on international belief in the US's fair information communication practices. Many larger countries like Russia and China are already considering building parallel Internet infrastructures apart from US infrastructure due to the US's recent reputation for unpredictable and unfair Internet industry practices. NATO's stated plan to retaliate with further cyberwarfare[603] will likely not provide less incentive to circumvent US Internet infrastructure.

---

[603] https://www.cyberscoop.com/western-allies-consider-offensive-cyber-warfare-pact-as-russia-launches-plan-for-independent-internet/

In Senator-Ted-Stevens speak, this is the equivalent of a nation having exclusive control of every major canal in the world while sponsoring piracy which forces other nations to dig their own canals, rendering one's own canals next to worthless and still overrun by brigands and militants.

"Klimburg notes that the Russian 'obsession' with foreign media and even civil society undermining their own information sphere 'shifted into high gear in the wake of the first wave of pro-democracy colour revolutions in Kyrgyzstan, Lebanon, and most notably, Ukraine.' The aforementioned fear of open access to information among the citizenry outlined in the previous chapter is the clearest dominant motivator behind China and Russia's leadership in the Cyber Sovereignty movement. Klimburg is right to insists the term 'colour revolutions' is hard to over-emphasise and that the pro-democratic movements occurring since 2010 'were profoundly frightening occurrences.' China and Russia have clearly learnt the lessons from the revolutions from the early decade and Internet Freedom, with Cyber Sovereignty the overarching strategy in preventing this history from repeating itself in either Russia or the Chinese mainland. For both China and Russia, the belief is that 'national security – read regime security – is not attainable until 'informational security' is established… For this, 'China seeks to establish a narrative wherein state power already exists in the cyber realm, but where the USA is a hegemon.' Herein lies a core weakness not only of the Cyber Sovereignty concept as a whole, but also of the stability of the 'marriage of convenience' enjoyed with Russia and any other subscriber to Cyber Sovereignty; the closeness of these relationships is 'not dependent on their ties with each other, but is defined in relation to the US.'"[604]

+ ADD "We all use the same Internet hardware and software. There is simply no way to secure US networks while at the same time leaving foreign networks open to eavesdropping and attack. There's no way to secure our phones and computers from criminals and terrorists without also securing phones and computers of those criminals and terrorists. On the generalized worldwide network that is the Internet, anything we do to secure its hardware and software secures it everywhere in the world. And everything we do to keep it insecure similarly affects the entire world."[605]

"In the immediate aftermath of the 9/11 attacks on the United States, for example, over 40 percent of American Internet users could not reach their Web site of choice to access news, and most of them switched to television for information."[606] The action taken by US congressional members to definitively end US support of Saudi attacks on Yemen, the failed efforts by the US and other nations for regime change in Venezuela, and the inability of the US to garner support domestically and internationally for a military invasion of Iran all indicate that the US is not in a condition conducive to further foreign military intervention at all.

These definitive policy changes directly contradict the stated Pentagon objectives of the early 2000s, clearly indicating *ex post facto* that it would not have been feasible for the US to pursue its war policy objectives any further in overt actions, as it was uncontestedly able to do in

---

[604] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 68.
[605] Click here p. 160-161.
[606] Bahador, Babak. *The CNN Effect in Action: How the News Media Pushed the West Toward War in Kosovo*. New York. Palgrave Macmillan. 2007, p. 6.

the early 2000s and before. This provides reason and necessity for the US to go about proxied passive-aggressive war policies under the Obama administration, as I am suggesting were taken via the Arab Spring by covert coups and wars in the Middle East.

Unconventional warfare and proxy methods towards conflict by the US military are publicly recognized options by US political leaders. Consider "the 1999 NATO war against Serbia, where Clinton, fearing public backlash over potential casualties, publicly ruled out the option of ground forces at the start of the campaign, had fighter jets fly at 15,000 feet, and did not authorize the use of Apache helicopters because of their high risk of being shot down."[607] As former Secretary of Defense Dick Cheney is quoted by *The New York Times* in September 2000 as saying:

> "I think it is important that we make sometimes difficult choices about when we're going to actually use military force, that we need to avoid situations where we commit troops because we can't think of anything else to do...Sometimes, I think we get into a situation where we have, because of the publicity given to a particular event -- you may have a real tragedy unfolding someplace in the world, but it doesn't affect vital U.S. interests. And you have to make a decision that you'll do whatever you can diplomatically, working through the international community or perhaps providing sustenance and medical supplies and support for humanitarian purposes, but you're not going to commit U.S. troops to combat to deal with that particular situation. Those are choices that presidents get paid to make."[608]

Freedom in the 21st Century, Brookings Institute quote "the government is almost ready to talk about regulating Myspace".[609] +ADD Obama's quote in Steed: "the Internet is like the wild, wild west." & "The answer lies in two arguments presented here: first, that the emergence of multipolarity and the relative erosion (or balancing) of American power has created the space for arguments that indeed already existed in the 1990s to benefit from real political backing. Second, the course of events in cyberspace have presented serious and genuine security concerns that can no longer be ignored; these can be roughly broken down into two realms of events, cybercrime and cyber-enabled/connected revolutions across the world. The former has perturbed Western nations most of all, who are now challenged to protect their own hyper-connected societies from harm. The latter, meanwhile, concerns above all autocracies – Russia and China especially – who have viewed events such as the Arab Spring and Colour revolutions as mortal threats enabled by Internet-connected devices and services. On multipolarity, right away realism must strike in asserting that no notion of an end to history could have expected to endure. To have believed so was no doubt an exercise in hopeful naivety at best and, at worst, a state of romanticised political delusion, born of the permissive climate of the 1990s where a belief in unipolarity, liberal triumphalism, and, consequently, apolitical Internet governance *could* be indulged."[610]

---

[607] Bahador, *The CNN Effect in Action*, p. 41.
[608] Cooper. "THE 2000 CAMPAIGN".
[609] The Brookings Institution. "Middle East Crises and Conflicts - The Way Ahead". Washington, D.C. 5 October 2017. Transcript.
[610] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019. p. 32-33.

In reality, the Internet was created in nuclear holocaust disaster scenarios by the RAND Corporation and the US Air Force during the Cold War[611], and later fell under the administration of the US Department of Defense.

"The application could also take control of a consenting user's account to automatically send out tweets. Prominent official IS members and supporters signed up for and formally endorsed the app as a trusted and official source of news. The Dawn of Glad Tidings automatically sent out links to official IS news releases and media, and hashtags that the ISIS social media team wanted to promote. Although the application had been suspended by Twitter at the end of Summer 2014, the number of pro-IS accounts in 2014 and 2015 remained significant, further enriched by thousands of bots (i.e., computer software pieces that act like actual Twitter users) tweeting and retweeting specific contents."[612]

"The National Security Agency and the FBI teamed up in October 2010 to develop techniques for turning Facebook into a surveillance tool...Documents released alongside security journalist Glenn Greenwald's new book, "No Place To Hide," reveal the NSA and FBI partnership, in which the two agencies developed techniques for exploiting Facebook chats, capturing private photos, collecting IP addresses, and gathering private profile data...The NSA describes its methods as "assumed authentication," ...The report states that the NSA also "disguises itself as a fake Facebook server"...Zuckerberg claimed he disapproved of the NSA's actions and said that he's spoken to president Barack Obama by phone [on the topic]".[613]

+ADD US Court of Appeals For the First Circuit Alexander Yershov v. Gannett Satellite Information Network, Inc. (Massachusetts) 26 April 2019 "Yershov brings the class action lawsuit against Defendant Gannett Satellite Information Network, Inc. for allegedly disclosing information about Yershov to a third party in violation of the Video Privacy Protection Act of 1988 (VPPA)...In ruling on a motion to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6), the distric tcourt found that the information Gannett disclosed concerning Yershov was "personally identifiable information" under the VPPA, but that Yershov was not a "renter, purchaser, or subscriber" of or to Gannett's video content and, therefore, not a "consumer" protected by the Act...We agree with the district court that the information disseminated by Gannett concering YErshov was PII, but we also find that the compalint adequently alleges that Yershov was a "consumer" under the VPPA. We therefore reverse the dismissal of the complaint and remand this case for further proceedings."..."Gannett is an international media company that produces news and enteratinment programing, including the newspaper USA Today...USA Today Moblie App...users must visit the Google Play Store...each time the user views a video cclip on the App, Gannett sens to Adobe Systems Incorporated (1) the title of the video viewed, (2) the GPS coordinates of the devicce...and (3) certain identifiers associated with the user's device, such as its unique Android ID."..."Adobe is an unrelated third party that offers data analystics and online marketing service to its clients by collecting

---

[611] Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008, 143-46.

[612] Monaci, Sarah. "Explaining the Islamic State's Online Media Strategy: A Transmedia Approach". *International Journal of Communication*, Vol. 11. 2017, p. 2843.

[613] Harrison, Weber. "How the NSA & FBI made Facebook the perfect mass surveillance tool". *Venture Beat*. 15 May 2014.

information about consumers and their online behavior."..."In late 2013, Yershov downloaded and installed the App on his Android device. Yershov does not allege that he opted to receive push notifications, so we will assume that he did not. Nevertheless, each time Yershov watched a video clip on the App, Gannett disclosed to Adobe the title of the viewed video, Yershov's unique Android ID, and the GPS coordinates of Yershov's device at the time the video was viewed. Using this information, Adobe was able to identify Yershov and link the videos he had viewed to his individualized profile maintained by Adobe."...Precedent referenced: "The profile contained a list of 146 films that Judge Bork and his family had rented from a video store. Members of Congress denounced the disclosure as repugnant to the right of privacy. Congress then passed the VPPA "to preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials. To effectuate this purpose, Congress in the VPPA created a civil remedy against a "video tape service provider" for "knowingly disclosing, to any person, personally identifiable information concerning any consumer of such provider" The statute defines the two terms in this case as follows: (1) term "consumer" means any renter, purchaser, or subscriber of goods or servicecs from a video tape service provider…(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific materials or services from a video tape service provided….While Gannet claims in its motion that it is not a "video tape service provider" under the VPPA, it did not challenge the sufficiency of Yershov's pleading as to this element of the claim...We agree with the district court that the information about Yershov that Gannett disclosed to Adobe fits the definition of PII. The statutory term "personally identifiable information" is awkward and unclear. The definition of that term ("identifies a person as having [obtained a video]) adds a little clarity beyond training our focus on the question whether the information identifies the person who obtained the video. Nevertheless, the language reasonably conveys the point that PII is not limited to information that explicitly names a person. Had Congress intended such a narrow and simple construction, it would have had no reason to fashion the more abstract formulation in the statute. See United States v. New Eng. Coal & Coke Co. (1963). Moreover, the language Congress did use to define PII begins with the world "includes". That word normally implies that the proffered definition falls short of caputing the whole meaning. Se In re Fahey (2015) (explaining how its interpretation satisfied "the premise that when a statute states that the universe of X i'includes' Y, one normally presumes that Y is merely an example of what is in X, and that X includes more that Y"). Here, we also have the benefit of the official Senate Report expressly stating that the drafters' aim was "to establish a minimum, but not exclusive, definition of personally identifiable information." This makes sense. Many types of information other than a name can easily identify a person. Revealing a person's social scurity number to the governemnt, for example, plainly identifies the person. Similarly, when a football referee announces a violation by "No. 12 on the offense," everyone with a game program knows the name of the player who was flagged. Here, the complaint and its reasonable inderences describe what for very many people is a similar type of indentification, effectively revealing the name of the video viewer. To use a specific example, imagine Gannett had disclosed that a person viewed 146 videos on a single device at 2 sets of specified GPS coordinates. Given how easy it is to locate a GPS coordinate on a street map, this disclosure would enable most people to identify what are likely the home and work addresses of the viewer (e.g., Judge Bork's home and the federal courthouse). And, according to the complaint, when Gannett makes such a disclosure to Adobe, it knows that Adobe has the "game program," so to speak, allowing it to link the GPS address and device identifier information to a certain person

by name, address, phone number, and more. (A U.S. government website reports findings that, in 2011, the GPS accuracy on Android smart phones ranged from five to eight meters...) While there is certainly a point at which the linkage of information to identify becomes to unceratin, or too dependent on too much yet-to-be-done, or unforseeable detective work, here the linkage, as plausibly alleged, is both firm and readily foreseeable to Gannett. The complaint therefore adequately alleges that Gannett disclosed information reasonably and foreseeably likely to reveal which USA Today videos Yershov has obtained...We turn now to a closer question: Does the complaint adequately allege facts plausibly establishing that Yershov is a 'consumer' in relation to Gannett within the meaning of the statute? In arguing that his complaint adequetely makes such a allegation, Yershov limits himself to arguing that he is a 'subscriber' within the meaning of 2710(a)(1), so we limit our own inquiry accordingly. For the following reasons, we think that Yershov is a 'subscriber'. We begin with the statutory text. Because it contains no definition of the term 'subsriber,' nor any clear indication that Congress had a specific definition in mind, we assume that the 'plain and ordinary meaning' of the word applies…'to recieve of be allowed to access electronic texts or services by subscription."..."We have also considered the opinion of the Elventh Circuit in Ellis v. Cartoon Network, Inc. (2015) While the court in Ellis agreed that one can be a 'subscriber' without making a monetary payment, it nonetheless found that the plaintiff's acts of downloading and using a free mobile device application from the Cartoon Network did not make him a 'subscriber' under the VPPA...subscriptions 'involve some or most of the following factors: paymet, registration, commitment, delivery, expressed association, and/or access to restricted content. It then found that there existed too few factors in the particular case before it, explaining that the plaintiff did not 'sign up for or establish an account,' 'make any payments,' 'become a registered user,' 'recieve a Cartoon Network ID,' 'establish a Cartoon Network profile,' sign up for any periodic services or transmissions,' or make any commitment or establish any relationship that would allow him to have access to exclusive or restricted content.' The Ellis court was also under the impression that the user of the application in that case did not have 'to provide any information to Cartoon Network.' We would describe the allegations (and their reasonable inferences) in this case quite differently. To use the App, Yershov did indeed have to provide Gannett with personal information, such as his Android ID and his mobile device's GPS location at the time he viewed a video, each linked to his viewing selections. While he paid no money, access was ot free of a commitment to provide consideration in the form of that information, which was of value to Gannett. And by installing the App on his phone, thereby establishing seamless access to an electronic version of USA Today, Yershov established a relationship with Gannett that is materially different from what would have been the case had USA Today simply remained one of millions of sites on the web that Yershov might have accessed through a web browser...Why, after all, did Gannett develop and seek to induce downloading of the App? And it is by no means self-evident that the version of USA Today one accesses with a browser is identical in all respects to the electronic version one accesses with the App."..."Image that Gannett have installed a hotline at Yershov's home, for free, allowing him to call Gannett and receive instant delivery of videos in exchange for his name and address, and he then used the hotline over the course of many months to order videos. We doubt that Congress would have intended that Gannett would have been free in such a scenario to publish Yershov's PII by claiming that he was not a purchaser, renter, or subscriber...We need simply hold, and do hold, only that the transaction described in the complaint - whereby Yershov used the mobile device application that Gannett provided to him, which gave Gannett the GPS location of Yershov's mobile device at the time he viewed a video,

hi device identifier, and the titles of the videos he viewed in return for access to Gannett's video content - plausibly please a case that the VPPA's prohibition on disclosure applies."[614]

+ADD Gannett Foundation Media Center (MacArthur's book forum 'Gulf War and Media')

"Slobogin and Schumacher [1993] argue that, in fact, the Court's conclusions about the scope of the Fourth Amendment are often not in tune with commonly held attitudes about police investigate techniques. To demonstrate this point, Slobogin and Schumacher tested four hypothesis: (1) the Court's conclusions about expectation of privacy do not correlate with citizens' actual understanding of privacy; (2) that people view searches of their own property as more intrusive than searches of others' property; (3) that a search with a specific objective (e.g., a frisk for drugs) was seen as less intrusive than a vague investigation; and (4) that crime control attitudes were inversely related to intrusiveness rankings. Slobogin and Schumacher urge judges to use their findings as a reminder that they may underestimate the intrusiveness of searching techniques and to reevaluate their analytical model for determining the reasonable expectation of privacy… [Robert] Power [1989] presents four norms as a framework for an intrusion paradigm that he argues will limit the adverse effects of technology use in surveillance and serve as guideposts for the preservation of privacy as technology evolves. Powers stresses that a clear and principled paradigm is critical because 'technological change is constant… the principle that is valid for today's technology may be a laughable anachronism tomorrow.' Currently, no bright line tests exist, and as police being to use enhancing devices, people begin to fear totalitarian/Orwellian consequences. Power's four norms for developing a principle are (1) that the observation have a legitimate purpose (reasonable cause); (2) that the observations be reasonably implemented (reasonable law enforcement conduct); (3) that some objects be specifically protected from all observation (e.g., homes, public restrooms); and (4) that each enhancement device be considered in context over time."[615]

Former IBM Security special advisor Bruce Schneier very blatantly affirms, with no argument to legal precedent or the laws being broken, that,

> "Corporations want your data. The websites you visit are trying to figure out who you are and what you want, and they are selling that information. The apps on your smartphone are collecting and selling your data. The social networking sites you frequent are either selling your data, or selling access to you based on your data. Harvard Business School professor Shoshana Zuboff calls this 'surveillance capitalism,' and it's the business model of the internet. Companies build systems that spy on people in exchange for services. This surveillance is easy because computers do it naturally. Data is a by-product of computer processes...Modern government surveillance piggybacks on existing

---

[614] *United States Court of Appeals For the First Circuit No. 15-1719 ALEXANDER YERSHOV v. GANNETT SATELLITE INFORMATION NETWORK, INC., USA TODAY.* Accessed 9 July 2019.

[615] Bloom, Robert M. *Searches, Seizures, and Warrants: A Reference Guide to the United States Constitution.* Westport, Connecticut: Praeger. 2003, p. 135-136.

> corporate surveillance...It [the NSA] said: 'Corporate American is spying on everyone. Let's get ourselves a copy.' And it does - through bribery, coercion, threats, legal compulsion, and outright theft."[616]

Governments internationally are interested in providing immunity for individuals in the technology industry fomenting civil strife and war abroad due to the easier access that creates to raw materials and the labor needed to produce ever-increasing amounts of minerals used in technological hardware. In 2008, 4 of the top 5 grossing corporations in the US were oil manufacturers, along with Microsoft. By 2014(?), the top four grossing corporations in the US were tech companies, including Facebook, Apple, Microsoft, etc. (find citation).

In 2013, the Ukraine experienced similar youth protests seen in the Arab Spring and Occupy movements, and it was widely reported by media that, amid the tumult, Shell Oil Company began an operation to extract natural gas in the Ukraine. There are endless examples of oil and gas companies moving in on war-torn areas to exploit resources, and it is widely recognized in the media that these companies are facilitated in these exploits by government agencies for the purposes of national enrichment. As militaries peak in this new phase of warfare called electronic warfare and space warfare, the tech industry not only enriches itself with more government contracts, it entrenches itself in the economic, material, service and expertise ecosystem of the new warfare. +Article on Syria electronic warfare center; The Intercept re-report on wargames planning US invasion of West Africa in 2025 (minerals only found there for tech).; Printed article on policy institute claims ISIS is expanding into West Africa. This is done entirely in order not to *pay* for the resources, likely because the very indebted nation of the US and those allegedly contributing to its GDP cannot pay. As the maxim goes, what one cannot beg, borrow, or buy, one steals.

Almost never addressed in policy discussions on media is the role of satellite technology services to the press. As a quarter trillion dollar industry annually profiting off of ground equipment sales, manufacturing, satellite launch services, and Earth observation services, the satellite industry represents 77% of the space economy, with only 1% of satellites in function for space observation, 35% of satellites dedicated to commercial communications, 19% to Earth observation, and 9% to military surveillance. These are all corporate, profits-driven industries. Many have disquieting names such as "UrtheCast", "ICEYE", "BlackSky Global", and "Planet".[617] The well-known public-facing corporations Amazon and Space X are also part of the satellite and satellite launch provider industry.

Despite the satellite industry's clear profitability, many of the services they necessarily provide, along with companies of split satellite-towers communications providers like Verizon, Sprint and AT&T, were declared by the International Criminal Courts (ICC) to be Crimes Against Humanity likened to genocide in the 1998 Rome Statute.

---

[616] Schneier, Bruce. *Click Here to Kill Everybody*, 57; 65.

[617] https://www.sia.org/wp-content/uploads/2017/07/SIA-SSIR-2017.pdf

To our purposes, it is of significant note that the satellite industry saw a 19% increase in US revenue between 2011 and 2012, by far the industry's largest revenue increase in the decade.[618] Part of this media industry services the public-facing media industries. For example, MAXAR Satellite Technologies company provides satellite Earth observation services by contract with the Associated Press and others in a program called the News Bureau Initiative.

"In the past year, the News Bureau has played a pivotal role in exposing the displacement and killing of Rohingya Muslims in Myanmar; **providing indisputable evidence** of human trafficking and illegal fishing **in an international court case**; **monitoring** the growth of **refugee camps** in Uganda; **chronicling** the physical toll of **wars in Iraq and Syria**; and **revealing the devastation** of numerous natural disasters, **including the California wildfires and hurricanes Harvey, Maria, and Irma**. The News Bureau was formally established in February 2017 by DigitalGlobe, **building upon earlier work the company did to enable investigative reporting projects**. Most notably, **DigitalGlobe provided the 'smoking gun' image to the Associated Press** (AP) that showed two trawlers loading slave-caught seafood onto a commercial cargo ship. **As a result of the** Seafood from Slaves **investigation**, more than 2,000 enslaved men were freed, **U.S. law was changed and AP was awarded the 2016 Pulitzer Prize** for Public Service. 'DigitalGlobe provided critical evidence we needed to expose the slave fishing operation and hold the responsible parties accountable for their actions,' said Marjorie Miller, AP Vice President of Global News and Enterprise. '**Access to high-resolution satellite imagery** has allowed AP to accurately report from parts of the world that are too remote, dangerous or inaccessible to reach in any other way.' Now as part of a family of industry-leading space and technologies companies under **Maxar Technologies, the News Bureau has access to radar satellite imagery from MDA and advanced analytic capabilities** from **Radiant Solutions**. Applications for our unrivaled combined capabilities include **broad-area monitoring** of illegal fishing, logging and mining; understanding urban development and environmental changes; and **gaining real-time insight into dynamic global events using crowdsourcing and social media analytics.** [619]

the hidden SAR effect on CNN and satellite surveillance audio/visual programming provided by the surveillance state industry to determine policy agenda of the media.

+ Find article on FBI scraping its own social mapping database in 2005? in favor of using Facebook for free (preface for national debt and crime link) and .

"The Bomb and the GNP"

We are well on our way to becoming a banana republic in every respect except, of course, that we don't grow bananas.

---

[618] https://www.sia.org/wp-content/uploads/2017/07/SIA-SSIR-2017.pdf

[619] Maxar Technologies. "Maxar Technologies' DigitalGlobe Celebrates First Year of Its News Bureau Initiative, Applying Space-Based Insights to Enhance Global Transparency". 5 March 2018. Internet resource.

Burt Prelutsky

This section argues that since the end of World War II sovereignty and global economies have been dictated by US national security interests. This section provides historical context to technology industries' conduct in the following sections Social Engineering and Proxy Wars and 'Going Native'. It provides historical backdrop for the more analytic section Recent Developments and Research and Development.
In this section "The Bomb and the GNP", I explain the way in which overwhelming presence of the security state has depressed the US and global economy by making all aspects of society subject to the security state, thereby creating something of a **security-banana republic**. I define this as a politically unstable country, or globe, operated as a private commercial enterprise with an economy entirely dependent on exploitative national security industries. The Banana Wars (1898-1934) which resulted from the Roosevelt Corollary on the Monroe Doctrine (1904), promising "the exercise of an international police power", suggests a causal connection between security states and banana republics. The material goods represented by bananas are in addition to the profits made by security industries in such places and may not be essential to constitute a banana republic. [REWORD - repeated]

+ADD **[TOPIC – supervenience of national security creates a 'banana republic']**

"Neorealism's perspective on international politics derives from its two core assumptions: the centrality of autonomous states wishing to survive and the salience of international anarchy. Because world politics takes place within a self-help realm, states must rely on their own resources to protect them-selves and further their interests. Whether they desire safety or opportunistic expansion, states are better served by superior, not equal, power. For this reason, neorealists argue, statesmen are usually more concerned with relative advantages than with absolute gains. The problem of uneven gains giving advantage to one side or another makes international cooperation difficult to achieve and hard to maintain. **The neorealist paradigm is built on a fundamental belief in strong links between anarchy, security, and relative gains.** Though states are not in a constant state of war, anarchy means that nations must constantly fear enslavement or extinction. Because the consequences of a mistake can be catastrophic, states must be cautious in assessing the intentions of both foes and allies, since today's friend may be tomorrow's enemy."[620]

+ADD after *Capital Ungoverned* quotes
"This line of argument would make it possible, without further examination, to dismiss external political or structural pressures as having done nothing more than facilitate an outcome that was already made imperative by the internal logic of the market. But the parsimonious, economistic explanation deals 'adequately' with on the 'stylized fact' – to borrow an economist's term – of liberalization only in the abstract. The economist's parsimonious explanation is less helpful to the investigator who confronts and tries to make narrative sense of voluminous masses of archival evidence. The fact that some reference to U.S. policy is indispensable to the narrative is, moreover, of central theoretical importance… The need to incorporate U.S. policy into the

[620] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 101.

explanation of liberalizing reform raises a second issue of theoretical importance. It nourishes the suspicion that another force is at work in the international political economy which is influencing change in U.S. policy. That force is uneven growth… For Gilpin, regularity in international economic relations requires stability in the underlying political order. But the underlying political order is weakened if uneven growth favors the rise of countries that contest the rules of international economic relations and if, inversely, it saps the strength of countries that enforce those rules. The current order, Gilpin speculates, is threatened by the end of the U.S. economy's uncontested supremacy in the world economy. That supremacy allowed the United States to play a leadership role in fashioning and enforcing the rules of international relations in the post-World War II era… Uneven growth, in this account, flows like an undercurrent in the international political economy. In time, that undercurrent can disperse and wash away the institutional constructs that ride the waves at the surface. Uneven growth may not be the only destructive undercurrent. Technological change and market rationality may be others. But the concept of uneven growth is particularly suggestive when one examines liberal reform in interventionist states. One might nevertheless resist the notion that **the United States, sole military superpower following the collapse of the Soviet Union and well positioned to dominate world markets in growth sectors such as information-processing technologies, declined as hegemonic power,** despite signs of decline as found, for example in the secular depreciation of the dollar relative to the mark and the yen or the achievement of parity in per-capita gross national product by European and East Asian economies. Such resistance might be justified if it were not the case that U.S. policy has sought more than once to slow or prevent what policymakers themselves have perceived to be a decline of U.S. influence in world politics and the international political economy. The dismantling of credit activism does not necessarily reflect the relative decline of the United States as a hegemonic power. It does, however, bear the imprint of American efforts to prevent that decline from occurring. **Broadly speaking, both credit activism and liberalization in financially interventionist states reflect the making and unmaking of a hegemonic world order, the purpose of which was to preserve the capitalist order from the forces that threatened it**. That order was compose of institutions and arrangements that sought to give the state the means to manage and direct capital in a way that preserved political stability within the framework of an open international economic order… Uneven growth undermined this protective international order by weakening the willingness and perhaps even the capacity of the hegemonic power to manage and underwrite the institutions and arrangements that supported it. **As the United States reacted against its self-perceived decline in the 1970s and 1980s, it unleashed the global shocks in money and finance that produced the pressures for reform documented here."** [621]

"To understand financial liberalization in interventionist states, one must first have grasped both the political purpose of interventionism and the external validation that it received from U.S. policy. Interventionism had no purpose other than to bolster the foundations of the capitalist order by aggressively addressing threats, both internal and external, to that order's survival. This meant several things. First, it meant promoting growth and keeping people at work. The 1950s were, in every advanced industrialized country and in international economic relations generally, a reaction against the 1930s. Second, it meant silencing capitalism's potential adversaries through compensation and even outright clientelism. Such compensation was sometimes financed through redistribution, but more typically through inflation. Third, in many countries it meant using policy to create or strengthen an indigenous industrial and financial elite. Finally, it

[621] Loriaux, Michael. *Capital Ungoverned*. P. 209-11.

meant promoting industrial growth, which was important not because it accelerated GDP growth – this would be difficult if not impossible to demonstrate – but because national elites considered industry the source of military and economic power in international politics.[REALIGNMENT OF WORLD MARKET TO US NATIONAL SECURITY CONCERNS] … That preoccupation became particularly insistent in the 1970s when the Nixon Doctrine, the fall of Vietnam, and the conjunction of an international oil and monetary crisis all pointed to the withdrawal of the United States from its hegemonic role. Capitalism was not only being defensed in South Korea, it was being nurtured. It is there that one finds the most extraordinary effort to create the material foundations that allowed Korea to thrive in a world capitalist political economy and to reform its society in a way that reinforced the chances of that success. The Korean state not only industrialized the country, it created the Korean industrial class. It was the state that transformed the owners of auto repair shops into the chief executive officers of multinational corporations, 'a striking substitution of the state for the 'natural' historical process of development.' Activist credit policy was the principal tool that the state employed in its experiments with 'social engineering' on this vast scale."[622] ; "Uneven growth diminished the willingness and perhaps even the ability of the United States to manage an open international system that was tolerant of credit activism… Those policies triggered four events that contributed directly to the liberalizing turn in world finance: (*a*) the dollar crisis of the late 1960s and early 1970s and the subsequent collapse of the Bretton Woods monetary order, (*b*) the collapse of the hegemonic order in the petroleum market (to the extent that that collapse was fomented by U.S. monetary policy), (*c*) the effort by the United States in the 1980s to defend its military preeminence in the world by borrowing heavily on world financial markets, and (*d*) the effort by the United States in the 1980s to rid the international political economy of the self- discriminatory arrangements that is had itself introduced and tolerated up and through the mid-1960s. The Bretton Woods system collapsed when the United States rejected devaluation as a response to international speculation against the dollar, refused demands by other countries to reinforce international controls on the movement of capital, and demanded that other countries revalue their own currencies. When other countries failed to revalue their currencies, the United States reneged on its commitment to exchange dollars held by foreign central banks for gold at a fixed price. **Joanne Gowa underscores the nationalist motivations that drove U.S. policy, which effectively relegated the survival of the postwar international monetary regime to a distant third-place priority, behind the prosperity of the domestic economy and U.S. security objectives**. The collapse of the Bretton Woods system imposed two kinds of stress on other countries. First, it deprived inflationary, trade-dependent countries of international solidarity in defending and readjusting the external value of their currencies by putting an end to the central banks' monopoly on international currency transactions. Currencies (or blocs of currencies) were made to fluctuate on the market, and the power of monetary officials to intervene to control the external value of their currencies was much diminished. Second, floating rates introduced the specter of destabilizing spirals of inflation and currency depreciation."[623]

From "The Legacy of Surveillance": "Surveillance intensity and social capital: Dependent variables: Our initial focus is on the influence of secret police surveillance in the former GDR on current levels of social capital in East Germany. Our dependent variable in this stage of our analysis is the level of social capital at the district level. Since we are interested in measuring

---

[622] Loriaux, Michael. *Capital Ungoverned*. P. 211-12.
[623] Loriaux, Michael. *Capital Ungoverned*. P. 219-20.

people's propensity to cooperate for reasons other than standard economic incentives, we focus on three measures of civic spiritedness that are hardest to explain with self-interested agents: electoral participation, sports club membership, and cadaveric organ donations… Our central explanatory variable is the surveillance density (Surveillance) in the districts in the former GDR as described above… For all three measures of social capital we find a statistically significant and negative relation between surveillance density and social capital. This is strong confirming evidence for our central conjecture that the scale and depth of penetration of people's private lives, as well as of the institutions of state and society in the GDR, has a lasting effect on social capital in East Germany even one generation after the oppressive regime's collapse. The results are not only statistically but also substantively significant. A one standard deviation increase in Stasi informer density (about 2.73 informers per thousand people) is associated with a 0.6 percentage point decrease in electoral turnout, and a decrease of 16 members in sports clubs per thousand people – or 10% of the sample mean. Similarly, a one standard deviation increase in surveillance intensity reduces the number of organs donated post mortem per 100,000 inhabitants by 1 across the districts in East Germany. Note that the mean number of organs donated per 100,000 inhabitants is a mere 2, thus suggesting that a one standard deviation increase in Stasi informer density reduces organ donations by up to 50% of the sample mean." [624] ; "electoral turnout measures not only social capital but may also contain characteristics of the post communist society such as individuals' attitudes towards democracy… The number of cadaveric organ donations is a powerful measure of social capital in its own right. This is because nondonors have been found to demonstrate a remarkable lack of trust in the fairness of organ allocation, as well as a lack of belief that donation is for the common welfare… Given the importance attached to top-level sport in the GDR, designated Stasi informers systematically filled all important positions in sports clubs, as they did in most other organizations… . This also implies that Stasi surveillance was higher where people gathered, pursued group activities and exchanged socially and economically… Since West Germany during the same historical period did not suffer from a state security body that invaded every aspect of people's lives and all spheres of state and society, our results suggest that **surveillance intensity and the ensuing social capital erosion in East Germany may be an important explanatory factor for the persistent differences in economic prosperity between East and West Germany.** In fact, when we set the surveillance density to zero for West Germany and to the mean value of 6.12 observed across the districts in our sample for East Germany, then following the regression estimates in Tables 3 and 6 surveillance in the former GDR explains 0.7 to 2.3 percentage points of the difference in the unemployment rate between East and West Germany. Using the figures set out at the beginning of this paper, this is a sizable effect and accounts for approximately 10.9% to 36.3% of the unemployment differential between East and West Germany. The mean difference in unemployment rate explained across our social capital measures is 1.6 percentage points, or **25.6% of the unemployment disparity**. Similarly, following our regression results the difference in surveillance between East and West explains € 97 to € 491 of the € 4,500 **difference in income per capita. This corresponds to between 2.2% and 10.9% of the overall gap, with a mean difference explained of 6.6% (€ 298).** Our results complement the impressive range of economic phenomena scholars have successfully explained using social capital: economic growth, financial development, size of firms, and innovation… We

[624] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010, p. 19, 21, 23.

furthermore find robust evidence that **surveillance intensity has a strong negative effect via social capital on current economic performance** in these regions. Since West Germany did not experience an oppressive regime shock and intense secret police surveillance during the same historical period, our **results suggest that Stasi surveillance and the ensuing social capital erosion in East Germany may be important explanatory factors for the persistent differences in economic prosperity** between East and West Germany. The results presented in this paper invite scholarly research on other postcommunist economies with substantial secret police activities to confirm the relationship between surveillance intensity, social capital and economic performance detected in this paper… **This has relevance for all economies around the world**, and for post-communist countries and those that have experienced other forms of oppressive regimes, in particular. Autocratic and hierarchical regimes that **perpetuate thanks to a repressive State Security apparatus, imposition or brutal force** as opposed to consensus are natural vehicles of creation of a culture of mistrust… The persistent differences in social capital and economic prosperity between East and West Germany are a telling case for policy-makers**: the formal model put forward in this paper indicates that, absent positive external shocks, it could probably require another several generations until the scope of cooperation in East Germany converges on the level characteristic of West Germany**."[625]

The actions taken during the COVID-19 pandemic by state entities, including the economic effects of population loss, lockdowns and trade disruptions, have proven Gowa's assessment legitimate, as US security policy continues to take primacy over the global economy in the most severe scenario to date.

[re: policymaking *Global Trends*: Long-Range Projections: A Cautionary Tale In the 20th century, experts forecasting the next 20 years—roughly the time frame of this study— often missed major geopolitical events, basing their predictions largely on linear projections without exploring possibilities that could cause discontinuities. Before WW I, while tensions between European "great powers" were on the rise, few had an inkling of major changes in the offing, from the extent of mutual slaughter to the downfall of age-old empires. In the early 1920s, **few envisioned the lethal situation about to unfold, ushered in by the Great Depression, Stalin's gulags, and an even more bloody world war encompassing multiple genocides. The postwar period saw the establishment of a new international system—many of whose institutions—the UN and Bretton Woods—remain with us. Although the bipolar and nuclear age did not lack war and conflict, it did provide a stable framework until the collapse of the Soviet Union**. The development of a globalized economy."[626] ;
"Globalization at Risk with the 2008 Financial Crisis? As with most of the trends discussed in this report, the impacts from the financial crisis will depend heavily on government leadership. Proactive fiscal and monetary policies probably will ensure the current panic and likely deep national recessions will not turn into an extended depression, although reduced economic growth could slow globalization's pace, increasing protectionist pressures and financial fragmentation. The crisis is accelerating the global economic rebalancing. Developing countries have been hurt; several, such as Pakistan with its large current account deficit, are at considerable risk. Even

[625] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010, p. 19-20, 25, 29, 38-40.
[626] Global Trends 2025, p. 5

those with cash reserves—such as South Korea and Russia—have been severely buffeted; steep rises in unemployment and inflation could trigger widespread political instability and throw emerging powers off course. However, if China, Russia, and Mideast oil exporters can avoid internal crises, they will be in a position to leverage their likely still sizeable reserves, buying foreign assets and providing direct financial assistance to still-struggling countries for political favors or to seed new regional initiatives. In the West, the biggest change—not anticipated before the crisis—is the increase in state power. **Western governments now own large swaths of their financial sectors and must manage them, potentially politicizing markets. The crisis has increased calls for a new "Bretton Woods" to better regulate the global economy. World leaders, however, will be challenged to renovate the IMF and devise a globally transparent and effective set of rules that apply to differing capitalisms and levels of financial institutional development**. Failure to construct a new all-embracing architecture could lead countries to seek security through competitive monetary policies and new investment barriers, increasing the potential for market segmentation."[627]

+ADD "the Political Instability Task Force reports **the factors that best predict state failure are political, not economic**. The nature of political regimes associates far more strongly with subsequent political instability than do indicators of economic wellbeing."[628]

This section provides historical context to technology industries conduct in the following sections Social Engineering and Proxy Wars and 'Going Native'. It provides historical backdrop for the more analytic section Recent Developments and Research and Development.

The history of American companies providing for the modern US defense industry can reasonably be considered to have initiated in 1940 in preparation for US involvement in World War II. The argument that US commercial manufacturers were originally opposed to contracting for defense purposes because they were not equipped to fulfill the orders, or that politically they were conscientious objectors, including Henry Ford of Ford, Alfred Sloan Jr. of GM, and public figure and aviator Lindberg, whose influence was in favor of anti-interventionism in the then-termed "European conflict", do not present the conflicts of corporate and political interest weighed by corporate owners in resisting American defense contracting. Sloan is quoted as casting the European front as "really nothing more or less than a conflict between two opposing technocracies."[629]

Technocracies are distinguished by political leadership of experts and industry professionals. Ford, General Motors, and IBM (owned by Thomas J. Watson) were all commercial contractors with Nazi Germany prior to the 1941 attack on Pearl Harbor. They were the main political industrialists to both technocracies, and as the technocrats to both sides in the war they could not then be called "opposing". Many of the individuals in charge of these corporations and individuals representing related manufacturing industries, such as Charles

---

[627] Global Trends 2025 P. 10

[628] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 9-10.

[629] Hyde, Charles K. *Arsenal of Democracy: The American Automobile Industry in World War II*. Detroit: Wayne State University Press, 2013, p. 3.

Lindberg, were Hitler supporters, favored the Third Reich's political philosophy, and had innovated specific products and services according to the Nazis' special orders. Likely, for these major US corporations and manufacturers and spokesmen figures, anti-interventionism signified little but being pro-corporate interventionists in foreign markets including in the Nazi German market, despite being acutely aware of the genocidal pogroms in place already in Europe.[630]

In fact, the US government itself would end up contracting with captured prisoner German Nazi innovators and engineers under the program termed Operation Paperclip. These included Nazi SS officers and scientists that could become leaders in the US intelligence and aeronautics industries, the most infamous of whom may be former Nazi SS Officer Wernher von Braun who went on to become head of the US space and rocketry industry.[631] Von Braun is recognizable from his having starred in the 1955 Disney film *Trip Around the Moon* made for public consumption during the space race. The US (and Soviet Russia's) willingness to recruit Nazi experts could have been predicted by the US' early insistence on contracting with Ford, GM and other such companies. Apparently the US' Trading With The Enemy Act of 1917, (expanded again in 1933, 1950, 1970 and 1971)[632] did not apply directly to the US government itself, desirable corporations, or experts.

+ADD More on rocketry and space industry and its irregular applications, its connection with unorthodox religions and science fiction since its inception, Jack Parsons, Hubbard https://www.wired.co.uk/article/jpl-jack-parsons

+ADD War Production Board created by Roosevelt, liaison between government and industry was the Automotive Council for War Production. Its Planning Committee created in February 1942 "to examine the feasibility of producing the war goods the military demanded for 1942 and 1943." Headed by Kuznets, Nobel Prize winner in Economics in macroeconomic analysis who "had developed national income accounting measures, including the concepts of GNP, GDP…"[633] State-controlled war production and the measure of gross national product were inextricably created. ;

+ADD "However, it also seems likely that Stalin's caution did not stem from fear of the atomic bomb as a decisive weapon. What alarmed him about the United States was Detroit – not SAC! He appears to have felt very strongly that no sensible government tangles with a nation with a GNP of $300 billion a year. Luckily we had both assets – the bomb and the GNP – so that any difference between U.S. and Soviet calculations was not crucial."[634]

---

[630] Black, Edwin. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Crown Books, 2001, p. 112, 113, 125, 140, 180, 201.

[631] Watkins, Jay. Book Review of *Operation Paperclip: The Secret Intelligence Program to Bring Nazi Scientists to America*, by Annie Jacobsen. (Little, Brown & Company, 2014). *Intelligence in Public Literature*, Vol. 58 No. 3. CSI Publications. Center for the Study of Intelligence. 6 October 2014. Electronic resource.

[632] https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1136&context=mjil

[633] Hyde. *Arsenal of Democracy*, p. 31.

[634] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 425.

In his book *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Edwin Black argues that IBM was totally complicit in Nazi occupation crimes because, not only was it acutely aware of the genocides occuring in Nazi Europe due to media coverage at the time, but most crucially, the IBM machines sold to the Nazis required continued servicing and regular deliveries of billions of specialized punch cards from IBM (known as Dehomag in Europe) in order to function, including at monthly intervals at concentration camps. An early form of computer coding or software, these machine-readable cards were coded to cross-index up to sixty fields on "slave labor cards", "Ghetto-registration cards", railroad cards of trains scheduled to death camps, and census cards, all coded patently by IBM with indicators specific to the cards' function, including fields for ethnicity, gender, age, country of origin, block assignment in Ghetto, routes of freight/passengers to be deposited at which concentration camp, and monthly death tolls at the so-called work camps.

Once in death camps, inmates were assigned IBM programmed codes. "In fact, the Auschwitz tattoo began as an IBM number."[635] Column 1 signified *Political Prisoner*, 12 *Gypsy*, 14 *Covert Prisoner*, 8 *Jew*, 5 *Clergy*, 2 *Bible Researcher*, 16 *Diplomatic Consul*, 3 *Homosexual*, 7 *Foreign Civilian Worker*, etc. When they died, the deaths were coded D-4 *Execution*, E-5 *Suicide*, and F-6 *Special Treatment*.

Despite the price this high-precision tech endeavor cost the regime, "The SS statistician [of The Race and Settlement Office] concluded that the high cost of the IBM equipment was justified because this was the 'exact instrument for complete surveillance both on a large scale and down to the smallest detail.'"[636]

Internal communications at IBM reflected a high awareness of the war ambitions of the Nazis, volleying terms and conditions queries back and forth in 1937 over "the 'new territories' to be handed to Dehomag [IBM Europe]", executives asking one another, "Considering present changes in the map of Europe, don't you consider it best to wait?". This was six days after the German takeover of Czechoslovakia and previously Austria, with Poland and Lithuania being the next 'map changes' being considered by IBM before they even took place. IBM was in vendor contracts with the war ministries of Yugoslavia, Rumania, Hungary, Poland, Sweden, Holland, France, *and* Nazi Germany simultaneously, but their most lucrative contracts by far were with the Nazis.[637] And in 1940, when IBM CEO Watson was asked by Nazis to sell control of Dehomag to the Nazis as US involvement in WWII became rumored, Nazi officials asked IBM executives, in an effort to transition to Nazi management of IBM machines, "who will produce the machines which are indispensable to the German war economy?" Black writes:

> if he [Watson] allowed Berlin to embark upon its own *ersatz* punch card industry, Hitler's data automation program might speed towards self-destruction. No one could predict how drastically every Reich undertaking would be affected. But clearly, the *blitz* IBM attached to the German *krieg* would eventually be subtracted if not severely lessened.... If IBM did not

[635] Black, Edwin. "IBM and the Holocaust". 26 February 2012. Presentation at Yeshiva University, New York, NY. Internet resource.
[636] Black. *IBM and the Holocaust,* p. 210-212.
[637] Black. *IBM and the Holocaust*, p. 165-66, 203.

> have a technologic stranglehold over Germany, the Nazis would not be negotiating, they would simply seize whatever they wanted. For Watson, it was a choice.[638]

After IBM was forbidden to continue business with the Nazis under the Trading with the Enemy Act, IBM took all of its revenue from Dehomag and exited Nazi Europe. This was one of the first uses of computers in times of war. IBM continues to contract with the US Department of Defense and the US Census Bureau.

Part of Black's strength of condemnatory argument is his being able to prove that IBM was exclusively responsible for end-to-end operations of the data and information technology needed to carry out the Nazi genocides. Now, technology is so much more multifaceted. Such contracts for technological warfare and war crimes today require the active complicity of tens of thousands of technology and media companies, not just tens of thousands of IBM employees as it did in the 1930s.

Weaponry technology requires at least six completely distinct technology industries today made up of tens of thousands of companies specialized in: development, manufacturing, end users, content providers, internet service providers and internet backbone providers. Each capability that is developed and deployed requires the expert complicity of each industry and each company, with that complicity being renewed and confirmed for some functions on a nanosecond by nanosecond basis.

"there was a propensity for government to favor secrecy about war until World War I when Allied leaders became converts to the view that war could be waged more successfully with publicity than with silence. 'There was even a growing belief in the Allied camp' Mathews concludes, 'that victory could not be assured without the encouragement to morale that would presumably come with more news… News had become a weapon in the arsenal of war, one that could not be ignored."[639]

"SPIEGEL: Do you think the United States is still an important factor in securing a peaceful solution to the Middle East crisis? Carter: Yes, as a matter of fact as you know ever since Israel has been a nation the United States has provided the leadership. Every president down to the ages has done this in a fairly balanced way, including George Bush senior, Gerald Ford, and others including myself and Bill Clinton."[640] [MOVE to other section?]

Social Engineering

Media action often preempts military action by the US. The use of media to impact public opinion is often addressed in terms of the effect it has on a population and policy. In this discussion, I focus on media broadcasting, in the broadest sense, as harbinger of war.

---

[638] Black. *IBM and the Holocaust*, p. 229-30.
[639] Roselle, p. 17-18.
[640] Spiegel Staff. "The US and Israel Stand Alone". *Der Spiegel*. 15 August 2006.

Likewise, "Other studies have focused mainly on social media networks involved in the foreign fighter recruitment process. Carter, Maher, and Neumann (2014) especially analyze the role of the so-called facilitators, spiritual guides who are not directly involved in terrorist organizations or in recruitment logistics, who nevertheless exert their ideological influence and pressure to support the cause of IS. Klausen (2015) remarks that regarding Twitter, a considerable flow of posts from foreign fighters in Syria does not directly reach followers in Western countries, but is controlled and retweeted either by terrorist organizations in the insurgent zones or by Europe-based organizational accounts associated with the banned British organization Al Muhajiroun and particularly with the London-based preacher Anjem Choudary. This reveals how, by exploiting an articulated and scattered network of social media disseminators and facilitators, locally produced propaganda could reach a potential global audience through network virality and pervasiveness."[641]

+ in hybrid warfare "…hackers, trolls, hired thugs, political 'technologists' and paid-for protesters are more useful than tanks, planes, and soldiers."[642]
"1. the use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society.
2. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."[643]

+ ADD "If a country's foreign policy were to favor one side in a conflict over another and eventually engage militarily, then it must be able to justify this by placing blame for the problems within a crisis on the side it opposes."[644]
+ADD "People in a city can influence operations by merely getting in the way while going about their daily routines. Noncombatants can actively assist one or both sides. Human beings are the only thinking components of the battlefield; they will tend to act so as to serve their own interests. They can often also be manipulated… Similarly applying the procedure to the information realm, consider friendly force use of deception: a particular section of the target audience might be considered as a field of fire for a PSYOP [psychological operation] campaign, a campaign seeking to conceal a force's operational intentions… Deception [is] actions taken to produce a disadvantageous misperception in the mind of a relevant decision-maker… Deception is among the most important types of adaptation. Previous RAND work has explored the relationship between urban terrain and deception, concluding that urban terrain facilitates the conduct of deception and amplifies deception tactics."[645]

---

641 Monaci, p. 2844.
642 Steed, p. 44.
643 Stevenson, Angus. "Social engineering". *Oxford Dictionary of English, 3rd Edition*. Oxford University Press. 2015.
644 Bahador, *The CNN Effect in Action*, p. 114.
645 Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 33, 35, 37.

"Adaptation [under Countering Adversary or Noncombatant Adaptation] is an activity, one that can either be turned to a force's advantage or left to use by others. It can be: Uncontrolled; Monitored and predicted; Guided; Prevented; Promoted."[646]
"Taking a sample from the counter-adaptive methods shown… the force with a technological edge could: [1] Attack an adversary at many points simultaneously. If the objective is to restore stable government, the friendly force could address shortcomings underlying popular disgruntlement…Addressing these many critical points simultaneously presents the leadership of the less capable force with multiple problems, severely tasking or overwhelming its ability to react and adapt effectively; [2] Take advantage of its surge capability to operate at a tempo beyond that the foe can match; [3] Continuously alter tactics, techniques, and procedures. Technologically superior U.S. forces suffered a tactical setback on October 3-4, 1993 in Mogadishu in part because they employed similar procedures repeatedly. Military forces, even unsophisticated ones, will learn lessons and look for opportunities to employ them. Diversity in tactics and procedures means that the foes' adapting to the last mission is less applicable to the next [NOT DONE OVER 20-70 YEARS re 9/11 & Arab Spring, Bin Laden's cement factory in Mogadishu in 1993 & Radio Free everywhere]; [4] Neutralizing an adversary's command and control structure. Whether via the removal of a commander, elimination of the opponent's communication capabilities, or overwhelming the enemy with information, denying the foe the resources needed to establish situational awareness and conduct analysis slows both its decision-making capability and the related ability to adapt."[647]

Senior Information scientist of the RAND Corporation, expert to the Senate Armed Service Cybersecurity Subcommittee and former project manager at DARPA, Dr. Rand Waltzman described his view of social engineering as "cognitive hacking", saying that, "People have been screwing with other people's minds forever, [But] an example of what *is* new: if you look historically, every time some new means of communication is introduced it was a major revolution in the way people conducted their business." [648]
The article goes on to describe social engineering as "how hearts and minds are won in the digital realm," the exact phraseology used by the Department of Defense about Iraqis during the early days of the US invasion of Iraq in 2003.

The aptly named Dr. Rand Waltzman explains that the US government is restricted in what data its employees can access in bulk social media collection, saying that "you know, the Chinese, the Russians, Hezbollah, the Mafia, basically every asshole on the face of the planet has

---

[646] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 38-39.
[647] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002, p. 39.
[648] Magee, Tamlin. "US government can't compete in information war, warns RAND Corporation: The RAND Corporation's Dr Rand Waltzman speaks with Techworld on the state of 'cognitive security' in the world and the 'democratization of weapons of mass disruption". *TechWorld*. 12 February 2018.

complete and open and unrestricted access to our public social media data – everybody but the US government."

Everybody also includes Dr. Rand Waltzman. He describes the red tape private people and corporations avoid, and regulated governments face, as setting "the bar for this kind of business so high that you can't even say the US [government] or Europeans are losing the game. They're not even in the game like that. This is beyond." He brings up the point that a private non-governmental group highly integrated with the US government, such as the RAND Corporation, would legally have to be tasked with government-sponsored social engineering.

Waltzman quotes to describe the societal role of social engineering, saying, "conscious and intelligent manipulation of the organised habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country."

In the Weberian framework, think-tank analysts are given the right by the State to legitimate infringement on the State's monopoly to information access and use of force. Major policy institutions act as loophole institutions that allow the government to act as it pleases without openly violating government rules of conduct. For example, when DARPA attempted to create the surveillance and monitoring project Total Information Awareness (TIA), it was ended when and "DARPA was almost shut down. It was a complete mess."[649]

Other comparisons of social media revolutions to Color Revolutions [+ADD quotes from ch 6 Bahador, pgs 97-127] https://russiamil.wordpress.com/2014/09/15/countering-color-revolutions-russias-new-security-strategy-and-its-implications-for-u-s-policy/ ; https://www.npr.org/2014/06/12/321392873/are-color-revolutions-a-new-front-in-u-s-russia-tensions ; https://news.yahoo.com/putin-says-russia-must-guard-against-color-revolutions-135807378.html?guccounter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAI6juX167hxzvv07wBgK29TfUmoyMz4Jb2dnFgweqMtsktwhNvKnYkT2qrFPF3p_aATtcd4FsdIqSseqAVAMjG9upCvIUoKGUsXWY3RE6S-FCMpUteMkBFy5789mFt6l3pzxtMrZt5WI6IQlgdt0ID8PSK3kHDOdDBF5wlZ2oSHm

The US National Intelligence Council wrote in 2009 in *Global Trends 2025* report, "These Islamic countries also receive foreign influences from European mass media, through satellite dishes and the Internet."[650]

"Between 2005 and 2010, the State Department funneled $12 million to opposition groups opposed to Assad. The US also financed Syrian exiles in Britain to start an anti-government cable TV channel they beamed into Syria."[651]

---

[649] Magee, Tamlin. "US government can't compete in information war, warns RAND Corporation: The RAND Corporation's Dr Rand Waltzman speaks with Techworld on the state of 'cognitive security' in the world and the 'democratization of weapons of mass disruption". *TechWorld*. 12 February 2018.

[650] Pg. 17 NIC World Trends 2025 {downloaded file]

[651] Bramhall, Stuart Jeanne. "The Arab Spring: Made in the USA: Review of Ahmed Bensada's Book". *Global Research.* 22 March 2018. Electronic resource. < https://www.globalresearch.ca/the-arab-spring-made-in-the-usa/5484950>. [previously published https://dissidentvoice.org/2015/10/the-arab-spring-made-in-the-usa/]

During the Soviet invasion of Afghanistan, the US sought to counter Soviet media efforts by broadcasting the US sponsored RadioFree Afghanistan station in 1985.[652]
-document from National Security Archives 1985 on Pakistani Intelligence aircraft broadcasting RadioFree Afghanistan[653]
-Reauthorized Radio Free Afghanistan in 2001[654] broadcast from Kuwait by then-Senator Joe Biden for $17 million in 2001 alone
-*Al-Hurra* television before US invasion of Iraq (already cited?)
http://eds.a.ebscohost.com.ezproxy.shsu.edu/eds/results?vid=0&sid=24164ff2-5bf5-489d-b18b-644f70abe70d%40sdc-v-sessmgr03&bquery=al-hurra&bdata=JmNsaTA9RlQxJmNsdjA9WSZ0eXBlPTEmc2VhcmNoTW9kZT1TdGFuZGFyZCZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d
-RadioFree Europe and Radio Liberty: 26 languages, available across social media platforms[655]
- https://www.globalresearch.ca/us-grant-35-million-promote-fake-news-bubble-syria-control-local-media/5701830
Oliver Ryan Clow, veteran and member of the Canadian Department of National Defence, explains that "Success was achieved in many previous wars through words, whether they were dropped from the sky (leaflets), plastered upon walls (posters), or transmitted over the air (radio). As a result, when the term Psy Ops is used, these mediums commonly spring to mind. The obvious consequence is that this limited exposure to Psy Ops has created a rut in our line of thought when it applies to *modern* Psy Ops."[656]
+ADD reference of Panama's Noriega sieged by US forces playing rock music outside church where he sought asylum
https://www.bbc.com/news/world-latin-america-40090809 ;
http://www.psywarrior.com/rockmusic.html ;
https://en.wikipedia.org/wiki/Operation_Nifty_Package
"**More importantly, satellite television channels such as *Al Jazeera*, although they have sometimes been accused of a biased political agenda, pride themselves on their precision concerning matters of fact and their criticism of corrupt Arab rulers. *The Voice of the Arabs*, on the other hand, was an overt vehicle for Egyptian state influence and often ridiculously inaccurate**. There was an ongoing tension between its avowed *raison d'être* as the forger of Arab unity and **the unedifying squabbles it ignited within the Middle East as a result of its habit of addressing Arab populations over the heads of their established rulers (?). It was a weapon wielded by the Nasser regime, rather than a genuinely collective voice. In the end, however, the weapon was as fatal to its makers as to their enemies.**
To sustain this argument, it is necessary to delve more deeply into the original plans and purposes of *The Voice of the Arabs*. It was, according to Mohammed Fayek, who later became Minister of National Guidance, "a nationalist project aimed at helping Arabs turn the page of colonial occupation

---

[652] Clarity, James F. "BREIFING; Come In, Afghanistan". *The New York Times.* 1 October 1985.
[653] [PRINTED]
[654] 107th Congress. "S. Rept. 107-125 - AUTHORIZATION OF 'RADIO FREE AFGHANISTAN'". Senate Report: Foreign Relations. US Congress. 14 December 2001.
[655] https://pressroom.rferl.org/about-us
[656] Clow, Ryan. "Psychological Operations: The Need To Understand The Psychological Plane of Warfare". *Canadian Military Journal (CMJ), Vol. 9, No. 1.* 2008, p. 24.

and division of their nation into small entities and build a better common future." … "Nasser himself announced his manifesto in Cairo's central Midan al-Tahrir:
We must follow the policy of a total war—the people's war. The enemy is now fighting us with money, hostile propaganda and the agitation of minds. This is the cold war between us and imperialism." …
"Minor revolutionaries from Aden were feted in Cairo; **trivial victories** such as the removal of the pro-British Principal of Aden Girls' College provoked sustained gloating across the airwaves." ..
"Ahmed al-Said acknowledges that **another part of *The Voice of the Arabs*' mandate was to inform Arabs of their own governments' sins.** This function first became apparent with a **concerted attack on the effective ruler of Iraq, Nuri al-Said, in 1954-55, over his support for the pro-British Baghdad Pact.** Nuri, with the subtlety for which he was known, initially responded only indirectly, intimating to the Egyptian Minister of Guidance, Salah Salem, that he found the whole programme far too lowbrow. Salem, known as "the Dancing Major" and the butt of many a joke, hurried home to demand that the great Egyptian author **Taha Hussein** be put on the air immediately. It had to be gently explained to him that Nuri was in fact resentful of the massive popularity of *The Voice of the Arabs*, **seeing it as a threat to his position. He was quite right. In late 1958, an Arab nationalist *coup d'état* in Baghdad** would force Nuri to flee disguised as a woman. He was discovered and killed, his body torn apart by the mob." ..
"Similarly, the Imam of **Yemen was overthrown in late September 1962 following a sustained campaign on *The Voice of the Arabs,*** most notably a series called "The Secrets of the Yemen" that had begun two months previously…Baydani even claims that his final radio announcement, on September 26, 1962, contained the secret code words—referring to a well-known Yemeni story—that signalled the start of the revolution… **Moreover, in the wake of the Yemeni revolution, King Saud and Crown Prince Faisal of Saudi Arabia,** who had already suffered from round condemnation of their personal lives and policies on The Voice of the Arabs "Enemies of God" programme throughout much of 1962, became the targets of even more insurrectionist propaganda. The "Committee of Free Princes," led by the exiled Prince Talal, was permitted to call for reform on Voice of the Arabs; and King Saud was explicitly told that he was the next target after the Imam.(19) Later, when Saud himself had been deposed by his brother**, his own hostile broadcasts from Cairo were carried on the same radio station.**"…
"The Voice of the Arabs, in other words, was in most respects the voice of the Nasser regime. "We cannot separate the policies of Nasser from the broadcasting," says Ahmed al-Said. From the outset, **it had strong links with Egyptian Intelligence, which had, indeed, come up with the concept of such a radio station in the first place. Both institutions, in a sense, performed the same job: They prepared the citizens of the Arab countries for revolution. As a result, they routinely shared information… *mukhabarat* officers, sometimes disguised as students** doing doctoral research, would call upon the trustworthy ones for situational reports. The *mukhabarat*, in their turn **would provide the presenters with feedback on the Arab people's response to their broadcasts**, advising them to raise or lower the tempo, as necessary… *The Voice of the Arabs* had been **very carefully designed to become a regional phenomenon. Following the establishment of the new Egyptian intelligence service** in March 1953, the Interior Minister, Zakaria Mohieddin, and intelligence officer Fathi al-Dib **had formulated an Arab nationalist action plan**, which included the development of a radio show as well as funding for Arab nationalist writers and students to study in Egypt…**It became a key foreign policy tool**, enabling Nasser to tailor his words precisely to a Pan-Arab audience." …
"It was this very tailoring of sentiments for a radical audience, however, that ultimately made the radio station a constraint on the Nasser regime. Ahmed al-Said goes so far as to argue that this was intentional. 'If Nasser's government did something wrong, we had to mention it. And

this happened. And he signed it.'… There is absolutely no supporting evidence for the contention that Nasser intended to allow *The Voice of the Arabs* to criticise his own regime.".. *"The Voice of the Arabs* radio station began preparing for a war on May 20,1967, when the regime ordered staff to 'heat it up.' Five days later, Nasser's military chief, Marshal Abdel Hakim Amer, allegedly told Ahmed al-Said that an Egyptian first strike was imminent, so they needed to be prepared to relocate if their transmitters were targeted. The radio station's military liaison officer informed Said two hours before the planned strike on May 27 that it had been called off, on Soviet orders. Once the war actually began, following the Israeli attack at dawn on June 5, the military continued to keep *The Voice of the Arabs* updated on the number of Israeli planes shot down, and other useful—if fictitious—morsels of information.(29) While the Egyptian air force lay in ruins on its runways, and Arab armies retreated on every front, ***The Voice of the Arabs* clung to the fantasy world it had created so painstakingly over fourteen years. It continued to boast of great victories even after Western media had made the scale of the disaster**—Israel rapidly took the Sinai Peninsula, Gaza, East Jerusalem, the West Bank and the Golan Heights—quite apparent. **Its credibility would never recover**."…
"Ahmed al-Said emphasises that his exaggeration of the number of planes shot down **was based on information provided by policy-makers whose numbers added up wrong.** It was, he says, his duty to follow orders in time of war, and to assist the army by issuing propaganda to deceive the enemy… **The "setback" of 1967 fatally injured the legitimacy of secular Arabism, facilitating the rise of the Islamist alternative in the 1970s**… He resigned before his loyal people fully realised the scale of the defeat, only to be called back by popular demonstrations**. His radio station, however, had been convicted** of deceit out of its own mouth, and could only be disavowed quietly."[657]

[REPEATED – from Radio-logical Warfare]

Audio radio and radar weaponry, although used for distinct purposes in war, have the combined effect to increase nuclear biological damage on a population. From the point of view of physics, the difference between radio and radar-enabled weaponry is in levels of directed radiation intensity. From the point of view of war weaponry strategy, any reason to increase the use of weaponry that will emit and cause radiation exposure to accumulate in a population serves as a weapon. This means it is not only the audible transmissions of radio, the words and ideas, that are strategy of war, but the pretext for higher transmission of radiation on a population is also part of the war strategy. Broadcasting stations would also make an ideal cover for radar weaponry control stations. As Biden's December 2001 bill stated, despite Voice of America radio already broadcasting successfully in Afghanistan in 2001 with "a substantial audience inside the country", $9 million, "The capital funding authorized in the bill contemplates construction of a new shortwave transmitter in Kuwait," and gives legal authority to exceed fiscal year 2002 Congressional budget in order to provide grant money exclusively in order to fund Radio Free Afghanistan. The bill also repealed "a permanent ban on construction of a U.S. shortwave radio transmitter in Kuwait. The ban was enacted in 1994, at a time of serious budget stringency and in the aftermath of the cancellation of a major transmitter project in Israel," and also designated the facility "to use U.S.-owned transmitters in Kuwait for broadcast of Radio Free Iraq or RFE/RL's Persian Service… The Committee expects both

[657] James, Laura. "Whose Voice? Nasser, the Arabs, and 'Sawt al-Arab' Radio". *Arab Media and Society*. Kamal Adham Center for Television and Digital Journalism of The American University in Cairo. 1 June 2006.

services to broadcast without hindrance or restriction from Kuwait by the end of the year."[658]

This Janus-faced use of media in war is apparent when considering the purpose of broadcasting audiovisual messages to a population, allegedly as information propaganda, while simultaneously destroying the electric grid that that population would need in order to consume that propaganda. +ADD reference to WWII Finnish-Soviet article

"Occasionally, however, remarkable results could be obtained. Late summer 1941, when the Finnish forces had already done a re-entry to the city of Viipuri, which was lost to Russia in March 1940, a couple of radio-controlled mines, see Figure 4, were found beside a bridge. Also, sudden explosions were heard in areas which should have been under Finnish control. Rapidly, it turned out, that the whole city seemed to be covered with such radio mines and Finnish specialists suggested a jamming action to be carried out on a frequency, which could be defined from the previously found mine. A popular Finnish folk song "Sakkijarven polkka" was played day after day through a powerful conventional AM transmitter. The choice of the record was not based on its popularity, but this particular piece of music (actually not a very nice one) happens to be practically continuous with no silent spots. Several triggering attempts by an audio triad could be heard on the band, but the music covered it until the batteries of the mines were exhausted. The action probably not only minimized the destruction of the city but also saved the castle of Viipuri for the coming generations… There exists a direct, though long relationship between the Radio Workshop of the Armed Forces, which produced the transmitters for Finnish guerilla troops; the State Electrical Workshop, which was responsible for many Air Force radios; and the present Nokia Telecommunications, the well-known supplier of both microwave equipment, cellular radio systems and - not too astonishingly - modern military communication infrastructure."[659]

Not all music used in radio warfare is audible songs familiar to listeners, however. Radio may broadcast music which is inaudible to the unaided human ear. For an example of (ELF) extremely low frequency music used in warfare, I highly recommend the (radio frequency) song titled "The Sun's Gone Dim and the Sky's Turned Black" composed by Icelandic composer Jóhann Jóhannsson (1969-2018) in his album *IBM 1401, A User's Manual.* The vocals of the track are imitative of ELF transmissions used in radio-enabled psychological warfare. Just like with any music, the transmission's effect on its environment, including the human mind and body, is housed within worded lyrics, tones/frequencies, durations and repetitions.

"Statement from Committee Chairman Richard Burr (R-NC):

"Increasingly, we've seen how social media platforms intended to foster open dialogues can be used by hostile foreign actors seeking to manipulate and subvert public opinion. This newly

---

[658] 107th Congress. "S. Rept. 107-125 - AUTHORIZATION OF 'RADIO FREE AFGHANISTAN'". Senate Report: Foreign Relations. US Congress. 14 December 2001.

[659] Eskeline, Pekka."The Story Behind Finnish Telecommunications Industry: Military Radio Systems and Electronic Warfare in Finland during World War I1 (1939-1945)". *IEEE AES Systems Magazine*, August 1996, p. 6-7.

released data demonstrates how aggressively Russia sought to divide Americans by race, religion and ideology, and how the IRA [Internet Research Agency] actively worked to erode trust in our democratic institutions. Most troublingly, it shows that these activities have not stopped. As we work to address these threats, these reports are proof positive that one of the most important things we can do is increase information sharing between the social media companies who can identify disinformation campaigns and the third-party experts who can analyze them."

Statement from Committee Vice Chairman Mark Warner (D-VA):

"These reports demonstrate the extent to which the Russians exploited the fault lines of our society to divide Americans in an attempt to undermine and manipulate our democracy. These attacks against our country were much more comprehensive, calculating and widespread than previously revealed. This should stand as a wake up call to us all that none of us are immune from this threat, and it is time to get serious in addressing this challenge. That is going to require some much-needed and long-overdue guardrails when it comes to social media. I hope these reports will spur legislative action in the Congress and provide additional clarity to the American public about Russia's assault on our democracy.""[660]

+CURRENT HEARINGS
+ADD Daniel Steed quotes *Cyber Politics*
+ADD https://www.forbes.com/sites/beasleydavid/2019/11/15/wall-street-journal-google-algorithms-altered-for-profit/#5b84f600283c

[TOPIC – Soviet glasnot-perestoika ('openness' of news & decentralized economic controls) signaled fall of Soviet Union, relate to social media revolutions & US security state policy guiding international policy towards deregulation – from *Capital Ungoverned*]

"In the authoritarian system media are depicted as a mouthpiece to disseminate the leadership's propaganda… For example, Soviet leaders predictably used state-controlled media to shape the coverage of Afghanistan in a way so pervasive that Soviet media did not even acknowledge the presence of Soviet combat troops in Afghanistan for five and a half years."[661]
"in both cases [US in Vietnam and USSR in Afghanistan] concern for the superpower's reputation was more important for convincing domestic audiences than it was for convincing international adversaries." (rosellle, 2)
"Factors related to communication itself include the role of television, access to media, technique in crafting message, and news values; each of these shape how leaders explain or frame withdrawal from a failed war."(roselle, 8).
"Certainly prior to glasnot, Soviet leaders were less concerned with policy legitimacy than with policy acquiescence and compliance… Krushchev, for example, set the agenda, made decisions with a small group of advisors (often cutting the military establishment out of foreign policy

[660] U.S. Senate Select Committee on Intelligence. "New Reports Shed Light on Internet Research Agency's Social Media Tactics". *Press Release of Intelligence Committee.* 17 December 2018.
[661] Roselle, Laura. *Media and the Politics of Failure: Great powers, communication strategies, and military defeats.* Palgrave Macmillian. Series in International Political Communication. 2006, p. 2.

decisions), and used the media to inform citizens and elites alike about new policies."(roselle, 10)
"Glasnot - a term used to designate a different approach to information and ideas, meant openness, publicity, and coverage of events and issues in the mass media that were previously taboo…prior to glasnot, the centralized control of mass media severely limited both critiques of Soviet policy and the ability of citizens to know of and comment on such conversations. Greater coverage of the issues confronting Soviet society opened the space available for discourse and allowed a larger number of people to participate. Glasnot called ordinary citizens to active participation in discussions of problems and policies, both in the domestic arena and in foreign affairs, at least in theory… Glasnot was a means by which people could also serve as a power base for Gorbachev against entrenched political interests opposed to change."(roselle, 11).

+ quote ~Glasnot originally term from 19th century Great Game era, preceded fall of USSR

The Glasnot-Perestoika reforms of the Soviet Union related to *Capital Ungoverned* thesis: "Seeking to bring the Soviet Union up to economic par with capitalist countries such as Germany, Japan, and the United States, **Gorbachev decentralized economic controls** and encouraged enterprises to become self-financing."[662]
[TOPIC- *glasnot,* military and GNP]
"[In 1990] *Glasnot* in Moscow has elicited comments from Russian economists that the Soviet economy was neither as large nor as efficient as previously thought in the West. The effect was to indicate that Russian military spending consumed over 20 percent of GNP, rather than 14-15 percent. Interestingly enough, a similar examination of the U.S. military budget would reveal that, including interest on the national debt (largely a result of defense spending, especially since 1980), the Veterans' Administration, and NASA support of military operations, the U.S. military spending goes from 6-7 percent of GNP to over 10 percent."[663]

News and all media are presented as an accurate reflection of reality to viewers, by virtue of the news genre. Truth and priority are expected to be identifiable by the genre. Viewers do not assume the underlying reality reflected in news or other media to be constructed events floated by viewers precisely because they are unassuming participants in a constructed scenario.

Nor should broadcastship intentionally border on pure fictions presented to create terrorized reactions, similar to the effect created by Orson Welles' *War of the Worlds* radio broadcast on the evening of October 30, 1938. Media do, however, treat viewers as paying test subjects for government policy decisionmakers.

As RAND wargame analyst Elizabeth Bartels writes on consensual participation in wargames by experienced politicians,

> For decisionmakers with limited wargaming experience, this can be a daunting challenge. Wargames can be deceptively simple — many do not even use complicated computer models — so it is all too easy to assume that no specialized skills are needed for success. At the same

662 https://www.britannica.com/topic/perestroika-Soviet-government-policy
663 Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You're Not Supposed to Know*. William Morrow and Company, Inc. 1990, p. 345.

> time, wargames are hugely diverse: interagency decisionmaking seminars that involve conflict without fighting, crisis simulations adjudicated by subject matter experts, and operational warfare in which outcomes are determined by complex computer models. For sponsors who may have only seen one or two games, it can be hard to understand the full range of wargaming possibilities and the common approaches that underpin them all.[664]

Manipulation of the presentation of facts and the presentation of false information as true to elicit genuine responses, not only constitutes social engineering and a predatory state, but also constitutes non-consensual human experimentation - a felony and crime against humanity. "One way to understand why and how leaders communicate during war involves deterrence theory. Deterrence theory, 'in its most general form,... is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits… deterrence theory… assumes that states are - and should be - terribly concerned about their reputations for living up to their commitments… what is striking then, about many occasions when officials acted to maintain the U.S.'s image for purposes of deterrence is that the target has often been friends and allies as much as opponents."[665]

Deterrence theory applies to media usage in the CNN effect. As exemplified in the effects of *glasnot*, media are often allied and adversarial to government, using their control of popular opinion, and increasingly of operational systems of electronic warfare to act as a fourth branch competing within government.

As I point out in the VNN Effect, the populace is completely left out of the understanding of deterrence strategy in media; the viewership is the object of persuasion and, therefore, deterrence. This does not reflect all broadcast-viewership relations, but certainly applies to those in which the broadcastship has the legitimate right to use violence against the viewership, and has the exclusive right to represent or not represent power structures or outright violence as they truly exist.

This creates between media and government an unstated mutual interest to protect their collective methods of control from third party infringement. It also creates between the two parties the incentive to gain greater influence over one another's principal method of control – the viewership.

+[Infringement - government infringement in the media industries, and media/technologists' right to infringement in government, and the exclusion of all third parties, and one another, by exercising their monopoly on violence.]

Within the framework of realism, industry power struggles for end-to-end control of the three domains necessary to war - public opinion, technology, and policy - is a main cause of both state persecution of journalists and media antagonism towards politicians. However, as both already have major monopolies on public opinion, technology and policy, they share the mutual interest to not further divide their own monopolies nor to increase the number or variety of opponents in the power struggle.

---

[664] https://www.rand.org/blog/2016/01/getting-the-most-out-of-your-wargame-practical-advice.html
[665] Roselle, 12-13.

Since the fall of the Soviet Union, which coincided with Gorbachev's *glasnot* - more or less the democratization of news information - and the rise of transnational media, we have seen the super states and media become the major superpowers vying for power and profit around the world.

The media acting as a clan vying for supremacy within the "tribe"[666], as Michelle Betz, a US journalist and media consultant who was convicted in absentia of illegally operating in Egypt in 2011, says when she writes, "they [the Egyptian government] didn't realise that there is a tribe in journalism."[667] Media more often than not represent the interests of the country in which they are based, but they may also challenge national power structures, and all parties do take part in proxy wars. The fact that her story is retold by *al-Jazeera*, media from an Arab culture based on literal tribes that make up a modern nation state, demonstrates the farcical layering in modern power struggles. In the case of the Arab Spring, we see the power struggle for monopolies on violence and infringement between government and media extend to other segments of the globe, exemplified in hacktivism.

Part of the cult of personality and power that hackers are promoted by is people believing the knowledge of hacking to be something extraordinary. Many chroniclers of 'hacks', meaning cybercrimes, display those beliefs in their writing and accept the vile character of hackers as something that must be tolerated from people who read metadata and learn to copy and paste text strings into command windows. In reality, hackers do very little action in their criminal enterprises, with even less excitement surrounding them.

H**acking is predominantly social engineering - which is why the almost ironic impression others have of hacking culture is so important to foster, despite the obvious lame reality. Point-and-click level computer misusage does not garner reputation for excitement without serious propaganda efforts.**

Hackers are not 'underdogs' prevailing virtually over stringent authority they are portrayed to be. Hacking companies, like The Hacking Team, are on the payroll of the federal government, are given immunity to commit cybercrime, and are hosted virtually by federal government agencies to hack private, corporate and sovereign systems.

These individuals are so state-sponsored they are even featured in former President Bill Clinton's 2018 novel *The President Is Missing*, a cyber thriller in which state-sanctioned ('white hat') hackers and a fictitious US president work together on national security threats. Unfortunately, it is not only in speculative fiction born of the imagination of retired octogenarian politicians in which hacking is a locus of excitement and heroism veiled in intrigue. Such portrayals and federal support are crucially **important for the success of hacking by social engineering.**

+ADD Boosting queries, pushing notifications, promoting tweets and trending topics, targeted advertising of sedition and civil strife. In an interesting ambiguity resultant in the US between democracy and capitalism, such techniques are used legally on private platforms to promote

---

666 Betz, Michelle. "Justice in Egypt: My so-called 'trial'". 23 June 2014. *Index On Censorship*.

667 Betz, Michelle. "Justice in Egypt: My so-called 'trial'". 23 June 2014. *Index On Censorship*.

capitalism, for example for commercial advertising and spending, but in this case the same techniques are repurposed and justified as promoting 'democracy'. [+ADD SQL Defense book]

These techniques are not only forced on users of platforms for advertising regular commercial purposes, but they are regularly used by hackers like Anonymous, for example in their 2008 'operation' in which "the Anon [Anonymous member] claimed to have found 'a bunch of' XSS vulnerabilities on Scientology.org. XSS, or cross-site scripting, was said to be the second most common hacking technique after SQL injection."[668] The malicious result of both platforms and hackers using these techniques is the resulting ambiguity in who is causing the alterations to effect social engineering. The ambiguity is increased due to the fact that internal members of tech companies are hackers (criminal technologists) as well as employees.
+ADD Army Bennett Arab Spring a RAND Corp. product

Further supporting the role unbalanced influence played in the Twitter Revolutions is the use of American cultural turns of phrase used to advertise about the revolutions. Referencing "the digital dimension that produced slogans such as 'the revolution will be tweeted' and 'democracy is just a tweet away'"[669], which was also used in real-time by *The New Yorker, New Scientist, The Atlantic, VICE, The Guardian,* books and visual media coverage of the Arab Spring protests.

As many young Americans are unaware, many young Arabs would be unaware that "The Revolution Will Be Tweeted" is a derivation on an American song released in 1970 titled "The Revolution Will Not Be Televised" by Gil Scott-Heron, which *The Guardian* claims was played at the highly televised center of Egypt's Tahrir Square as the revolution was being tweeted under the hashtag #therevolutionwillbetweeted. [670]

It is highly unlikely that such a slogan was fully culturally understood by Arabic-speakers, and less likely that it was produced by Arabic-speakers. It is even less likely that it was produced for mass consumption by Arabic-speakers. The conclusion can be no other than that such slogans for Arab revolutions were produced by Americans for Americans in order to encourage American participation in foreign revolutionary coups. "Democracy Is Just A Tweet Away" is also word play on a common English refrain.

"The art of world-making entails the development of complex audiovisual and textual storytelling based on the repetition and redundancy of aesthetic items, such as symbolic images, songs or soundtracks, and textual references or characters, which provide the users with a coherent imaginary world among different media platforms… They provide the audience of believers with the fundamental key of interpretation and sense of engagement based on the common faith. In this sense, they are semantic triggers, which lead the readers to additive comprehension across the transmedia story world."[671]

---

[668] Olson. *We Are Anonymous,* p. 68.
[669] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution", p. 185.
[670] Lester, Paul. "Gil Scott-Heron: the revolution lives on". *The Guardian*. 26 August 2015. Internet resource.
[671] Monaci, Sarah. "Explaining the Islamic State's Online Media Strategy: A Transmedia Approach". *International Journal of Communication,* Vol. 11. 2017, p. 2848; 2855.

Since the assassination of Egypt's president Anwar al-Sadat in 1981, it has been unusual to deal with social movements of the Middle East within the pan-Arabist paradigm, and many experts trained since have only done so in historical contexts. Definitely, since the US execution of Saddam Hussein and the violent expulsion of Ba'athists there by US forces, pan-Arabists have had no growing political appeal. This paradigm is another highly unusual aspect of the Arab Spring.

Transition :"Media scholar David Jay Bolter (Bolter & Grusin, 2002) introduced his book *Remediation* with a reflection on the events of 9/11, describing how, for the first time in history, an audience could watch that dramatic show of terror and despair on the Web. Millions of people witnessed what was later called the most horrific show in the history of contemporary live media."[672]

The CNN effect according to Steven Livingston's definition is "the impact of new global real-time media on diplomacy and foreign policy" acting as "as an accelerant of policy, an impediment to it, and a policy agenda setter."[673] "Under this scenario, failure to react in a timely manner creates an image of aloofness and even irresponsibility for governments".[674]

& "But older technologies likely played an even bigger part in the transmission process: Al Jazeera and other Arab language satellite TV channels conveyed emotions of the crowds in real time. Text messages through ubiquitous (and anonymous) pay-as-you-go cellphones reached thousands in minutes. In Syria and Yemen, cellphone cameras—coupled to YouTube—ensured the sights and sounds of repression were seen despite efforts of governments to prevent it."[675]

& "the CNN effect can be an impediment relates to breaches in operational security that may occur from the transmission of sensitive information"(9) & As a policy agenda setter, the meaning is obvious, taking into account that it is a for-profit industry that sells the new or repackaged which gravitates to visualizations of great human suffering whether or not it is a topic of national interest.

As Bahador puts it, "Foreign policy, however, does not and cannot function in this manner... If foreign policy is to follow the agenda set by media, it will increasingly be forced to engage in a variety of theatres, only to shift resources abruptly once that situation becomes less fashionable." The "policy-media interaction model" demonstrates its ability to change a policy of nonintervention in the case of the 1991 Gulf War media coverage of the Kurdish crisis which appeared to expose the suffering caused by a lack of policy intervention in Iraq.[676]

Interestingly, following that change in a policy of non-intervention, the 1991 Gulf War became the first global event to be exclusively covered by CNN for the initial two weeks due to electrical outages caused by aerial bombings of Baghdad which CNN alone was technologically

---

[672] Monaci, Sarah. "Explaining the Islamic State's Online Media Strategy: A Transmedia Approach". *International Journal of Communication,* Vol. 11. 2017, p. 2842.
[673] Bahador, *The CNN Effect in Action,* p. 4, 7.
[674] Bahador, *The CNN Effect in Action,* p. 7.
[675] Ries, Charles P. "The Year of the Arab Spring". *The RAND Blog*. 20 December 2011. Internet resource.
[676] Bahador, p. 10-11.

prepared to circumvent, resulting in a significant subscription increase over the duration of the war.[677]

As quoted in "Explaining the Islamic State's Online Media Strategy", scholar Weimann found that, "In 1998, fewer than half of the groups designated as foreign terrorist organizations by the U.S. State Department maintained websites; by the end of 1999, nearly all these terrorist groups had established their presence online".[678]

If the statement is taken as true that "all state-media relations can be reduced to propaganda,"[679] the question remaining to be asked is, propaganda benefiting whom?

The Arab Spring has been very destructive and in other cases completely ineffectual. [Those countries hit hardest by the after-effects of the Arab Spring vs. Bahrain, Saudi Arabia, Tunisia, Egypt, Jordan.] As the RAND Corporation proclaimed in December 2011:

> Violence against Copts in Egypt, Sunni-Alawite-Kurdish tensions in Syria, Sunni-Shia rivalries in Bahrain, and the caldron of sectarian and tribal struggles in Yemen are evidence of the re-emergence of ancient suspicions at a time of rapid change. In Libya, regional and tribal rivalries must be reconciled in order to construct a viable state. In Egypt, the military, which seemed to be a hero of Tahrir Square for pushing Mubarak aside, of late has been reluctant to concede power… Israel will need to re-think its relationships with its neighbors.[680]

"Leon Panetta served as U.S. secretary of Defense, CIA director, White House chief of staff, and member of Congress. Jeremy Bash served as Secretary Panetta's chief of staff at DoD and CIA: 'In signing historic peace agreements with Israel this week, the leaders of the United Arab Emirates and Bahrain are showing immense courage. Those leaders have long ago concluded that the Jewish State of Israel did not need to be feared in the Middle East, but that there were forces — extremist Shia elements and extremist Sunni elements — that ought to be feared and confronted… Both of these elements resort to terrorism and violence to achieve their objectives. And both pose direct threats to U.S. forces, our allies such as Israel, Egypt, and Jordan, as well as our key Gulf partners. In short, the countries of the Gulf and Israel have a common set of fears and thus a common sense of courage that will allow them to reshape the modern Middle East… For these agreements to remain strong and permanent, Saudi Arabia should also make peace with Israel.'"[681]

According to Brookings Institute analyst Federica Saini Fasanotti, Libya "is not a real state... Libya has never been a state since the Ottoman empire. So, not a state in those times, not a real state during the Italians, and with Gaddafi was a strange state as well because of not investing in anything." Her co-analyst moderating, also from Brookings, concurs saying, "Libya

---

[677] Bahador, p. 3.
[678] Monaci, p. 2842.
[679] Bahador, p. 11.
[680] Ries, Charles P. "The Year of the Arab Spring".
[681] https://thehill.com/opinion/international/516833-leon-panetta-this-is-what-courage-looks-like-in-the-middle-east

is in a strange place where even though it doesn't really have a state, it does now have a fair amount of oil revenue coming back."[682]
+ADD failed state discussion from [PRINTED]
https://journals.sagepub.com/doi/pdf/10.1177/0192512113480054 Fragile and Failed States
https://doi.org/10.1111/j.1468-2486.2007.00728.x Failed States and Global Security, Stewart Patrick

The claim that Libya has never been a real state as recognized by US policy is easily contradicted, as the United States had an ambassador appointed to Libya working under the auspices of the State Department leading up to 2011. Ambassador Christopher Stephens' torture, rape and murder, along with three other US staff, were filmed and electronically distributed following the September 11, 2011 Benghazi attacks on the US Embassy and CIA annex.

In addition to this fact, US policy recognition of Libyan statehood is evidenced in the US recognition of the African Union. Muammar Ghaddafi was responsible for the founding of the African Union, a state-like institution similar to the European Union that encompasses and extends beyond Libya's borders.

+Gold standard not likely a money Islamic State traded in (oil, meaning dollar, and cryptocurrencies), reason some say for Gaddafi and Saddam's fall at NATO hands.[683] "Issue 11 of Dabiq (August–September 2015/1436) shows a more complex synergistic storytelling strategy that develops around the video *The Dark Rise of Banknotes and the Return of the Gold Dinar* presented as the incipit of the magazine. The video is introduced in a full page along with the English hashtag #return_of_the_gold_dinar and is available online in a short version produced by Al-Furqan Media and a long version branded by Al-Hayat." The article written in IS magazine by John Cantlie, a British photojournalist who was kidnapped by unknown fighters along with journalist James Foley in 2012. + more on Cantlie https://en.wikipedia.org/wiki/John_Cantlie "Cantlie's role is supporting, with detailed arguments and in a journalistic style that differs entirely from the doctrinal tone of Dabiq articles, some key issues of IS reports against Western countries. He is the IS spokesperson who appeals to the United States and the United Kingdom to pay ransom for hostages, as appears in Dabiq 4, in an article published after James Foley's execution, or also in the articles "If I Were the U.S. President Today" (Dabiq 5) and "Paradigm Shift" (Dabiq 8) in which he claims a change of attitude toward IS should be considered by his enemies as a legitimate state and not just a terrorist organization."[684]

(Saudi Arabia not addressed in lit?) video"Saudi Arabia *escaped* the Arab Spring."[685] With obvious geopolitical importance, note the only Arab countries that 'escaped' the Arab Spring are

---

[682] The Brookings Institution. "Middle East Crises and Conflicts - The Way Ahead". Washington, D.C. 5 October 2017. Transcript.
[683] https://onlinelibrary.wiley.com/doi/full/10.1111/mepo.12310 ; https://theecologist.org/2016/mar/14/why-qaddafi-had-go-african-gold-oil-and-challenge-monetary-imperialism ; https://www.iol.co.za/pretoria-news/dont-dare-dump-the-dollar-15264019
[684] Monaci, p. 2850; 2855.
[685] https://youtu.be/fS6xpmg-3u4?t=2843 Kingdom Come or Kingdom Gone? Saudi Arabia and the Future of the Middle East 47:30

close US allies in the Gulf and other "more friendly countries like Morocco and Jordan" (training activists article). Another country outside of the Arab World which also experienced a dramatic rise in protests spurred by Twitter protests in early spring of 2011 is Venezuela.[686] Venezuela's "Twitter revolution" leader Leopoldo Lopez, an anti-oppostion politician, was arrested with terrorism charges later in 2014.[687] The only apparent commonality Venezuela shares with the Arab Spring countries is that it is also a member of OPEC.

+Twitter in arab spring articles.

"The essential analytical starting point for the explanation of empire lies in the relationship between a metropole and a periphery, the latter penetrated by transnational forces and actors. Three essential conditions for the establishment of an imperial relationship can be conceived of as thresholds for a metropole, for transnational penetration, and for a periphery… The extension from the metropole of economic and sociocultural or ideological forces and the institutions that carry them provide both an incentive for metropolitan interference in peripheral politics and a means of penetrating the domestic society of the periphery. In these extensions peripheral elites find sources both of transnational, imperial loyalty (religion, ideological affinities) and of more material payments for their allegiance. Extensions are thus – from the metropolitan side – sources of considerable power over the periphery. Indeed, it is the substantial degree of power that transnational extensions can generate over the internal policy of the periphery that distinguishes empire from the lesser influence of hegemony."[688] This is achieved via social engineering.

"Social media's enhanced influence was also a result of explicit strategies on the part of Internet activists, who targeted satellite and independent news organizations as a means of spreading their message and controlling the narrative of the revolution. As a result of satellite television's reliance on social media and activists' outreach strategies, it is impossible to untangle the independent impact of broadcast media from social media."[689]

Content and Platform Providers

There's one company now you can sign up and you can get a movie delivered to your house daily by delivery service. Okay? And currently it comes to your house, it gets put in the mailbox when you get home and you change your order but you pay for that, right? But this service is now going to go through the internet, and what you do is you just go to a place on the internet and you order your movie, and guess what? You can order ten of them delivered

---

[686] "Venezuela". *Freedom in the World.* Freedom House. 2012.

[687] Friedman, Uri. "Why Venezuela's Revolution Will Be Tweeted The country's street protests are playing out dramatically on the social network." *The Atlantic.* 19 February 2014.

[688] Doyle, Michael W. *Empires.* Cornell University Press. 1986, p. 129.

[689] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. The RAND Corporation. 2013, p. 54.

to you and the delivery charge is free. Ten of them streaming across that internet and what happens to your own personal internet? [690]
Senator Ted Stevens

In this section I show examples in which the full spectrum of the American ICT industry had to be aware and highly involved in the activities that led to the Arab Spring. "Such a connection is critical for the CNN effect, because it is important not only to demonstrate that the policy changed after such events, but to also link the policy change to the media images and framing of the events."[691] [REWORD]
"Increasingly, algorithms invisibly shape our realities and guide our decisions**. In the laissez-faire model, these algorithms are profit-driven. In the authoritarian model, they are control-driven.** Neither is good for democracy."[692]

+ADD "suppressing content […] is itself a tactic of manipulation. Authoritarian information manipulation tactics include building online information platforms to censor speech,… pressuring private sector actors such as the NBA to present information according to specific narratives; or coordinating activity of inauthentic social media accounts to amplify information… Focusing on countering the underlying behavior of actors engaged in malicious activity takes a more systemic approach to countering information manipulation than focusing on content… Whereas an authoritarian approach would censor speech by subject matter and, in some cases, imprison those responsible, democratic actors should look to expose and remove coordinated deception on the part of state and non-state actors."[693]

+ADD "**YouTube** has also tried to secure its platform from foreign actors. Last week, the company said it banned almost 2,600 channels linked to China as part of investigations into **"coordinated influence operations" on the site**. YouTube also took down dozens of channels linked to Russia and Iran that had apparent ties to influence campaigns. Google on Thursday said it will give people more information on who's behind the political advertisements that run on Google and YouTube. The **company's political ad transparency report, which Google first started releasing two years ago [2018]**, will include new ways to sort campaign spending."[694]
+ADD [Relate Act to ISIS sex slave trade and its proliferation on US-regulated Internet with third party oversight] ""Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020" https://www.theverge.com/2020/1/31/21116788/earn-it-act-section-230-lindsey-graham-draft-bill-encryption ;

---

[690] Wired Staff. "Your Own Personal Internet". *Wired Magazine*. 30 June 2006.
[691] Bahador, p. 35.
[692] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 80.
[693] Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest". *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs, p. 82.
[694] Nieva, Richard. "YouTube bans videos containing hacked information that could interfere with the election". *CNET*. 13 August 2020.

"(b) Purpose.—The purpose of the Commission is to develop recommended best practices that providers of interactive computer services **may choose to implement**… SEC 4(a.1.A) that providers of interactive computer services **may choose to engage in** to prevent, reduce, and respond to the online sexual exploitation of children, including the enticement, grooming, sex trafficking, and sexual abuse of children and the proliferation of online child sexual abuse material… (B.i) Alternative Best Practices… shall take into consideration - (I) the size, type of product, and business model of a provider of an interactive computer service; (II) whether an interactive computer service— (aa) is made available to the public; (bb) is primarily responsible for the transmission and storage of information on behalf of other interactive computer services; or (cc) provides the capability to transmit data to and receive data from all or substantially all internet endpoints on behalf of a consumer; and
(III) **whether a type of product, business model, product design, or other factors related to the provision of an interactive computer service could make a product or service susceptible to the use and facilitation of online child sexual exploitation…** (3.B-C, I, K) Matters Addressed…(B) coordinating with **non-profit organizations** and other providers of interactive computer services **to preserve**, remove from view, and report child sexual exploitation; (C) **retaining child sexual exploitation content and** related user identification and location data [OPPOSITE OF EU 'RIGHT TO BE FORGOTTEN' LAWS];… (I) **employing age rating** and age gating **systems** to reduce child sexual exploitation;… (K) contractual and **operational practices to ensure third parties, contractors, and affiliates comply** with the best practices… (b.1.A) Publication of Best Practices… **upon agreement with the Secretary of Homeland Security and the Chairman of the Federal Trade Commission**, shall— (A) approve or deny the recommended best practices"[695]
+ADD "Attorney General William P. Barr has told people close to President Trump — both inside and outside the White House — that **he is considering quitting over Trump's tweets about Justice Department investigations**, three administration officials said, foreshadowing a possible confrontation between the president and his attorney general **over the independence of the Justice Department.** Barr publicly warned the president in a remarkable interview with ABC News that **his tweets about Justice Department cases 'make it impossible for me to do my job**.'"[696]

As researcher Monaci notes, "to date, few contributions have focused on media strategy used by IS and how it exploits different media platforms, audiovisual contents, and synergies among various media assets to enhance its messages. IS propaganda has been quite simply defined as "multidimensional" (Ingram, 2015, p. 730) or as a "mix of techniques at the crossroad between moviemaking and videogames" (Maggioni & Magri, 2015, p. 87)."
+ADD compare to Army posture on speculative fiction and DoD modeling and simulation

---

[695] https://www.congress.gov/bill/116th-congress/senate-bill/3398/text
[696] https://www.washingtonpost.com/politics/trump-raises-possibility-of-suing-those-involved-in-prosecuting-roger-stone/2020/02/18/238279fc-5250-11ea-9e47-59804be1dcfb_story.html

"Stern and Berger (2015) analyzed how IS strategically used Twitter between April and June 2014 with the application "The Dawn of Glad Tidings," which enabled its users to receive up-to-date news about IS progress. The application could also take control of a consenting user's account to automatically send out tweets. Prominent official IS members and supporters signed up for and formally endorsed the app as a trusted and official source of news. The Dawn of Glad Tidings automatically sent out links to official IS news releases and media, and hashtags that the ISIS social media team wanted to promote. Although the application had been suspended by Twitter at the end of Summer 2014, the number of pro-IS accounts in 2014 and 2015 remained significant, further enriched by thousands of bots (i.e., computer software pieces that act like actual Twitter users) tweeting and retweeting specific contents. Those bots were particularly active, for example, in retweeting IS official propaganda messages, such as the videos of beheadings and the video *Flames of War* released in September 2014 by Al-Hayat."[697]

Twitter, Inc. is an American company based in California. Its "products and services" include Twitter as well as "Promoted Tweets, Promoted Accounts and Promoted Trends". Twitter and accompanying services are described as "a platform and information database" designed to "provide targeting capabilities based on audience attributes, such as geography, interests, keyword, television conversation, content, event and devices that make it possible for advertisers to promote their brands, products and services, amplify their visibility and reach, and complement and extend the conversation around their advertising campaigns".[698] Facebook, Inc. is also an American company based in California that describes itself similarly as a communication platform and database that "also engages in selling" third parties access to "reach people based on a range of factors, including age, gender, location, interests and behaviors" in "algorithmically-ranked series of stories and advertisements individualized for each person".[699] This is the long way of stating that merely through virtue of these companies' business models, government agencies and other companies invested in, say, direct war-profiteering are granted legitimate access as third party advertisers to "complement and extend the conversation around their advertising campaigns", even if it is war or coup campaigning, in the locations and to the people of their choosing.

"ISIS further developed the Al Hayat Media Center, a sophisticated media platform specifically aimed at non-Arabic speakers, particularly young Muslims."[700] "The new magazine mirrors the former in terms of structure and content type; both are produced and released online by Al-Hayat Media Network. Along with videos and magazines released by a media organization based on the main Al-Hayat hub, a significant propaganda flow stems from social media accounts on Twitter, Facebook, Telegram, among others."[701] Unfortunately, the sources do not explain why or how ISIS was able to use the name of a major mainstream Saudi-owned Arabic

---

[697] Monaci, p. 2843-2844.
[698] "Profile: Twitter Inc (TWTR.N)". *Reuters*. Accessed 31 July 2019. Internet resource.
[699] "Profile: Facebook Inc (FB.O)". *Reuters.* Accessed 31 July 2019. Internet resource.
[700] Boms, "New Media", p. 199.
[701] Monaci, p. 2843.

language newspaper based out of London, *Al-Hayat*. Both news sources Al-Hayat vied for the same audience, the Arabic-speaking diaspora in Europe.

+"Both fiction, such as the Hollywood movies cited, and nonfiction transmedia products have a tendency to maintain internal linear consistency in all media platforms, such as the movie, the video game, or the online video. At the same time, they exploit each media content through social network sites that allow the audience to interact with the main content (e.g., through hashtags) without altering its own particular linearity or consistency. According to transmedia strategies, the IS house organ Dabiq, by means of hashtags and online videos promoted in the magazine, provides further content and media platforms with which individuals can interact. Starting from a particular element of the narration presented in the magazine (e.g., hashtags or as link to a video), IS could enrich, multiply, and spread different posts related more or less closely to the main one. That was also the main strategy deployed by the application The Dawn of Glad Tidings, which had the specific role of amplifying the reach of messages spread by Twitter."[702]

A Google executive in Dubai, Egyptian Wael Ghonim created the Facebook page in summer 2010 to raise awareness of police brutality against youth called "We Are All Khaled Said". RAND analysts point out this resulted in an 100% increase in Google searches of search term "Khaled Said", "followed by incremental measures aimed at defining the group and its common beliefs, identifying who was responsible (Mubarak and the police) and finally, presenting opportunities for users to channel their outrage through collective political action." The group had gained momentum over the six months preceding the Arab Spring protests in Egypt with half a million members.[703]

By "slowly introducing an activist prism through which to view events in Egypt, "We Are All Khaled Said" had greater success in politicizing the members it reached" compared to the April 6 Movement (a then-current strike by industrial workers, named in reference to an infamous instance of British violence against Egyptian police in colonial Egypt). The April 6 Movement group was started on Facebook by a local Egyptian female student. When she was arrested, she claimed she was surprised by the sudden following her group had gained online - 70,000 members in two weeks. She was forced to publicly recant her political views in order to be released from detention.[704]

Ghonim, who had been granted leave by Google to travel to Egypt during the uprising, was arrested and detained for eleven days after arriving in Egypt to join in on protests. He was then released to give a teary television interview in which he celebrated protesters, and was free to join in on the protests taking place in Tahrir Square.[705] Ghonim has since been awarded the JFK Profile in Courage Award in 2011, listed in TIME Magazine's Top 100 Influential People

---

[702] Monaci, p. 2847.

[703] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. The RAND Corporation. 2013, p. 60-61.

[704] Boms, 195.

[705] The Editors of Encyclopaedia Britannica. "Wael Ghonim: Egyptian Activist and Computer Engineer". *Encyclopaedia Britannica, Inc.* 19 December 2018.

edition 2011, nominated for a Nobel Peace Prize in 2011, and more recently awarded a non-resident fellowship at Harvard University's Democratic Governance Center.[706]

Max Weber: "'sterile excitation,'…It is an excitation that plays so great a part with our intellectuals in this carnival we decorate with the proud name of 'revolution.'"[707]

Many other Arab protest leaders not directly working for American tech companies were otherwise trained specifically in "campaigning, organizing through new media tools and monitoring elections". Through institutes connected by a 1983 Congressional endowment of $100 million annually administrated by the US Republican and Democratic Parties, the US State Department, the International Republican Institute, the National Democratic Institute for International Affairs and Freedom House held technology training sessions sponsored by Facebook, Google, MTV, Columbia Law School, Project on Middle East Democracy and other NGOs beginning in 2008 in order to train Arab youth in social media protest methods.

These leaders included Bashem Fathy and Bassem Samir of Egypt, Oraib al-Rantawi of Jordan and Entsar Qadhi of Yemen and other leading members of the April 6 Youth Movement, the Egyptian Democratic Academy, the Bahrain Center for Human Rights, and other activist groups from Jordan and Morocco who, in their own testimonials say they "learned how to organize and build coalitions. This certainly helped during the revolution," and "All these efforts, by local and international organizations, paved the way for what's going on today." In fact, more than 10,000 Egyptians were trained in similar programs held by USAID alone. Some members are quoted as being rightly suspicious, recognizing that the organizations training the protesters were also providing training for the Arab states' security investigative services who the protesters were allegedly being trained to subvert. Eventually, the Egyptian government made meeting for the training sessions physically impossible and conducted investigations into meeting members. Meanwhile, many members went on undisturbed to successfully organize a coup against the then-current regime in Egypt. As Jordanian activist al-Rantawi put it, "These youths didn't come from nowhere and make a revolution."[708]

Al-Jazeera, ostensibly in support of their own employees imprisoned in Egypt, reported in a 2017 article titled "Interpol: Red Alert!" on the story of Michelle Betz, a US journalist and media consultant who was convicted in absentia with illegally operating in Egypt in 2011 under a US NGO. Through a process with the Commission for the Control of Interpol's Files (CCF) she describes as "completely Kafkaesque", she was later able to remove her name from Interpol's red-flag list that is distributed internationally to law enforcement. Betz, in her own narrative, states that she was also convicted of bringing foreign funds into the country. In a

---

[706] "Wael Ghonim". *Harvard Kennedy School Ash Center for Democratic Governance and Education.* Accessed 5 August 2019.

[707] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958, p. 115.

[708] Nixon, Ron. "U.S. Groups Helped Nurture Arab Uprisings". *The New York Times*. 14 April 2011. Electronic resource.

statement that could be described as completely Shylock-esque, the article goes on to quote a Dutch lawyer representing a similar case against Azerbaijan, appraising the CCF as "Completely ineffective. It's a joke."[709] Indeed, Betz writes that "the NGOs, the US State Department, the lawyers - all tried to assure us that this was all political (between the US and Egypt) and that this would 'all go away'... Just as with the Al Jazeera case, logically, it never should have happened." She also describes another American and several Egyptians working for the NGO who were taken into the US Embassy in Cairo who "then finally flew them out in the middle of the night after some backroom deal was worked out with Egyptian officials." Betz adds that on the official Egyptian document charge the "Judicial officials didn't even have my full name," which would be the case if she was in fact was not operating in Egypt legally. She concludes posturing that "they [the Egyptian government] didn't realise that there is a tribe in journalism, which does not suffer injustice and attacks on its own... including injustices wrought on our tribe."[710] Perhaps the Arab Spring beginning in Tunisia was a subtle nod towards Ibn Khaldun's concept of *'asabiyya* by some sociologically savvy journalist tribe.

+ ADD TRANSITION

Analysts of the RAND Corporation write in 2013, despite the Muslim Brotherhood having won the democratic elections following the coup against Mubarak, that the earlier Muslim Brotherhood's uniting with liberal-secular *Kefaya* movements in 2004-2006 against succession of the Mubarak line did not have democracy as an ultimate goal either. The only "real existential threat to the Mubarak regime was the potential formation of a popular, liberal political movement with democracy as its primary objective. Such a movement's *raison d-etre* would be the removal of Mubarak." Of course, *rasion d-etre*,'ultimate goal' and 'primary objective' can be used interchangeably, yet RAND implies that the secular-Islamist unifying movement of 2004-06 which had removal of the Mubarak line as its ultimate goal did not do so to such an intrinsic degree that it could be called its *raison d-etre*. And it did fail in whatever it was trying to do or be, but when a democratic election ensued following the 2011 coup of Mubarak in which an Islamist party won, the response from the Western media was disappointment and confusion, especially when the polls reflected what could have been predicted in the 2004-06 movements.[711] Paradoxically, the military coup staged by the current Egyptian President al-Sisi in 2013 was accepted readily by US analysts as the natural consequence of what happens when a majority chooses wrong in a democracy.

"Naturally, with ego such a big driver of the early December [2010] attacks, discussions in #command soon broke down. After Civil, Switch [both server hosts to Anonymous IRCs and bot army managers], and the nine hundred people fruitlessly using LOIC hit Mastercard.com, the small group in #command decided, on a hubristic whim, to attack Amazon.com the next day, Deccember 9, at 10:00 a.m. eastern standard time. That's when the operators realized that Civil

---

[709] Spiller, Sarah and Callum Macrae. "Interpol: Red Alert!: How states have used Interpol alerts to persecute exiled dissidents and refugees across international borders". *Al-Jazeera*. 12 January 2017. Internet resource.
[710] Betz, Michelle. "Justice in Egypt: My so-called 'trial'". 23 June 2014. *Index On Censorship*. Internet resource.
[711] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. The RAND Corporation. 2013, p. 57.

and Switch had disappeared. The operators pushed the attack time to December 9 at 2:00 p.m., hoping the botmasters would return. At 1:30 p.m., the entire AnonOps IRC network went down. It turned out that Civil and Switch had been squabbling with some of the operators in #command and were now using their botnets to attack AnonOps in retribution. When the IRC network came back online about an hour later with a few hundred participants, nobody wanted to attack Amazon anymore. There weren't enough bots and there didn't seem to be a point."[712]
"Especially pertinent is the realisation 'that your average cyber attacker will be part of an organisation that is far closer to a corporate enterprise in its structure."[713]

"[the number of **pro-IS accounts in 2014 and 2015 remained significant, further enriched by thousands of bots** (i.e., computer software pieces that act like actual Twitter users) tweeting and retweeting specific contents. Those bots were particularly active, for example, in retweeting IS official propaganda messages]... The ISIS Twitter Census funded by Google carried out a study in partnership with the Center for Middle East Policy (U.S.) on Twitter profiles that supported the Islamic State during the period 2014–15. They analyzed 46,000 pro-IS profiles on Twitter between Syria and Iraq, and focused on 20,000 accounts to draw **a general demographic snapshot of Twitter's IS population**. Among the findings, the **researchers observed that much of IS's social media-based success can be attributed to a relatively small group of hyperactive users in the range of 500 to 2,000 accounts, which tweet in concentrated high-volume bursts."[714]**

+ADD "**Botnet armies** on Twitter and exploitation of Facebook are strongly suspected of fuelling so-called 'echo-chambers'… ensuring that public debate descends into a state of near emotive anarchy".[715]

In September 2019, the US Congress announced its intent to investigate platform providers Facebook, Twitter and Google for anti-trust violations. As is clear in the story of Ghonim, who continues to meddle in Egyptian politics, most recently by publicly shaming current Egyptian President al-Sisi whom Ghonim is apparently also dissatisfied with,[716] tech company employees are capriciously in bed with, and then deposing, politicians.

After receiving the job, Google's newest CEO Sundar Pichai was public celebrated on Twitter by Indian Prime Minister Modi,[717] who was elected for his Hindu nationalist stance to make India an entirely Hindu country and is known for inciting violence and purges against Muslims in India.

---

[712] CITE – *Many faces of Anonymous*
[713] Steed, p. 35 / Davey Winder "How Organised is Organised Cybercrime?" Raconteur 17 December 2017 https://www.raconteur.net/risk-management/how-organised-is-organised-cybercrime
[714] Monaci, p. 2844.
[715] Steed, p. 45.
[716] "Face of Egypt's 2011 revolution asks el-Sisi to repent in video: Wael Ghonim says the president should apologise to widow of Mohamed Morsi, Egypt's first democratically elected leader." *Al-Jazeera.* 11 September 2019.
[717] "PM Narendra Modi congratulates Google CEO Sundar Pichai on Twitter, others join in". 11 August 2015. *The Indian Express.* Electronic resource.

[+ADD Weber demagogue & businessman quotes] This sophomoric political idealism means tech leaders know just enough politics to be extremely dangerous, indicated by their political involvement taking the form of ordering government change and eliminating 'political rivals' by the same methods they order takeout food.

If Congress were truly holding investigations into anti-trust behavior, it would be forced to name the US Government and many other governments worldwide as partners in Google and Twitter's illegal competitor mergers, and the US government itself as object of corporate technology takeover. The fatal hubris of technologists to take over entire governments lies in their purist attempts to essentially replace all notions of government with point-and-click 'direct democracy', which can be completely corrupted, rigged and despotically ruled by even average programmers.

Direct democratists are typically extremist technologists who say, 'No more voting, no more police, no more trials, no more banks, no more representatives, no more paper mail or paper money, no more face-to-face identity politics. Everything is more direct, including democracy, online.' Direct democratists propose to be judge, jury, executioner, and messenger. In direct democratist utopia, technologists hold the only valuable knowledge, the keys to the city so to speak, and are able to lord over all others not part of the tech community who now represent a disabled and untouchable class. [+ADD Electronic Frontier Foundation 1998 manifest]

Sadly, most of their political ideas are not political but social values that are highly formed by being part of a well-paid group of usually young men with only technical educations. They may feel entitled to create social change to correct 'outdated' perceptions of their social inferiority, 'dork status' so to speak, and bring it in line with the high status they have come to recognize themselves with in the professional sphere. They are not willing to actually do the work of mastering political science or getting elected to political office because this would force them to moderitize and negotiate with political realities, instead of reacting vitriolically in personal attacks to what really are different social values and cultural ideas. Because they are not experienced or educated in politics, they can only rely on gut reactions and almost always take their own opinions as *the* moderate standard. Extremist technologists tend to become direct democratists when they desire to change the status quo, of even a far off place, that does not make sense within their belief system.

Although I have alleged that platform and content provider companies have worked in tandem with government entities like NATO, the Pentagon and the FBI to overthrow governments, I believe the endgame for technologists is to *replace* government functions. This can be seen already in government functions, for example in the FBI's exclusive means to report, ironically, cybercrime being an online mediated submission form, the IC3.
+ADD Pandemic Internet-only response

It is also evidenced in Amazon's bid to handle all Pentagon computing, data storage and retrieval, complicated by Amazon CEO Jeff Bezos' ownership of *The Washington Post*, which has definite political agendas that go beyond financial gain as well.[718]

Other evidence for this can be seen in Facebook's attempt to establish its own currency, the Libra, which of course is not legally sanctioned by consent of the governed and is a capital offense. The description of their cryptocurrency is also an example of exclusionary direct democratism, stating:

> Facebook won't fully control Libra, but instead get just a single vote in its governance like other founding members of the Libra Association including Visa, Uber and Andreessen Horowitz, ... Facebook's audacious bid to create a global digital currency that promotes financial inclusion for the unbanked actually has more privacy and decentralization built in than many expected. Instead of trying to dominate Libra's future or squeeze tons of cash out of it immediately, Facebook is instead playing the long-game by pulling payments into its online domain. Facebook's VP of blockchain, David Marcus, explained the company's motive and the tie-in with its core revenue source during a briefing at San Francisco's historic Mint building… it could be globally ignored by consumers who see it as too much hassle for too little reward, or too unfamiliar and limited in use to pull them into the modern financial landscape. Facebook has built a reputation for over-engineered, underused products. It will need all the help it can get if it wants to replace what's already in our pockets.[719]

The fact that Facebook plainly states that it is intending the Libra to attract transaction activity away from the US dollar is only further highlighted by the fact that the event was held a former federal mint. Essentially, Facebook plans to create a market of goods and services in the US (and abroad) which cannot be purchased with the US dollar (allegedly still good for all debts private and public) or any other national currency. The Libra will be controlled by direct voting from corporate shareholders, and it is probably assumed that the consumer's dollar spent is their vote cast, recreating a poll tax of sorts. Only, it's not a dollar, and it's not issued by an elected government.

It is a social media company offering to void, not to fill in a void within, existing social contracts between governments and governed. It is creating an alternative to national currency, creating corporate parallels to national economies, national voting processes, and therefore, to nationhood. Were governments were doing something to prevent the execution of plans like Facebook's Libra currency, the plans would be laughable in their reductionist approach to human civilization.

Social media companies make their wealth by 'data mining' people's life details; people are consumed by social media companies as raw earth is consumed by mining companies. People are not only the consumers of media platforms, they are the product.

"This not even applies to intelligence services, with the Amazon Web Services now openly advertising its Secret Region service, specifically designed to provide cloud solutions of

---

[718] https://fortune.com/2019/04/10/pentagon-jedi-project-amazon-microsoft-cloud-services/

[719] Constine, Josh. "Facebook announces Libra cryptocurrency: All you need to know. The use cases, technology and motive behind the new digital money". *Tech Crunch.* 18 June 2019.

information up to Top Secret level. Indeed, this Secret Region is the result of a $600 billion contract that Amazon won from the Central Intelligence Agency in 2013 to cater specifically to Top Secret cloud storage requirements."[720]

If I saw that these individuals and companies were making political decisions solely to benefit company profits or the country in which it is based, I would compare content platform providers to mercantilist colonial enterprises, like The East India Trading Company. [+ADD monopoly trial of East India Company?, or in Great Game section] However, I do not see enough evidence to suggest tech political activities are done entirely for market domination or entirely at the behest of any government. I believe it is done for domination over the political arena itself. That is, were it up to me, I would not only accuse these companies of crimes like those IBM committed in facilitating the European Holocaust but of plotting to undermine nearly all governments in the world, and of severe deprivations of liberty and self-determination of the citizens of any given country.

End Users

So you want to talk about the consumer? Let's talk about you and me. We use this internet to communicate and we aren't using it for commercial purposes. We aren't earning anything by going on that internet. Now I'm not saying you have to or you want to discriminate against those people. The regulatory approach is wrong. Your approach is regulatory in the sense that it says, 'No one can charge anyone for massively invading this world of the internet.' [721]
Senator Ted Stevens

With a black suited faceless figure in front of a laurel-crowned globe, its logo looks like that of an off-brand intelligence contractor. Its Wikipedia history page reads like an index of CIA coups and military operations: Operation Payback, Operation Oklahoma, Operation Cartel, Operation Tunisia, OpSaudi, OpISIS. To much expressed internal dismay, the group admits the FBI instigated and coordinated the Occupy Wall Street movement in 2011 through it, resulting in the arrests of many of its protesters.[722]

+ADD March 6, 2012: **"[US court documents] reveal an astonishing degree of co-operation between the FBI and its source [Hector Xavier Monsegur, known as 'Sabu'], who gave the bureau details of other hackers and advance notice of attacks – which the FBI then apparently allowed to happen. The FBI even provided its own servers for members of hacking collectives to use**… The FBI agent confirms the conference call under question did indeed take place, and believed information on **how to gain access had been gleaned from a previous email hack of the Irish police force**, the Garda. Two weeks later, [hacker] anonsacco got in touch with Sabu again through private chat. 'Hey mate. Would you like **a recording of a call between SOCA and the FBI** regarding anonymous and lulzsec?' he said. **'I think we need to hype it up. Let the feds think we have been recording their calls.' Sabu's responses are not recorded,** but the indictment says he agreed to receive **the file, which was then checked by**

[720] Steed, p. 20.
[721] Wired Staff. "Your Own Personal Internet". *Wired Magazine.*
[722] *The Hacker Wars*. United States: Phase4, 2015.

the FBI and found to indeed be a recording of the conference call. Five days later, the recording was posted online… A cache of more than 5m emails taken from an attack on the company's [Stratfor] servers in December 2011 is currently being **published by WikiLeaks, but** the indictment documents reveal that **straight after the attack, Sabu offered an FBI-owned server to store the cache – which was quickly accepted**… **This not only gave the FBI access to review or even potentially amend the cache**, but also an inside track on Anonymous' discussions on how to use the documents, and potentially – though not revealed within the files unsealed to date – conversations between Anonymous and WikiLeaks… **Sabu's online persona has been silent since the legal files have been unsealed, but had continued unabated until shortly before, with recent tweets angrily denouncing the federal government**."[723]

In the same year, the group was at the center of a geopolitical watershed of revolutions and coups across the Middle East and beyond.[724]

The trail of crumbs from the mostly failed Arab Spring movement and its results that lead directly to the cyber-social activities for which Anonymous took responsibility have found the media and academia nose-blind. Or, I will argue that Anonymous' broad proclamation "they are us, and we are them" is correct. [725]

This may explain the reluctance toward self-reporting by federal agents, media, academia and others responsible. Instead, we find critics lauding the assumed good intentions of Anonymous' activities, deeming them "democratizers". This in spite of that same appellation being given a few years earlier to the US military's 2003 invasion of Iraq.

In contrast to Arab governments' usual suspicions of foreign meddling and their very public crackdowns on Arab Spring protesters, it is surprising to note state-sponsored media Al-Jazeera's willingness to laud and practically vouch for the integrity of an American hacking collective's,[726] even publishing admissions of crimes from the group, in which the group is shocked and motivated to action by its own leaks and hand-holds its "contacts", walking its acolytes step-by-step through this "new activism" by distributing online and print instructions to reworking communications technology for revolutionary political ends.[727]

I believe that if the genre of the al-Jazeera article were not off-set by the seeming non-violent nature of the political crimes being claimed, it would resonate with more readers as reminiscent of one of Al-Jazeera's more unique genres and one that nearly got Qatar aerially bombed by the US in 2004[728] - that genre of broadcast Bin Laden and other extremist videos. This also resembles the state-sponsored terrorism genre of the 'instructive technological articles',

---

[723] https://www.theguardian.com/technology/2012/mar/06/lulzsec-court-papers-sabu-anonymous?intcmp=239

[724] Ryan, Yasmine. "Anonymous and the Arab uprisings: The cyberactivists discuss their work and the broader global push for freedom of speech and freedom from oppression." *Al-Jazeera*. 19 May 2011.

[725] Anonymous representative of Anonymous. "A hacktivist message announcing at 'Anonymous Operation Last Resort at the United States Congress plan to censour any internet website'". 5 November 2013).

[726] Ryan, "Anonymous and the Arab Uprisings".

[727] Anonymous. "Opinion: Anonymous and the global correction: A loosely organised group of hackers is targeting oppressive regimes and says this is just the beginning." *Al-Jazeera*. 16 February 2011.

[728] Al-Jazeera Staff. "Memo: Bush wanted Aljazeera bombed". *Al-Jazeera*. 22 November 2005.

such as those on electronic sabotage and bomb-making disseminated to the Muslim World by American (Muslim) revolutionary Jesse Morton in his magazine *Jihad Recollections*.[729]

While the distance to that comparison remains to be shown, it is interesting to note that one of the most prominent publishing members of Anonymous, Barrett Brown, was recently suspended from Twitter, then reinstated after a bevy of socially concerned fans went into online hysterics, Twitter claiming "the suspension was an 'error'" due to, as *The Daily Dot* article states, complaints from a "Nazi". The media article then quickly deviates to encourage Anonymous in its newest social justice "operation" which was interrupted by this unfortunate mix-up at Twitter, completely disregarding any discussion of the screenshots published with the article in which Brown writes in an open Twitter debate, "Those aren't gangbangers. These are gangbangers...we'll sell you to the Vietnamese...It's a gang, bitch. See if you recognize me now," after which he was "erroneously" suspended, and then reinstated by Twitter.[730]

As author of *We Are Anonymous* Parmy Olson writes, **it was clear that the character of any member of Anonymous, even in its early days, was "becoming increasingly ambiguous as he constantly watched and laughed at gore, rape, racism, and abuse. Everything was 'cash' or 'win'...[**they] knew the difference between right and wrong - they just chose not to recognize either designation on 4chan [website]. Everyone accepted they were there for lulz [laughs], and that the act of attaining lulz often meant hurting someone. It was no wonder that a future tagline for Anonymous would be, 'None of us are as cruel as all of us.' William's [a member of Anonymous] increasing ambivalence over sex and morality was being multiplied on a mass scale for others on 4chan and would become a basis for the cultlike identity of Anonymous."[731]

Another very prominent member of Anonymous, Andrew Auernheimer, a convicted felon and self-identified white-supremecist pictured in photos with a swastika tattoo on his chest paid for by his Syrian 'Alawite girlfriend, is known for his vocal anti-semitism, including joking in the documentary *The Hacker Wars*, to the amusement of the interviewer, that he believed the Jews of Europe deserved genocide. Auernheimer committed printer hacks in which he sent Nazi swastikas to the printer workstations of Jewish individuals, simply to record their alarmed responses via hacked webcams and share these videos online with fellow hackers. His participation in the Occupy Wall Street protests portray him holding a sign reading "Zionist Pigs Rob Us All". Auernheimer also worked as webmaster for Neo-Nazi website *The Daily Stormer*.

Wired Magazine describes him in the following way:

> Former president of the 'Gay Nigger Association of America,' an amalgam of online trolls, he took credit for a hack on Amazon that delisted hundreds of titles with gay and lesbian themes. Spouting Malthus, he wondered aloud about the most efficient way to kill off 4 billion of the earth's 6 billion people, and once compared trolling to 'eugenics,' a way to

---

[729] *American Jihad.* United States: Showtime. 2017.
[730] Gilmour, David. "Twitter lifts 'permanent' suspension of activist Barrett Brown Twitter says the suspension was an 'error.'" *The Daily Dot.* (24 June 2019). Internet resource.
[731] Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. London: William Heinemann, 2013, p. 37.

> purify the Internet by driving off the 'filth' and 'retards' (meaning bloggers). 'I hack, I ruin, I make piles of money,' he boasted to a New York Times writer. I make people afraid for their lives.' One such victim was Kathy Sierra, a Java programmer and educator, who suffered a campaign of harassment she's convinced Auernheimer orchestrated. She was threatened with rape, dismemberment, and was doxxed—her address and social security number posted online. A false narrative percolated, claiming Sierra was a former sex worker. It culminated in death threats, and convinced Sierra to leave the Internet for six years. Weev blustered about all this to the Times in 2008 but later claimed the reporter fabricated parts of the story.

Despite his later denials, the criminal activities he confesses to are what Olson, writer of *We Are Anonymous*, terms "a life choice…the porn, jokes, and shocking images...seriously harassing someone was called a 'life ruin'...'dox' them, or find their true identities, send them threats on Facebook, or find their family members and harass them, too. The jackpot was nude photos, which could be sent to family, friends, and co-workers for pure embarrassment or even extortion."[732]

This is the group the FBI saw fit to work with in 2011 to stage the Occupy Movement and Arab Spring IRC, to grant immunity to for their crimes, and later to merge with until becoming indistinguishable. Such is the asset management program of state-sponsored terrorism. The principal FBI asset of Anonymous known as Sabu (Monsegur) was given in December 2010 "the secret channel for hackers, #InternetFeds" where he "and the others in #InternetFeds increasingly talked about focusing their efforts on another growing news story: revolution in the Middle East."[733]

+ADD https://www.theguardian.com/technology/2012/mar/06/lulzsec-court-papers-sabu-anonymous?intcmp=239

This hacker and others were responsible for the cyber attacks in Tunisia and Egypt followed immediately by "cyber attacks on the governments of Libya, Egypt, Zimbabwe, Jordan, and Bahrain," and "worked with hackers to take government websites in Algeria offline"; requested sites in Anonymous chat rooms insisted further on cyber attacks in Libya and Bahrain after the first failed to achieve similar coups, and by February 2011, included calls for cyber attacks on Iran.[734]

Auernheimer also told another media outlet *Gawker* of a judge in his trial that "She's a mean bitch, I hear. I can see it in her eyes, she's a black Baptist Bush appointee and I don't think she's a fan [of the Gay Nigger Association of America]." Despite all of this, he was charged by the FBI for compiling a list of email addresses according to predictable changes made to AT&T URLs that he noticed while logging in himself. He was represented by a pro-bono lawyer Tor Ekeland, who would later appear on *Al-Jazeera News* inebriated, and Auernheimer found guilty in 2012 of one count of identity fraud and one count of conspiracy to access a computer without authorization. The decision was overturned after 13 months in prison, and Auernheimer moved

---

[732] Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. PAGE?

[733] Olson, Parmy. *We Are Anonymous*, p. 140-41.

[734] Olsen. *We Are Anonymous*, p. 148; 146; 175.

to Lebanon. The *Wired* article ends with a reminder from the lawyer that "hackers have groupies".[735]

Jesse Morton now works with the same NYPD Director of Intelligence Analysis that arrested him, Columbia University Professor of Public and International Affairs Mitch Silber, still disseminating publications (of a now different opinion) after serving 3.5 years of an 11.5 year sentence for al-Qa'eda-linked "terrorist activity".[736] As Morton recollects, "I'd begun my trek out of extremism and had become an asset of the FBI."[737]

Barrett Brown, despite publicly taking responsibility to a crowd in New York City for coordinating the technical aspects of the Arab Spring revolts[738] and taking part in stealing customers' financial information from the Visa and Mastercard credit card companies and exploiting that information for financial gain, was only arrested after publicly sharing a video in which he threatened to cyberstalk an FBI agent's children.[739]

The Tunisian blogger and programmer involved in Anonymous' shut down of seven Tunisian government websites, Slim Amamou, who had been arrested, was released the day of President Ben Ali's exile and four days later made interim government Minister for Youth and Sports.[740] + More on this

"the international mobilization of youth in Occupy movements around the globe, a level to which the Bahraini activists also aspire," and other protesters.[741]
https://www.theatlantic.com/technology/archive/2011/11/anonymous-barrett-brown-armed-mexican-drug-cartels/335861/ Zetas - re: el chapo "The idea that figures of authority, from teachers to the media, misunderstood the true talents of hackers was something Monsegur [Anonymous member 'Sabu' and FBI asset] understood all too well. As a young Latino living in the projects where his own family dealt drugs, he did not fit the description of nerdy computer hacker." + attacks against LOIC attacking PirateBay (101).[742] LulzSec [section of Anonymous] trafficks in Bitcoin, a crypto currency.[743]

---

[735] Penenberg, Alan. "The Troll's Lawyer". *Wired*. 5 January 2015.
[736] Morton, Jesse and Mitchell Silber. "NYPD vs. Revolution Muslim: The Inside Story of the Defeat of a Local Radicalization Hub". *CTC Sentinel, Vol. 11, Issue 4.* Combating Terrorism Center at West Point. April 2018. Internet resource.
[737] Morton, Jesse. "Opinion: I Invented the Jihadist Journal: I deradicalized after 3½ years in prison. Now I'm reclaiming the medium to combat violent extremism". *Wall Street Journal.* 3 June 2019. Internet resource.
[738] "Barrett Brown in New York: Barrett Brown speaking at a pro-wikileaks and pro-bradley manning press conference". *YouTube*. 4 April 2011. Internet media.
[739] Brown, Barrett. "Why FBI Agent Robert Smith Has Two Weeks To Send my Property Back", parts 1-3. *YouTube.* 11 September 2012. Internet media.
[740] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution". Rābī, 'Ūzī, and 'Abd -I. Bū'asrīyah. *Lost in Translation: New Paradigms for the Arab Spring*. Sussex Academic Press. 2017. Internet resource.
[741] Karolak, Magdalena. *The Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Academica Press. 2014, p. 3-4.
[742] Olsen. *We Are Anonymous*, p. 135; 101-03.
[743] Olsen. *We Are Anonymous*, p. 429.

Not only can hackers gain access or be granted access to space and electronic weaponry systems, which can be used as lethal weapons, but hacking culture encourages the recreational use of similar human tracking systems. Researcher Michael Scarito of MIT, a self-described "multidisciplinary hacker masquerading as an electrical engineer", presented an hour-long seminar at the DEFCON 19 conference titled "Build Your Own Radar System", advertised on the DEFCON website by the following description:

> Radar is used extensively by the military, police, weather, air travel, and maritime industries - why not you? Come learn how to build a radar imaging system on the cheap! This talk will explain the basics of how radar works as well as how to measure range and velocity of your chosen targets. You will learn how to use synthetic aperture techniques to generate a two- or even three-dimensional image. The hardware and software design will be totally opened up so you can go home and build your own system.[744]

His presentation features basically two coffee cans wired together with a battery, which he admits bringing onto a commercial airplane with very few questions asked by TSA in order to transport to it the conference. While nothing but possible nuclear weapon proliferation came of this presentation, the FBI did arrest another technologist at a DEFCON conference earlier in 2001, Dmitry Sklyarov, after he presented an instructional on bypassing encryption in Adobe Acrobat in order to copy copyrighted e-books.[745]

https://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/

Through-the-wall imaging via synthetic aperture radar. [EPA Particulate Matter Standard-policy reinforced] ICC Crimes Against Humanity.

+ Definition of genocide as *systematic* expulsion, castration or murder of a group or part making up a group. "Prevention of Procreation:…This may be due to the large number of castrations that take place in armed conflict as well as the frequency of violence aimed at male reproductive organs. Indeed, perpetrators themselves, at times, will explicitly express the intention of depriving the victim of their procreating capability… This is particularly true of sexual violence against women in armed conflicts of an ethnic, racial or religious dimension in which the prevention of their giving birth to members of the same ethnic, racial or religious group may be a particular focus of perpetrators. This may be prevented or impeded through forcible impregnation, damaging the reproductive organs or creating stigma on the part of raped women… The linkage between the prevention of procreation on the part of both sexes would seem to be recognized by the Rome Statute of the International Criminal Court, which lists enforced sterilization as a crime against humanity, defined in the elements of crimes, in part, simply as the deprivation of ' biological reproductive capacity '. This is wide enough to encompass male sexual violence such as castration or other genital mutilation that leads to the inability to procreate."[746]

---

[744] Scarito, Michael. "Build Your Own Radar System". DEFCON. August 2011. <https://www.youtube.com/watch?v=8nJIeVeOeBA>; <https://www.defcon.org/html/defcon-19/dc-19-speakers.html>.

[745] Schneier, Bruce. *Click Here to Kill Everybody*, p. 41.

[746] Sexual Violence against men in conflict, p. 273-274

[TOPIC - State-sponsored rape, sexual violence as tactic of war, irregular warfare implies non-soldiers meaning women and children, irregular warfare describes wartime conduct that constitutes war crimes, compare sex trafficking by US surveillance state as precursor of sex trafficking in warfare zones] +ADD "Edward Snowden, the National Security Agency contractor turned whistle-blower, claims that "incredibly weak" oversight of U.S. surveillance programs enabled military personnel to obtain sexually explicit photos of people under surveillance and to sometimes share them with others. In an interview with the *Guardian*, Snowden talked about the impact of poor auditing systems within the NSA. He claimed many people sifting through monitored communications were 18 to 22 years old and suddenly put in a position of extraordinary responsibility that was sometimes abused. "In the course of their daily work they stumble across something that is completely unrelated to their work, for example an intimate nude photo of someone in a sexually compromising situation but they're extremely attractive," said Snowden."So what do they do? They turn around in their chair and they show a co-worker. And their co-worker says: 'Oh, hey, that's great. Send that to Bill down the way,'" he said. "He said the interception of intimate images was "routine enough" and described it as "sort of the fringe benefits of surveillance positions."[747]

"Another form of sexual violence in which the dynamics of power and dominance are particularly evident is that of forced nudity. There are all too frequent reports of women having been forced to strip naked. They have been ' subjected to humiliating strip searches, forced to parade or dance naked in front of soldiers or in public, and to perform domestic chores while nude ' . One particularly infamous incident involved women being forced to take off their clothes and dance naked on a table while being watched by male soldiers. This was subsequently held by the International Criminal Tribunal for the former Yugoslavia to constitute an inhumane act for the purposes of crimes against humanity. Individuals who are forced to strip naked feel exposed, vulnerable and without dignity. These feelings are exacerbated when the forced nudity is accompanied by threats of a sexual nature. Some male survivors state that, ' the humiliation of being interrogated while naked was a very drastic event in their lives.' Depending on the particular cultural context in which this forced nudity takes place, the effects may be particularly severe. Another survivor thus states that, ' [w]e stood nude in front of UPC [Union of Congolese Peoples] officials … I was so shocked. I had never seen my father in this way. In our culture, it is not right. First they molested us … then they raped us.'… This is not very different from male rape committed in time of peace. In Algeria, ' [i]t was made known unofficially by the authorities that men had been raped in detention, and should no longer have the status of adult males in the community '"… "A consideration of sexual violence in conflict cannot be divorced from the very particular context in which it takes place. In conflicts of an ethnic, racial or religious character, sexual violence is often targeted against individuals belonging to particular ethnic, racial or religious groups rather than being sporadic or opportunistic in nature in order to symbolically dominate that entire group. An analysis of the ways in which male and female bodies are symbolically constructed may be useful in considering this proposition. The symbolic construction of the female body tends to be that of the community… Accordingly, an attack on the female body is a symbolic attack on the personification and culture of the entire community. In much the same way as sexual violence against women may symbolize to offender and victim alike the destruction of the national, racial, religious or ethnic culture as appropriate depending on the context of the conflict, sexual violence against men symbolizes the disempowerment of the national, racial, religious or ethnic group. "[748]

---

[747] https://time.com/3010649/nsa-sexually-explicit-photographs-snowden/

[748] Sexual violence against men in conflict, P. 269; 271.

+ Hackforums slave girl sales "Man I feel dirty looking at these pics," wrote one forum poster at Hack Forums, one of the top "aboveground" hacking discussion sites on the Internet (it now has more than 23 million total posts). The poster was referencing a 134+ page thread filled with the images of female "slaves" surreptitiously snapped by hackers using the women's own webcams. "Poor people think they are alone in their private homes, but have no idea they are the laughing stock on HackForums," he continued. "It would be funny if one of these slaves venture into learning how to hack and comes across this thread." By finding their way to forums filled with other ratters, these men—and they appear to be almost exclusively men—gain community validation for their actions. "lol I have some good news for u guys we will all die sometime, really glad to know that there are other people like me who do this shit," one poster wrote. "Always thought it was some kind of wierd sick fetish because i enjoy messing with my girl slaves." As another poster put it in a thread called ☆ ShowCase ☆ Girl Slaves On Your RAT, "We are all going to hell for this..." But he followed it with a smiley face. Welcome to the weird world of the ratters. They operate quite openly online, sharing the best techniques for picking up new female slaves (and avoiding that most unwanted of creatures, "old perverted men") in public forums. Even when their activities trip a victim's webcam light and the unsettled victim reaches forward to put a piece of tape over the webcam, the basic attitude is humorous—Ha! You got us! On to the next slave! And there are plenty of slaves."[749]

The youth movement of barely adult and adolescent men participating in crimes of genocide and persecution advertised as a social activity is reminiscent of another one of Nazi Europe's genocidal social organizations, described here by Jan Karski, Polish Holocaust whistleblower:

> He pushes me to the window. 'Look at it. Look at it.' There were two boys. Nice-looking boys. *Hitlerjugend* in uniforms. They walked – every step they made, Jews disappearing, running away. They were talking to each other. At a certain point, a boy gets to his pocket. Without even thinking, shoots, saying, "Maaaah!". Some broken glass. Some shouting "Ahhhh!" The other boy's congratulating him. They go back. So, I was paralyzed. [Jan Karski describing activities he witnessed from the Hitler Youth in the Warsaw Ghetto in 1942] [750]

The people who have been members of Anonymous are responsible for complicity in as many deaths in genocidal wars, as many wars in as many countries, the destruction of an entire continent, and have been given as much license to violence by the State and provided war weapons as the Europe's Hitler Youth, with none of the bad press and none of the social responsibility. They lack uniforms and an end to their story. [REWORD]

Just as in the Yugoslav War, the US media has played the same role in the Arab Spring wars. Journalist and editor Glen Greenwald, who is now under criminal investigation in Brazil where he resides, and his newspaper *The Intercept* have been under scrutiny for withholding

[749] https://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/
[750] https://collections.ushmm.org/search/catalog/irn1003915

information from the classified files leaked by Edward Snowden that warned of the coming devastation in Syria.[751] https://www.mintpressnews.com/intercept-withheld-nsa-doc-that-may-have-altered-course-of-syria-war/233757/ Greenwald is alleged to be the sole holder of the so-called Snowden Files, which never were actually leaked to the public (only 1% of the files have ever been revealed) but only to Greenwald himself.

Glen Greenwald is a favorite journalist of the hacker crowd due to his role as the main recipient and gate-keeper of the Snowden files since they were revealed. He is so intimately involved with the Anonymous hacker group that he is featured as endorser and reviewer on the cover of McGill University professor Gabriella Coleman's 2015 book *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. He is also the former editor and publisher of Anonymous frontman Barrett Brown's journalistic articles.

In my own attempts to contact *The Intercept,* Edward Snowden's outlet Freedom of the Press Foundation, and Barrett Brown, who is a self-employed journalist, over a period of three years concerning a host of inquiries about individual cyber privacy, cyberstalking, electronic human trafficking and tracking, and their professional practices concerning cyber privacy, I have received no response.

These individuals are media journalists who are closely associated with Anonymous and hacktivism. Glen Greenwald of *The Intercept* and Edward Snowden of *Freedom of the Press Foundation* both refused to release information collected from 2013 government leaks that would have forewarned of devastating events in Syria at the hands of Saudi Arabia, the US State Department and NSA. It was estimated in 2016 that since 2013, less than 1% of the so-called Snowden leaks had been released. "In the years since, journalists have released more than 7,000 top-secret documents that Snowden entrusted them with, which some believe is less than 1% of the entire archive."[752] Why this is so, and why alleged whistleblower Snowden himself has not revealed information in his own media outlet requires explanation.

Edward Snowden is not simply a reneged civilian surveillance contractor, but he was a member of the CIA beginning two decades ago where "he was part of the small army of tech-savvy people the C.I.A. hired in the early 2000s".[753] In response to his recent book *Permanent Record*, which he has advertised on his Twitter account with a photo of a topless woman holding up the book, the US Department of Justice has sued to prevent release and claim proceeds of. Snowden responded by directing interested traffic to the Bitcoin market, a brand of cryptocurrency often involved in online drug sales and sexual exploitation,[754] in order to buy the book.[755]

---

[751] Webb, Whitney. "The Intercept Withheld NSA Doc That May Have Altered Course of Syrian War". *MPN News*. 30 October 2017. Electronic resource.
[752] Szoldra, Paul. "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks". *Business Insider*. 16 September 2016.
[753] Burrough, Brian, Sarah Ellison and Suzanna Andrews. "The Snowden Saga: a shadowland of secrets and light". *Vanity Fair*. May 2014.
[754] Francis, Jeff. "Police say human traffickers are turning to Bitcoin". *Bitcoinist*. 15 October 2017.
[755] Marinoff, Nicholas. "DOJ lawsuit over tell-all book is "good for Bitcoin," says Edward Snowden". *Decrypt*. 18 September 2019.

It should be noted that the US federal Secret Service has not investigated or condemned Bitcoin as illegal currency, and so such a statement by Snowden is, once again, a feigned aggression against the US in order to maintain the socially engineered reputation as rebel hacker.

Proxy Wars and 'Going Native'

[TOPIC – Intro: how coups and wars of Arab Spring were incited/accomplished by manipulating Internet proxies, and therefore demographics of politics by presenting themselves as citizens of those Arab states – integral to social engineering.]

"In accepting this conditioning reality and its interaction with the concerns of political actors, far more credence is lent to Khanna's view that 'geopolitical competition is evolving from war over territory to war over connectivity.'"[756]

"This work has sought to establish what circumstances led to this state of affairs in cyber security by revealing the insecurities suffered in and through cyberspace, reflecting challenges that run far deeper than the immediate impacts of cybercrime, cyber espionage, or cyber attacks themselves. Instead, it needs to be accepted that the maturation of computing technologies, connected with internetworking innovations and encryption practices, have presented fundamental disruptions to social, economic, and political orders themselves." [757]

"With that broadened impact in mind, a series of conclusions are offered on the politics and technology of cyber security:

1. There are technological realities that greatly shape our security concerns…

The first of these is that *there will be an increased tension between the universality of Internet standards and the demands of political sovereignty*. In particular, the reliance of communications and the global economy on TCP/IP and DNS through the root server will ensure the tension between maintaining the globally connected Internet based on universal protocols and satisfying political demands to impose sovereignty will only increase, or certainly encounter difficult episodes in practice. Serious propositions for fragmentation would involve either wholesale segregation from the global networks in the fashion of North Korea, or the implementation of new technologies that permit leaving the original infrastructure behind. This is an important factor to consider for, as noted by the Global Commission on Internet Governance, 'efforts to gain political and economic advantage bring the network toward fragmentation and away from universality.'… Second, geography still matters. Among the many utopian visions projected into cyberspace has long been an assertion that geography was no longer relevant, that a demise of geographic importance was a self-evident reality in our modern hyper-connected, globalised world. Yet with the importance of submarine cables and data centres established this work, it is plain that cyberspace has a fundamentally physical reality that is grounded in the geographically physical world. Internet protocols cannot function without cables to travel through, and data must ultimately be stored somewhere physically real. These two technological facts carry significant conditioning realities of great interest to strategic actors: first, who owns the infrastructure? A significant geopolitical advantage underwrote the ability of the NSA and GCHQ to conduct the surveillance operations that were betrayed by Edward Snowden. That advantage was dominance of the submarine cable infrastructure through which a disproportionate amount of traffic traversed." [(pg. 95-96 – relate to Internet Backbone section)]

2. The apolitical honeymoon is over; political sovereignty will be established…

---

[756] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 95.
[757] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 94.

The 'sovereignty gap' that Kello rightly identified where state influence – even its fundamental importance – has waned is certainly now the subject of vigorous redress from governments all over the world… Perhaps the biggest challenge facing the Free Internet Coalition is recognising that they have never viewed the contest as a geopolitical one, whereas Beijing, Moscow, and other have always viewed the Internet as a threat to their national security. (pg. 97)

3. Cyberspace must be seen as a crucial geopolitical battleground of the 21st century".[758]

I am working within the definition of the Information Age, and therefore information warfare and information technology, given by Holocaust researcher Edwin Black:

> *The Information Age is the individualization of statistics*. Not only can I count you as a member of the crowd, I can individualize the information I have about you. And the Information Age was invented not in Silicon Valley, but in Berlin in 1933.[759]

Known as "the new media model created by means of ICT", "aside from encouraging civic action, social media can help authoritarian rulers trace these activists and silence them, as was the case in Tunisia and Egypt."[760] These two capabilities of the new media model are not contradictory. The encouragement of civic action is an integral part of tracing activists as,

> Media can serve as a significant driver for mobilization. However, for media to play that role effectively, it will need to be able to highlight the need for change and the growing demand for it (or what Clay Shirky dubbed 'angerness') and provide the content that could justify the need to act.[761]

As Karolak writes in *The Social Media Wars*, the government is **'simultaneously target, sponsor, and antagonist for social movements as well as the organizer of the political system and the arbiter of victory'**."[762]

Boms describes the Tunisian protests as beginning with the release of a *Wikileaks* report describing the opulent and wasteful lifestyle of Tunisian political elites along with the dissemination of images of a young Tunisian's desperate "self-immolation" due to economic problems.[763] **It should be noted that disseminated images of a monk's self-immolation were also the cause of civil unrest in Vietnam that directly led to US invasion and coup in 1963**. At the time, U.S. President John F. Kennedy was quoted to say, "No news picture in history has generated so much emotion around the world as that one."[764]

The breakout of Tunisian protests, considered to be the beginning of the Arab Spring, was followed with similar inciting messages of government cruelty disseminated throughout new

---

[758] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 94, 97-98.

[759] Black, Edwin. "IBM and the Holocaust". 26 February 2012. Presentation at Yeshiva University, New York, NY.

[760] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution". *Lost in translation : new paradigms for the Arab Spring.* 2017, p. 188.

[761] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution", p. 196.

[762] Karolak, Magdalena. *The Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Academica Press. 2014, p. 13.

[763] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution", p. 192.

[764] Lindsay, James M. "The Water's Edge: TWE Remembers Thich Quang Duc's Self-Immolation". *Council on Foreign Relations blog post*. 11 June 2012.

media platforms in the countries that followed in protest, including Egypt, Libya, Syria, Bahrain, Morocco and Palestine.[765] Boms notes, "Internet-based opposition to the regime came also from outside Tunisia. Groups like Anonymous, an international Internet activist group, used the help of 'hacktivists' (hacker activists) to take Tunisian government sites offline".[766]

To state that the new media opposition came *also* from the outside negates the facts presented but affirms the conclusions of this thesis.

"Each participant was identified by six random letters and the country his or her computer was in (though many had spoofed that with proxy servers to avoid detection). The countries with the greatest number of participation computers were Germany, the United States, and Britain."[767]

More precisely stated to facts, the Internet-based opposition originally came *only* from the outside. To address the quote's context, Anonymous itself has stated very clearly, "We are Anonymous. We are Americans," in a statement disseminated from the group in 2013.[768] Further, the chapter traces the origins of all Arab Spring protests to reports disseminated by *Wikileaks*, whose Australian editor Julian Assange is quoted as writing of Wikileaks:

> The CIA is the world's most dangerously incompetent spy agency. It has armed terrorists, destroyed democracies and installed and maintained dictatorships the world over. There are good men and women at the CIA but if our publications are any guide *they work for Wikileaks*.[769]

+"The victimization of Wikileaks, they figured, would strike a chord with Anonymous and bring hordes of users to their new network. It was great publicity. Who were these people in #command [IRC]? Known as 'operators' of the new chat network, they weren't hackers per se but computer-savvy individuals who maintained the network and who would play a crucial role in organizing ad hoc groups of people, large and small, over the coming weeks. Many of them got a kick out of hosting hundreds of people on their servers."[770]

+ADD "The young programmer [WHO?] wrote a web script that Tunsians could install on their web browsers that would allow them to avoid the government's prying eyes. The script was about the length of two sides of paper, and Tflow [a member of Anonymous] tested it with another Anon in Tunisia, nicknamed Yaz, then pasted it onoto a website called userscript.org. He and a few others then advertised the link in the #OpTunisia chat room on AnonOps, on Twitter, and in digital flyers. It got picked up by a few news outlets. The hacktivist Q was one of the #InternetFeds members and also one of the dozen channel operators in the #OpTunisia channel. He began talking with Tunisians on AnonOps - the ones who were web-savvy enough

---

[765] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution", p, 193-96.
[766] Boms, Nir. "Virtual Reality: New Media, the Arab Spring and the Democratic Revolution", p. 193.
[767] Olsen. *We Are Anonymous*, p. 115.
[768] Anonymous representative of Anonymous. "A hacktivist message announcing at 'Anonymous Operation Last Resort".
[769] Akmen, Tolga. "CIA is world's most dangerously incompetent spy agency". *Going Underground*. *RT*. 16 May 2017.
[770] Olsen. *We Are Anonymous*, p. 109.

to access it via proxy servers - and encouraged them to spread the news of the script through their social networks. 'OpTunisia fascinated me,' Q later said in an interview. 'Because we actually did make an impact by pointing Western media to the things happening there.' Within a few days, news of the script had been picked up by technology news site *ArsTechnica* and it had been downloaded more than three thousand times by Tunisian Internet users."[771]
+ADD "The function of social media references, such as Twitter hashtags in a transmedia strategy, is focused on audience engagement. Twitter, in particular, is one of the favorite social network tools because it provides proselytes with the opportunity to access contents posted online in relation to a specific hashtag or topic and to easily and efficiently spread other posts by retweeting them to broader networks of followers (Klausen, 2015). The use of hashtags becomes a first line of engagement, which starts Dabiq as the tent pole of the narrative and is oriented to Twitter followers; it is also a second trajectory that starts from Twitter posts and brings the audience from the hashtags back to the magazines. In both cases, media contents could exist independently from one another, but, at the same time, they establish synergic mutual relations. This simple content flow from Dabiq to the video and then to hashtags and the reverse clarifies a basic synergistic storytelling strategy. The main narrative is framed through three different media contents, namely, textual advertisement in Dabiq, online video, and Twitter posts related to the hashtags, which can be accessed and experienced by an audience scattered worldwide."[772]

As noted on his June 2009 blog *Boing Boing* titled "Cyberwar guide for Iran elections", well-known activist journalist and former European director of the Electronic Frontier Foundation Cory Doctorow[773] instructs followers on "how to actually help the protesters and not the gov't in Iran." He states that "The purpose of this guide is to help you participate constructively in the Iranian election protests through Twitter." He matter of factly recognizes that Iranian "security forces are monitoring this [#iranelection] hashtag, and the moment they identify a proxy IP they will block it in Iran," and that "Security forces are now setting up twitter accounts to spread disinformation by posing as Iranian protesters." He encourages his followers to create "new proxies for the Iranian bloggers," and most interestingly to "Help cover the bloggers: change your twitter settings so that your location is TEHRAN and your time zone is GMT +3.30. Security forces are hunting for bloggers using location and timezone searches. If we all become 'Iranians' it becomes much harder to find them."[774]

"It [the Tunisian government] blocked all Internet requests from outside Tunisia, shutting itself off from foreign Internet users like Sabu. Sabu wanted to deface the site of Tunisian prime minister Mohamed Ghannouchi, but he would have to do that from inside the country, and he wasn't about to get on a plane. So on January 2, he signed into the #OpTunisia chat room with its dozen channel operators and several hundred other Anons from around the world, including Tunisia. There was talk of using proxies and potential DDoS attacks; questions about what was

---

[771] Olsen. *We Are Anonymous*, p. 142.
[772] Monaci, p. 2850.
[773] "Cory Doctorow: EFF Special Advisor". *EFF: Electronic Frontier Foundation*. Accessed 8 August 2019. Internet resource.
[774] Doctorow, Cory. "Cyberwar guide for Iran elections". *Boing Boing*. 16 June 2009. Internet resource.

going on. Then Sabu hit the caps lock key and made his grand entrance. 'IF YOU ARE IN TUNISIA AND ARE WILLING TO BE MY PROXY INTO YOUR INTERNET PLEASE MSG ME.'... Sabu got a private reply from someone with an automated username like Anon8935... The man said only that he'd been a street protester and now wanted to try something different, something on the Internet. Trouble was, Anon8935 didn't know a thing about hacking. Sabu gave him some simple instructions, then said, 'My brother. Are you ready?'...'You realize I'm going to use your computer to hack pm.gov.tn?' 'OK,' the man replied. 'Tell me what to do.' Sabu sent over some brief instructions for downloading and installing a program that would let Sabu take control of the man's computer... The Tunisian government had set up a firewall to stop foreign hackers from attacking its servers; it had never expected attackers to come from within its own borders…'Thanks, brother,' Sabu said. 'Make sure to delete everything you downloaded for this and reset your connection.' After a few minutes the man went offline, and some days later, Sabu hung a Tunisian flag in his house. Sabu then heard that the man had been arrested. While he felt bad for his volunteer, Sabu did not feel guilty. A higher cause had been served. 'Operation Tunisia,' Sabu later recalled, ' was the beginning of a serious technical advancement for Anonymous. On January 14, Tunisian president Ben Ali stepped down."[775]

In a 2011 study on Arab Spring Twitter activity titled "The MENA protests on Twitter: Some empirical data", media and journalism professor Deen Freelon collected metadata from five million tweets in Twitter's tweet archives before Twitter made its archives closed to public use on March 20, 2011. Freelon analyzed the perceived location of origins of tweets under seven hashtags representing seven countries: Egypt, Libya, Tunisia, Bahrain, Morocco, Yemen and Algeria. He notes that in every analysis, the large increases in tweets under a country's protest tag came from outside that country, and from outside the Middle East and North Africa region.

Freelon concludes that his study "indicates that, at least in the early days of the Arab Spring, Twitter served primarily as a platform for communication by international observers about the events. There is also limited evidence of a pan-Arabic public conversation within these hashtags, but this is not their primary purpose." He details that only when international spikes in Twitter activity pass did in-country participants become active again.

Freelon also compares the Arab Spring social media activity with that of the 2009 Iranian protests via social media, stating that "Twitter seems to fall into Aday et al.'s (2010) 'external attention' category of new media roles."[776]

+ADD "Our findings suggest that the vast majority of attention to Arab Spring content came from outside of the MENA region and, furthermore, that mass media, rather than citizen media, overwhelmingly held the world's attention during the protests. We thus conclude that Twitter was broadly useful as an information channel for non-MENA onlookers but less so for protesters on the ground."[777]

---

[775] Olsen. *We Are Anonymous*, p. 143-45.

[776] Freelon, Deen. "The MENA protests on Twitter: Some empirical data". *Dfreelon.org*. 19 May 2011.

[777] https://journals.sagepub.com/doi/pdf/10.1177/0002764213479373

"patterns of consumption of Arab Spring– related content using a unique data set constructed by combining archived Twitter content with metadata drawn from the URL shortening service Bit.ly… "[778]

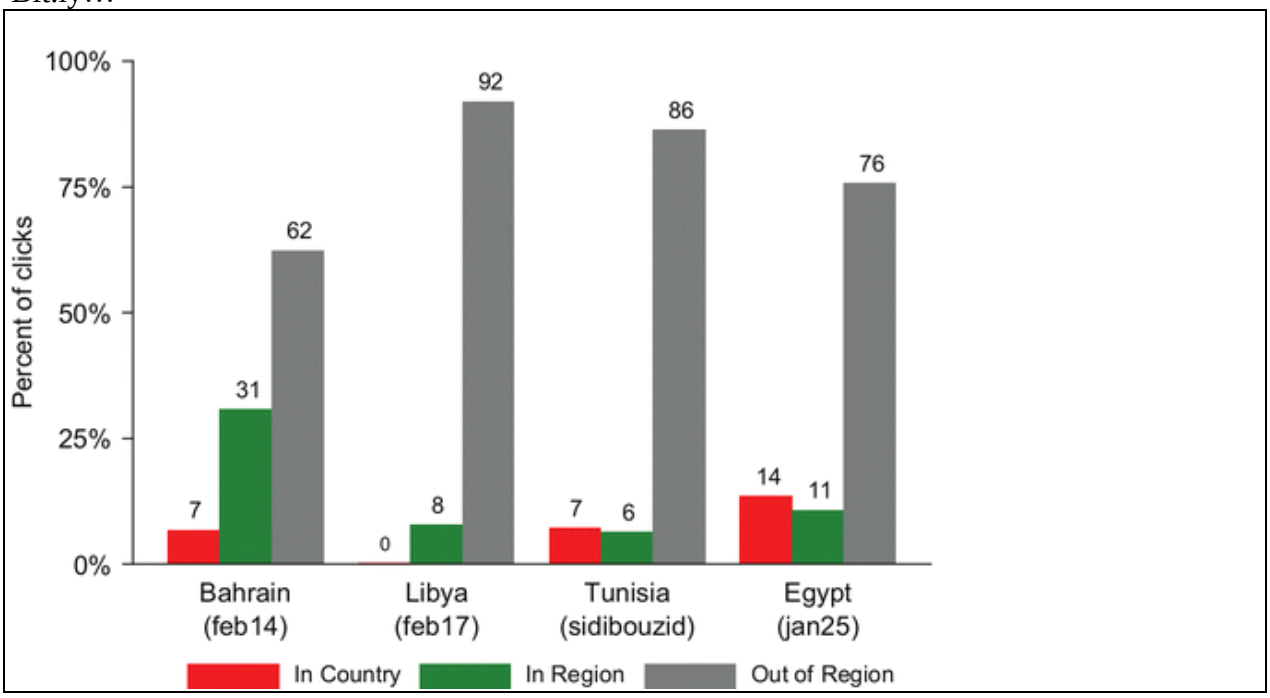


Table "Percentage of clicks on bit.ly links, by location (January 1 to April 1, 2011)" from Aday et al. "Watching from Afar: Media Consumption Patterns Around the Arab Spring".
+ADD 'In Region' indicates clicks coming from within the Middle East and North Africa (MENA). 'Out of Region' indicates activity originating from outside the MENA region."#sidibouzid (Tunisia; 79,166 total tweets), #jan25 (Egypt; 665,092 total tweets), #feb14 (Bahrain; 48,015 total tweets), and #feb17 (Libya; 885,724 total tweets)."[779]

Likewise, in his article, "The Challenges of Social Media for the Intelligence Community", Andrew Liaropoulos finds that:

> Twitter was mainly utilized by outsiders, by observers and journalists in other countries. Reporters that could not *reach* the revolution on the ground, scrolled the English language tweets in order to get useful insight. Twitter has basically been used to gain external attention and solidarity and not solely to coordinate people on the ground. Surprisingly the tweets were not written in Farsi, but in any other language in order to reach supporters of the Green Movement, outside Iran… The Green Revolution was the first major world event broadcasted via social media and succeeded in gaining international attention, but Twitter was not a key mobilizing factor within the country itself. Twitter was relatively new and few Iranians used it in 2009. Furthermore, outside supporters of the Green movement, by changing their stated location made it difficult for analysts to reach solid conclusions about the exact number of Twitter users from Iran and the true number of those involved in protests.[780]

[778] https://journals.sagepub.com/doi/pdf/10.1177/0002764213479373
[779] https://journals.sagepub.com/doi/pdf/10.1177/0002764213479373
[780] "The Challenges of Social Media for the Intelligence Community" Andrew Liaropoulos, p.8-9

+ADD Ukraine Orange Revolution & Twitter
"Although digital media played a role in Ukraine's 2004 Orange Revolution and Twitter had a role in organizing the civil unrest in Moldova after the Party of Communists won the majority of seats in the 2009 parliamentary election, it was not until the Green Revolution in Iran that social media revealed its true potential. The protests in Iran in June 2009, where the first signal of what was going to happen in the coming two years in the Middle East and North Africa."[781]

The field of Middle Eastern studies has a long history of speaking for Middle Easterners, going back centuries to when it was referred to as Oriental Studies. This role of Western participation in Middle Eastern affairs is part of what Edward Said defined as Orientalism in the West. From Rudyard Kipling's *Kim*,- about a young Irish boy who acts as a spy by disguising himself in the garb and languages of various Indian ethnicities and religions,- to Anglo actors in black face portraying Othello, to T.E. Lawrence's legacy as Lawrence of Arabia, the idea of representing the Orient has fascinated "bright young Westerners".[782] **The introduction of technology into this long-standing Orientalist trend has enabled new generations and larger numbers of Westerners to represent the East for Easterners.** After all, "social media, by its very nature, is only an extension of the social context in which it operates."[783] **And the unusually high level of participation displayed by foreigners in the Arab Spring who otherwise do not concern themselves with events in the Middle East demands explanation.**

+ADD "Iran receives coronavirus aid from unexpected source, Washington (CNN), The State Department is using social media to encourage Iranians to share information with the Trump administration -- both on an encrypted tip line and through an online survey -- about the coronavirus pandemic that is devastating the country. **'This is Iran's Chernobyl**,' said one **administration official of the outbreak, who described social media portals as a tool to bypass the Iranian regime and connect to the country's people.** The US began encouraging Iranians to use the encrypted messaging app last year [2019], when Iranian demonstrators took to the streets and US officials wanted to learn more about the regime's bloody crackdown. Now, with Covid-19 devastating Iran, the tip line has been reinvigorated, administration officials told CNN. This time**, the goal is to collect information from Iranians, find ways to share that information when it is determined to be accurate and leverage the coronavirus in an effort to fortify a relationship with the Iranian people, the officials said**."[784]

---

[781] "The Challenges of Social Media for the Intelligence Community" Andrew Liaropoulos p. 8
[782] CITE Said, Edward. Orientalism.
[783] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*. RAND Corporation. 2013, p. 72.
[784] https://www.cnn.com/2020/03/18/politics/state-department-coronavirus-iran-outreach/index.html

"Social media may have harmed the revolution by letting the government monitor activists and by permitting Facebook users a free ride and the feeling that they were participating without incurring the costs of civil disobedience."[785]

Internet Service Providers

I just the other day got,- an internet was sent by my staff at 10 o'clock in the morning on Friday and I just got it yesterday. Why? Because it got tangled up with all these things going on the internet commercially. [786]
Senator Ted Stevens

"Internet surveillance often involves the cooperation of telecommunications providers, who give the intelligence agencies copies of everything that goes through their switches...We know that the NSA installs surveillance equipment at AT&T switches inside the US, and has collected cell phone metadata from Verizon and others. Similarly, Russia gets bulk access to data from ISPs inside its borders."[787]

A 2019 article in *Bloomberg Businessweek* titled "How to Take Back Your Email" represents well the common efforts people make in order to prevent hackers gaining access to their data, which for end users purchase private hardware like email servers and private modems (versus connecting via a hotspot subscription). The article suggests readers buy a $500 server that is managed by a software company that will ensure a domain name is granted and will duplicate data in an encrypted cloud service for $100 a year.[788]

This is no different from various commercial cloud models, excepting the purchase fee of a small server, and realistically results in the FBI inevitably serving court orders to server providers and managers once the company becomes known to officials, along with a gag order that prevents those managing the servers from informing users.[789] This is in some contrast to Google, Inc. which voluntarily contracts with and hires surveillance state executives, though the effect is the same to users.

In fact, many major content and platform providers have become Internet service providers as well, removing another important layer of competition that should serve as a buffer for user privacy. Despite sincere attempts at maintaining privacy through anti-malware software and even through private hardware, an end user or content provider must still go through an Internet service provider.

---

[785] Tkacheva, Olesya, et al. "Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt". *Internet Freedom and Political Space*, p. 44. RAND Corporation. 2013. Internet resource.
[786] Wired Staff. "Your Own Personal Internet". *Wired Magazine.*
[787] Schneier, Bruce. *Click Here to Kill Everybody*, 65.
[788] Chafkin, Max. "How to Take Back Your Email". *Bloomberg Businessweek: How To Fight Big Tech*. 12 August 2019, p. 46-49.
[789] Lyman, Will, et al.. *Frontline: United States of Secrets: The Inside Story of the Government's Mass Surveillance Program.* 2014.

+ADD "'I have the bots, so I make the shots,' he would say. Everything was controlled on IRC."[790]
+ADD "Sabu and a few others from #InternetFeds discovered there were just two name servers hosting Tunisia's government websites. This was unusual - most governments and large companies with Web presences ran on several name servers, so a hacker taking down a few usually didn't do much damage. In Tunisia's case, however, shutting down just two name servers would take the government completely offline."[791]
+ADD Anonymous IRC dropped in Amazon hack. Amazon DoD contractor.

Even the coder who believes himself to be the most clever hacker is using a corporate Internet service provider to access the Internet, which in turn is using Internet infrastructure like fiber optic cables belonging to the US government and Internet service providers like AT&T and Google.

[TOPIC – DNS]

+ADD p 45 info on Egypt's lack of technical capabilities to access servers, etc.? Ability to shut off Internet in Egypt, first blamed on DNS. "We are your SPs." ([Internet] Service Providers) Anonymous representative of Anonymous, in a hacktivist "Message to Scientology".[792]
"But while high-bandwidth national networks rely on fiber-optic landlines and undersea cables, tactical networks have to work on the move, which means they're wireless. So tactical cyber warfare depends on *electronic* warfare, the use of radio waves to detect, disrupt, and deceive the enemy's transmissions while protecting your own. Unfortunately, the Army disbanded its electronic warfare corps after the Cold War."[793]

"In 2007, over the course of 22 days a Russian attack on Estonia took out commercial and government servers with distributed denial of service attacks; not just public websites but also what one report called 'more vital targets, such as online banking **and the Domain Name System,' without which people can't find or look up websites and online servers**."[794] [Repeated]

Internet Backbone Providers

No, I'm not finished. I want people to understand my position. I'm not going to take a lot of time. They want to deliver vast amounts of information over the internet. And again, the internet is not something you just dump something on. It's not a truck. It's a series of tubes. And if you don't understand, those tubes can be filled and if they are filled, when you put your message in, it gets in line and it's going to be delayed by anyone that puts into that tube enormous amounts of material, enormous amounts of material.

---

[790] Olsen. *We Are Anonymous,* p. 114.
[791] Olsen. *We Are Anonymous,* p. 142.
[792] (21 January 2000). Internet resource. <https://en.wikiquote.org/wiki/Anonymous_(group)>
[793] Freedberg, Sydney J., Jr. "Can Army Afford The Electronic Warfare Force It Wants?".
[794] https://spectrum.ieee.org/podcast/telecom/security/is-cyberwar-war

Now, we have a separate Department of Defense internet now, did you know that? Do you know why? Because they have to have theirs delivered immediately. They can't afford getting delayed by other people.[795]
Senator Ted Stevens

+ADD [2nd mention] "Development of the Repository began in late 2015, and it currently houses over 750 completed and future DoD wargames entries. Access to details about these wargames is open to all DoD personnel via the **Secret Internet Protocol Router Network**, and the details include summaries of results from over six hundred wargames and full-length reports from over one hundred wargames."[796]
+ADD ARSTechnica "How Egypt did (and your government could) shut down the Internet 1/30/2011, Domain Tech "DNS not to blame for Egypt blackout" 1/28/2011, "Egypt severs Internet connection amid growing unrest: Internet connections across Egypt have been cut, as authorities geared up for a day of mass protest" 1/28/2011 [printed out]
"So vital is DNS to the ubiquity of cyber attacks that the nascent National Cyber Security Centre (NCSC) in Britain has centered its flagship defence program – Active Cyber Defence – on DNS filtering in order to reduce the attack footprint in the UK." (p. 14)
+ADD "The answer reveals an unpalatable reality; that cyberspace not only has, but also is fundamentally dependent upon, a physical geographically based architecture. Nowhere is this more real than in the critical role played by submarine cables. Submarine cables matter most above other physical components of transmission (notably, orbital satellites) for one reason: the very vast bulk of all content traversing cyberspace does so through submarine cables. Estimates can vary on the exact amount, with the International Cable Protection Committee (ICPC) statin it to be over 95%, the UK Policy Exchanges holds the figure at 97%, where as Parag Khanna goes even further, stating that submarine cables 'crisscross the earth like yarn wrapped around a ball, carrying 99 percent of intercontinental traffic.' Single cables within that yarn carry as much as 160 terabits of data across the Atlantic *every second*. This matter so intently simply because of the naïve impressions that seem to exist regarding cyberspace and the Internet more generally, as Blum sagely put it, 'The preferred image of the Internet is instead a sort of nebulous electronic solar system, a cosmic "cloud."' [+ADD commentary: this is due to successful marketing campaigns by technology companies to create allure around their product] Reality could not be further from the truth; cyberspace is not a purely virtual space at all, totally devoid of geography and indeed "up in the cloud." There is a physical reality to cyberspace that is made nowhere more pronounced than via submarine cables, the "tubes" through which cyberspace exists." (p. 15-17)
+ADD "Why should this matter in security terms? In the first, and worst, instance, these cables can be attacked by actors seeking to disrupt the activities of an opponent. Simply put, as a nation becomes more connected to and dependent upon cyberspace, that nation's relative vulnerability

[795] Wired Staff. "Your Own Personal Internet". *Wired Magazine.*
[796] Heath, Garrett and Oleg Svet. "We Run Wargames Programs for the Joint Staff. Here's What We've Learned". *Modern War Institute at West Point webpage*. 19 October 2018.

to cyber attack increases in kind. Furthermore, being able to disrupt the primary use of connected infrastructure through denial of access to submarine cables could have catastrophic impact upon a nation's ability to communicate, trade, and conduct financial transactions, among numerous other applications, Sunak's 2017 *Policy Exchange* paper on the insecurity of submarine cables illustrates these impacts very well, noting the case where damage caused by civilian ships to submarine cables between Italy and Egypt in December 2008 reduced traffic between Europe and the Middle East by 80%. This impacted American military forces in Iraq at the time, who had to reduce their daily unmanned aerial vehicle (UAV) sorties from Balad Air Force Base from the hundreds to the tens due to a lack of available bandwidth [move to Monopoly on Violence/Infringement section w/restatement]... whoever can master, control, and exploit the submarine cables to best effect will develop a very valuable geopolitical advantage." (p. 17-18)

As mentioned earlier, in *The CNN Effect in Action* the author writes that "Such models, like realism, assume unitary governmental decision-making with a high degree of control over implementation and access to near-perfect information," characterized by control of and information to the three domains necessary to war: "popular passions, operational instruments, and political objectives". [797]

+ADD Wargame practitioners control over internet backbone

Today, domain and IP distribution and regulation online is under the control of ICANN, an American NGO under contract and supervision by the US Department of Commerce. Vinton Cerf, a former engineer at IBM, made his name as one of the original creators of the packet-switching network, the first iteration of the modern Internet, under the funding of DARPA while a researcher at UCLA. He later became chairman of ICANN, and then Vice President of Google, Inc.[798] Other ICANN board members include: Khaled Koubaa, public policy manager for North Africa of Facebook; Manal Ismail, the Executive Director for International Technical Coordination at the National Telecom Regulatory Authority (NTRA) of Egypt; Avri Doria of the UN Working Group on Internet Governance (WGIG); Sarah Deutsch, an attorney at Verizon Communications; Ron da Silva, Executive Director for Internet Tool & Die Company and founder of a block-chain enterprise; Becky Burr, a partner at DC law firm Harris, Wiltshire & Grannis; Maarten Botterman, Senior Advisor to the Dutch Government and Scientific Officer to the Communications Technology Research program of the European Commission; Chris Disspain, member of the United Nations Secretary-General's Internet Governance Multi-stakeholder Advisory Group; and Cherine Chalaby, Executive Director of Accenture and chairman of Rasmala, a Middle East-based regional investment bank in Egypt.[799]

The notion that the US government does not have complete dominion of every domain on the Internet, including .onions (dark web sites), is absurd, as it maintains direct technical and legal control of all DNS servers, and the American NGO ICANN, formerly under direct US

---

[797] Bahador. *The CNN Effect in Action*, p. 57-58, 47.
[798] https://www.britannica.com/biography/Vinton-Cerf#ref1068958
[799] https://www.icann.org/resources/pages/board-of-directors

control until 2009 and supervision until 2016, must approve and index all Internet domains and IPs, including passing policy to approve domains in non-English characters, as in 2010, to be used exclusively abroad. The first non-English script domains were Arabic-script domains which went live in Egypt, Saudi Arabia, and the UAE in May of 2010. [800]
"Alongside the Internet, ICANN too has grown significantly during its 20 years of operating, 'from a marginal budget of less than $1 million in 1999 to $60 million in 2010 and around $160 million in 2015. ICANN is not a perfect organisation however, nor are its operation viewed as entirely objective and benevolent, instead 'many still see ICANN as captive to US interests.' Such a view persists even after the US Government's formal relinquishing of its contractual oversight of ICANN, announced in 2014 and finalised in 2016. Lucas puts the reason why in blunter terms, when he says that 'ICANN has few friends. It is seen as secretive, dominated by Western, male engineering types, and prone to security lapses.' Most significantly, however, is the suspicion among nations of the lack of government representation in this governance model, with Klimburg citing Vladimir Putin's infamous declaration that the entire Internet project was little more than a 'CIA project,' as indication of how deeply ingrained is the belief of Western bias in the governance model."[801]

The notion that onion browsing or any type of encrypted Internet service, such as most payment and log-in systems, is untraceable is also absurd. The multiple agencies and branches of the US Department of Defense and many private institutions with major government contracts such as IBM, Google, MIT, and Rice University all have quantum computers on-site which can be accessed with regular institutional login credentials.

Quantum computers have the capability to decode and trace all encrypted traffic even without access to port identifiers, as evidenced in academic research. In a paper titled "Deep Packet", a method that "can identify encrypted traffic" using neural networks[802]; "Can encrypted traffic by identified without port numbers, IP addresses and payload inspection?" which found that with machine learning "it is possible to identify encrypted traffic tunnels with high accuracy without inspecting payload, IP addresses and port numbers. Moreover, it is also possible to identify which services run in encrypted tunnels."[803]

"A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning" found that,

> it's still possible for a local observer to fingerprint top monitored sites on Alexa and Tor traffic can be classified amongst other HTTPS traffic in the network despite the use of Tor's protections... The attack assumes a local observer sitting on a local network fingerprinting

---

[800] https://www.britannica.com/topic/ICANN
[801] Steed, p. 24.
[802] Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R. et al. "Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning". *Springer*. 13 May 2019.
[803] Alshammari, Riyad & Zincir-Heywood, A. . Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?. *Computer Networks*. Vol. 55, Issue 6. Elsevier. April 2011.

top 100 sites on Alexa; results gave an improvement amongst previous results by achieving an accuracy of 99.64% and 0.01% false positive.[804]

In "Analyzing HTTPS Traffic for a Robust Identification of Operating System, Browser and Application" the author notes that,

> Desktops and laptops can be maliciously exploited to violate privacy. There are two main types of attack scenarios: active and passive. In this paper, we consider the passive scenario where the adversary does not interact actively with this he device, but he is able to eavesdrop on the network traffic of the device from the network side. Most of the internet traffic is encrypted... In this paper, we show that an external attacker can identify the operating system, browser and application of HTTP encrypted traffic (HTTPS)... We provide a large data set of more than 20,000 examples...We run a through a set of experiments, which shows that our classification accuracy is 96.06%.[805]

In the paper "I Know What You Saw Last Minute—Encrypted HTTP Adaptive Video Streaming Title Classification" researchers show,

> that an external attacker can identify the video title from video HTTP adaptive streams sites, such as YouTube. To the best of our knowledge, this is the first work that shows this. We provide a large data set of 15000 YouTube video streams of 2100 popular video titles that was collected under real-world network conditions. We present several machine learning algorithms for the task and run a thorough set of experiments, which shows that our classification accuracy is higher than 95%.[806]

"Analyzing Android Encrypted Network Traffic to Identify User Actions" shows that,

> In most attack scenarios, the adversary takes the local or remote control of the mobile device, by leveraging a vulnerability of the system, hence sending back the collected information to some remote web service. In this paper, we consider a different adversary, who does not interact actively with the mobile device, but he is able to eavesdrop the network traffic of the device from the network side (e.g., controlling a Wi-Fi access point)... using advanced machine learning techniques...show that our attack can achieve accuracy and precision higher than 95%, for most of the considered actions.[807]

Finally, in "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic" researchers study decryption used in a data

> gathering technique for adversaries, network administrators, investigators and marketing agencies… called AppScanner, for the automatic fingerprinting and real-time identification of Android apps from their encrypted network traffic...used to train our supervised learning algorithms. Our fingerprint generation methodology is highly scalable and does not rely on

---

[804] Almubayed, Alaeddin & Hadi, Ali & Atoum, Jalal. "A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning". *International Journal of Computer Network and Information Security (IJCNIS)*. 2014.

[805] Muehlstein, Jonathan & Zion, Yehonatan & Bahumi, Maor & Kirshenboim, Itay & Dubin, R & Dvir, Amit & Pele, Ofir. "Analyzing HTTPS Encrypted Traffic to Identify User Operating System, Browser and Application". 15 March 2016.

[806] Dubin, Ran et al. "I Know What You Saw Last Minute—Encrypted HTTP Adaptive Video Streaming Title Classification." *IEEE Transactions on Information Forensics and Security,* Vol. 12. 2017.

[807] Conti, Mauro et al. "Analyzing Android Encrypted Network Traffic to Identify User Actions." *IEEE Transactions on Information Forensics and Security,* Vol. 11. 2016. Electronic resource. <https://www.semanticscholar.org/paper/Analyzing-Android-Encrypted-Network-Traffic-to-User-Conti-Mancini/e46b0fe8d8be88617494c58a0f5c5cea9e0f37fb>.

> inspecting packet payloads, thus our framework works even when HTTPS/TLS is employed...We automatically profiled 110 of the most popular apps in the Google Play Store and were later able to re-identify them with more than 99% accuracy.[808]

In fact, not only are encrypted technologies not encrypted effectively, but using encrypted browsing, such as Tor, increases the length of time the NSA is permitted by policy, enacted by Attorney General Eric Holder in 2009, to hold a user's "communications that are enciphered or reasonably believed to contain secret meaning" for "any period of time during which encrypted material is subject to, or of use in, cryptanalysis," or "reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed."[809]
+ADD Steed quotes marked pgs. 12-18
+ADD From the American 2011 *International Strategy for Cyberspace* and NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) *Tallinn Manual:*
"'In particular, States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure.'… That infrastructure is clearly established, 'the physical, logical, and social layers or cyberspace are encompassed in the principle of sovereignty.' Further, to this, with *2.0*'s second rule, a strong hand is lent to the Cyber Sovereignty cause: 'A State enjoys sovereignty authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations. … a State's sovereignty in the territorial sea, archipelagic waters or straits used for international navigation is limited under customary international law by the rights of innocent passage, archipelagic sea lanes passage, and transit passage, respectively.' In essence, what the manual is saying is that while a state can exercise authority over its particular *jurisdiction* of cyberspace, it cannot do so over cyberspace itself *per se*, exactly in the same manner that a state can exercise sovereign authority over territorial waters but not lay claim to the ocean itself."[810]
+ADD **[TOPIC - Final and extremely economically damaging decision simply for conducting 'wargames' and aggressive tactic against other nations or even domestic companies. Major irrevocable forfeiture by US for sake of cyberwarfare and cyberespionage.]**

"The Domain Name System (DNS) and the Root Server System very much bring the logical and hey physical realities of cyber space together, each with interesting security concerns, as both are fundamentally intertwined and cannot be separated. In essence, the DNS is the addressing system of the Internet, which translates a user's request into an IP address to visit and/or send/receive data to/from. DNS is also sometimes referred to as the root zone, with the Root Server System acting as a distributed network of physical servers upon which to process and direct those address requests from users as they come in. The Root Server System is the top-level layer of the DNS hierarchy providing IP addresses for users, and just below this top-level layer lies the

---

[808] Taylor, Vincent F. et al. "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic." *2016 IEEE European Symposium on Security and Privacy (EuroS&P).* 2016.
[809] Goodin, Dan. "Use of Tor and e-mail crypto could increase chances that NSA keeps your data". *Ars technica.* 20 June 2013.
[810] Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019, p. 69-70.

domain level itself, where operators make provision for domain registrations like .com or .org etc…. Cyberspace cannot function without its logical layer processes of submarine cable for signals to traverse; the DNS and Root Server System is also crucial to the operation of the Internet as we know it. As without TCP/IP packets could not be created to send, without submarine cables there would be no infrastructure to send them across, and without DNS there would be no way for users to know where to send their packets."[811]

Former IBM Security special advisor Bruce Schneier writes: "What it [the Internet] can't handle is systemic attacks against the underlying protocols. The base of Internet protocols were developed without security in mind, and many of them remain insecure to this day...There's no security in the Domain Name Service that translates Internet addresses human-readable names to computer-readable numeric addresses, or the Network Time Protocol that keeps everything in synch. There's no security in the original HTML protocols that underlie the World Wide Web, and the more secure 'https' protocol still has lots of vulnerabilities. All of these protocols can be subverted by hackers," and authorized administrators.[812]

"But Sabu [an Anonymous member and FBI informant] wanted Anonymous to be more than just kids playing hacker. He wanted Anonymous to change the world...He conquered networks, then basked in his achievement. He was more interested in the cachet of taking over the entire Internet service providers (ISPs) than pranking Scientologists...He did not shy away from big targets or big talk. In his decade underground he claimed to have taken control of the domain-name systems of the governments of Saudi Arabia, Puerto Rico, the Bahamas, and Indonesia." After this hacker took over the entire IP system of Puerto Rico by criminally administrating the servers of their contractor EduPro, "the U.S. military gave control of the Vieques base [Puerto Rican island and site of U.S. Navy bomb test killing] back to the locals two weeks later," after allowing the disruption and hacker's message to remain on government websites and servers for days.[813]
https://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet/
http://domainincite.com/3370-dns-not-to-blame-for-egypt-blackout

"ISPs are generally connected to other ISPs through Internet backbone providers such as UUNET and PSINet. Backbones own or lease national or international high-speed fiber optic networks that are connected by routers, which the backbones use to deliver traffic to and from their customers. Many backbones also are vertically integrated, functioning as ISPs by selling Internet access directly to end users, as well as having ISPs as customers. Each backbone provider essentially forms its own network that enables all connected end users and content providers to communicate with one another. End users, however, are generally not interested in communicating just with end users and content providers connected to the same backbone provider; rather, they want to be able to communicate with a wide variety of end users and

---

811 Steed, p. 13-14.
812 Schneier, Bruce. *Click Here to Kill Everybody*, 22-23.
813 Olsen. *We Are Anonymous*, p. 133-34; 137-38.

content providers, regardless of backbone provider. In order to provide end users with such universal connectivity, backbones must interconnect with one another to exchange traffic destined for each other's end users. It is this interconnection that makes the Internet the "network of networks" that it is today. As a result of widespread interconnection, end users currently have an implicit expectation of universal connectivity whenever they log on to the Internet, regardless of which ISP they choose. ISPs are therefore in the business of selling access to the entire Internet to their end-user customers; ISPs purchase this universal access from Internet backbones. The driving force behind the need for these firms to deliver access to the whole Internet to customers is what is known in the economics literature as network externalities."[814]

Relocate

Even so, violent political philosophies such as mutual assured destruction, preemptive strikes, other sorts of rationalized violence in game theory, and pogroms, can justify violence, but they do not explain the propensity for violence for any given instance. They are theories acted upon, not acts theorized upon. So, the Bosnia model must have an impetus or it would not have become a model. The impetus is part of cyber-realism I have already discussed at length - the end-to-end knowledge of the effects and control of the escalation caused by radiation exposure, considered along with the profitability of radar weaponry and surveillance mechanisms. These represent the impetus for recreating 'mad' models.

The industries I and others have pointed out as most integral to instigating and profiting off of violent political upheavals, especially those outside of conflict zones - news media, law enforcement, technologists, and military - are those industries with the highest use of radiation-enabled surveillance. Even in zones and times of peace, these industries remain revolution-crazed or combatant as if *they* were under attack. In his 1946 essay on atomic weaponry *Gentlemen: You are mad!*, Lewis Mumford argued that, "The chief madmen claim the titles of general, admiral, senator, scientist, administrator, Secretary of State, even President. And the fatal symptom of their madness is this: they have been carrying through a series of acts which will lead eventually to the destruction of mankind, under the solemn conviction that they are normal responsible people, living sane lives, and working for reasonable ends."
When it comes to political violence of our own, we are accustomed to "look at madmen and pass by," as Lewis Mumford also wrote.

+ADD "Is a Mass Psychosis the Greatest Threat to Humanity?"
https://academyofideas.com/2021/02/mass-psychosis-greatest-threat-to-humanity/?utm_source=rss&utm_medium=rss&utm_campaign=mass-psychosis-greatest-threat-to-humanity

But in a look at historical viewpoints on instances of political violence, there is no lack of histories of poisoned rulers turned mass murdering tyrants, from Caligula to Fidel Castro.

---

[814] Kende, Michael. "The Digital Handshake: Connecting Internet Backbones". *OPP Working Paper*, No. 32. Office of Plans and Policy, Federal Communications Commission. September 2000. Working paper.

The industries I and others have pointed out as most integral to instigating and profiting off of violent political upheavals, especially those outside of conflict zones - news media, law enforcement, technologists, and military - are those industries with…

When it comes to revolts made by whole swathes of leaderless people, Mary Matossian's short 1984 article *The Time of the Great Fear* on the French riots of 1789 offers a useful critique. Matossian notes that, similar to the Arab Spring protests, the French riots would been lost to history if they had not preceded the French Revolution. Matossian analyses ...(in pdf emailed) rumors of brigands, burning, looting, precursor to French revolution, article says due to rumors, and paranoia from ergot poisoning - a fungus in the wheat chaffs that caused millennial hallucinations at the same time in other European countries. [MOVE QUOTE to Afterthoughts?] +QUOTE: "In any event, it is also important to note that ergot seems to arouse a wide range of unusual and often colorful mental states and that these were unusually frequent in France in the fall of 1789. In Grenoble, a group of convulsionaries preached that the return of the Jews was imminent, that 'Elias has come, that he is getting ready to carry out his mission very soon,' and that the 'reign of a thousand years of Jesus Christ is at the point of beginning.' In Périgord, the prophetess Suzette Labrousse, who had visions of heaven and hell, began to gain a following not long after the Great Fear. The American historian Clarke Garrett has observed: 'In 1789 and 1790, it was widely believed in France that religion and revolution would triumph together.' Millennial hallucinations, possibly triggered by ergot poisoning, were also reported in Scotland, Sweden, and the United States in the eighteenth and early nineteenth centuries. It appears, then, that the role of ergot was to create a suggestive state of mind and to distort perceptions in its victims, while political and cultural factors determined the precise nature of the interpretations that victims place upon their symptoms. In some cases, the suggestible mental state manifested itself as visions of brigands coming to steal crops; in others, as apparitions of the millennium. Many factors besides ergot gave these visions shape and color and conditioned reactions of fear or of religious fervor."[815]

Mumford himself, while he admits he too is affected by nuclear culture, writes that "madmen are planning the end of the world," in reference to making the atomic bomb. Despite his clarity on the detrimental effects of atomic energy and culture, he displays the millennialism Matossian describes. I address at greater length the possible relation between the mental effects of some types of poisoning, sometimes intentional as irregular warfare, revolution, and political millennialism in the section The Greater Middle East Plan. [REWORD]

Recent Developments and Research and Development

"York," Pyle said, "wrote that what the East needed was a Third Force." Perhaps I should have seen the fanatic gleam, the quick response to a phrase, the magic sound of figures; Fifth Column, Third Force, Seventh Day. I might have saved us all a lot of trouble,

[815] Matossian, Mary Kilbourne. "The Time of the Great Fear". *Sciences,* 38-41. New York Academy of Sciences. 1984, p. 41.

even Pyle, if I had realized the direction of that indefatigable young brain.
Graham Greene, *The Quiet American*

The funding cycle of violence, shocking developments publicized will result in more demand for research and development, part of the cyclical mechanism described in this section. Mutual perpetuation of R&D with 'bad policy' is self-evident in modelism and the state of arrested political and scientific development populations find themselves in.

"G. K. Chesterton's classic spy novel, *The Man Who Was Thursday* (1908), centers on a secret society of seven revolutionaries, known as the Central Anarchist Council, sworn to destroy the world. For security reasons, the anarchists call themselves by the names of the days of the week—Sunday, Monday, and so on. **As the plot unfolds, we learn that all of the anarchists, with the exception of Sunday, are actually undercover agents** working for the ultrasecret New Detective Corps organized by Scotland Yard to overthrow the Anarchist Council. The Corps is so shadowy that none of its agents knows of the others' true identities or purposes. The story ends when Sunday, the lone anarchist and mastermind of the Council, manages to escape the pursuit of Scotland Yard by revealing that he, too, is not who or what he appears to be; in fact, he is not even human: [Sunday's face] grew larger and larger, filling the whole sky; men everything went black. In the end, anarchy triumphs; … Just as six of the Council members prove to be law-enforcers in anarchists' clothing fighting a nonexistent (non-human, at least) threat, neo-realist states are all security-maximizers, who, because they exist under anarchy, sometimes act like aggressors, though none has any interest in non-security expansion. Also, **just as in Chesterton's tale there is no concrete anarchist society, only the inextinguishable threat of anarchy, in neorealism, insecurity is caused not by greedy actors but by die inescapable self-help nature of the system."**[816]

+ADD "An unbroken arc of knowledge and power connects the European or Western statesman and the Western Orientalists; its forms the rim of the stage containing the Orient. By the end of World War I both Africa and the Orient formed not so much an intellectual spectacle for the West as a privileged terrain for it. The scope of Orientalism exactly matched the scope of empire, and it was this absolute unanimity between the two that provoked the only crisis in the history of Western thought about and dealings with the Orient. And this crisis continues now."[817]
+ADD "Beginning in the twenties, and form one end of the Third World to the other, the response to empire and imperialism has been dialectical… Unable to recognize 'its' Orient in the new Third World, Orientalism now faced a challenging and politically armed Orient. Two alternatives opened before Orientalism. One was to carry on as if nothing had happened. The second was to adapt the old ways to the new. But to Orientalists, who believes the Orient never changes, the new is simply the old betrayed by new, misunderstanding dis-Orientals (we can permit ourselves the neologism). A third, revisionist alternative, to dispense with Orientalism altogether, was considered by only a tiny minority. One index of the crisis, according to Abdel Malek, was not simply that 'national liberation movements in the ex-colonial' Orient worked

[816] Schweller, Randall L. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3. 24 December 2007, p. 90.
[817] Said, Edward. *Orientalism*. Vintage Books: New York. 1978, p. 104-105.

havoc with Orientalist conceptions of passive, fatalistic 'subject races'; there was in addition the fact that 'specialists and the public at large became aware of the time-lag, not only between orientalist science and the material under study, but also – and this was to be determining – between the conceptions, the methods and the instruments of work in the human and social sciences and those of orientalism.'… The impact of colonialism, of worldly circumstances, of historical development: all these were to Orientalists as flies to wanton boys, killed – or disregarded – for their sport, never taken seriously enough to complicate the essential Islam."

+ADD Bizarre propagandistic rhetoric advertising not the Middle East, advertising research guide to the confusion caused by same policy research industry. UN translator author. "Lost in the Labyrinth: What's Really Going On in the Middle East?": "If you have been following recent events in the Middle East and you are confused by the tangled web of wars and proxy wars, sectarian splits, revolutions, and counter-revolutions that are convulsing the region, do not worry. You are not alone. Policy makers, prime ministers, and presidents alike have been wrong-footed by the dizzying speed of change as the old order in the Arab world collapses and a new one fights its way into existence. The post-Arab Spring Middle East is rife with contradictions, inconsistencies, and the kind of complications that make your head spin. Finding your way through this labyrinth is no easy task… If all of this leaves you wondering what's really going on in the Middle East, how this mess happened, and what is likely to happen next, the place to start looking for answers is not in the great imperial Arab cities of Baghdad, Cairo, or Damascus. It is not even in the sacred cities of Mecca, Medina, or Jerusalem**. The place to start looking is not in the Middle East at all. It is in the Balkan city of Sarajevo** where on a sunny summer day, over a century ago, a man driving a car took a wrong turn and changed the course of history."[818]

The Bosnia Model, The Rumsfeld Model

Hegel remarks somewhere that all great, world-historical facts and personages occur, as it were, twice. He has forgotten to add: the first time as tragedy, the second as farce.
Karl Marx, *The Eighteenth Brumaire of Louis Bonaparte*

+ADD "**Most of the small wars** of the United States have resulted from the obligation of the Government under the spirit of the Monroe Doctrine and **have been undertaken to suppress lawlessness or insurrection**. Punitive expeditions may be resorted to in some instances, but **campaigns of conquest are contrary to the policy of the Government of the United States**."[819]

[TOPIC - RAND Corporation's significance of the Rumsfeld Model - civilian control of military, but military (DoD) headed by civilians – implication: war crimes punishable]

The Rumsfeld Model is a model of strategically placed incompetents in decisionmaking roles. In *Succession Management for Senior Military Positions The Rumsfeld Model for*

[818] McMillan, M.E. *From the First World War to the Arab Spring: what's really going on in the Middle East?* Palgrave MacMillan: NY. 2016, p. 1.
[819] U.S. Marine Corps. *Small Wars Manual.* Department of the Navy: Headquarters United States Marine Corps. 1940. Reprint 22 December 1990, p. 2.

Secretary of Defense Involvement, the RAND Corporation analysts describe what they have termed 'The Rumsfeld Model'. The model is applied "when, **for development purposes, an individual is deliberately placed in a position for which there were better-qualified candidates**, the placement will best benefit the organization if it is part of a carefully considered career path."[820]

+ADD "One major consequence of the Arab Spring, the anti-government uprising that spread across the Middle East more than six years ago, and the geopolitical tumult that followed has been that new smuggling and trafficking routes and networks throughout the Middle East and North Africa have emerged, with criminal groups and terrorist organizations taking advantage of continued instability in key geographic hubs throughout the Mediterranean region… The modus operandi ISIS has developed for funding foreign fighter travel and for financing external operations to conduct attacks in the West works particularly well with a local criminal funding model. This model fits into how ISIS conceives of extra-territorial contributions on a tactical level."[821]
+ADD "That's the issue here – Serb repression has long since passed the point of legitimate self-defence. This is what gives outsiders the grounds – if not the right – to intervene in a civil war. Besides, Kosovo is too strategically placed for its troubles ever to be just an internal matter. If Kosovo exploded, other countries could well go up in flames with it."[822] Perspective of opinion-maker journalist and commentator for *The New Yorker*.

In academic discourse models are used to detail an instance of methodology or best practices for the purpose of instructing others how to recreate a successful experiment or policy. I will show here that the Yugoslav War (1991-1995) and genocide in Bosnia has become a model used by US politicians and foreign policy advisors for more recent wars involving the US and NATO. I point out this model in order to show that its recreation, with all the devastating consequences, is deliberate. Awareness of the deliberate misuse of policy modeling can prevent the continued recreation of devastating and insidious policy if informed action is taken to prevent the policy from being enacted.

+ADD "As I tried to point out in discussing **how von Manstein persuaded Hitler to try to attack** through the Ardennes Forest, **it sometimes takes only one persuasive person with a bright idea, plus one gambling decision maker with authority**, to result in a situation where a government might move in a direction which 99 per cent of a bureaucracy think inadvisable. Indeed, most of the bureaucracy may not even hear about the idea until it is too late to register objections."[823]
+ ADD "This was borne out in judgments handed down by the International Criminal Tribunal for the former Yugoslavia (ICTY). The Stakić Trial Chamber heard evidence of a group of male prisoners, half of whom were 'naked from the waist-down and standing, and half the group was kneeling. According to Witness B: "They were positioned in such a way as if engaged in intercourse. "' Before the Cesić Trial Chamber, Cesić admitted intentionally forcing at gunpoint two detained Muslim brothers to perform fellatio on each other in the presence of other people.

---

[820] Hoehn, Andrew R., Albert A. Robbert, and Margaret C. Harrell. *Succession Management for Senior Military Positions The Rumsfeld Model for Secretary of Defense Involvement*. The RAND Corporation. 2011, p. 14.
[821] Clarke, Colin P. "ISIS Is So Desperate It's Turning to the Drug Trade". *The RAND Blog*. 25 July 2017.
[822] Ignatieff, Michael. *Virtual War: Kosovo and Beyond.* Metropolitan Books. 2000, p. 21.
[823] Kahn, p. 446.

The Blagoje Simić trial judgment notes that, ‘ [s]everal Prosecution witnesses gave evidence that detainees were subjected to sexual assaults. One incident involved ramming a police truncheon in the anus of a detainee. Other incidents involved forcing male prisoners to perform oral sex on each other and on Stevan Todorovic, sometimes in front of other prisoners ’ . The Todorovic sentencing judgment itself notes that Todorovic accepted that he ordered Witness C and Witness D to perform oral sex on each other and ordered Witness E and Witness F to do the same, laughing while it went on. There is also the notion of ‘ rape plus ’ , the ‘ plus ’ being HIV/AIDS, forced pregnancy for women, or another consequence of rape, which may have been the very purpose for the rape in the first place. For example, in Kosovo, the OSCE reported one interviewee recounting that, ‘ he saw two male detainees being raped by two policemen who declared that they had AIDS… Perhaps the best evidence of genital violence comes from the conflict in the former Yugoslavia, not necessarily because this was the conflict that had the highest incidence of that practice but because it is the conflict that has been the most thoroughly investigated in terms of sexual violence… A number of other forms of sexual violence are committed in armed conflict in addition to rape and enforced sterilization. The imagination of perpetrators in this regard knows no bounds… Of Kosovo, it has been noted that, outside situations of detention, the most common way of sexually humiliating men was to force them to strip naked in public. There are reports of men being made to repeatedly undress and dress, undress and stand naked for periods of time and undress in front of a group of women. Another infamous incident involving the forcible nudity of men is that **relating to the treatment of prisoners at Abu Ghraib.**”[824]

+ADD “This episode in particular is a clear example of Lucas Kello’s state of *unpeace* prevailing, whereby there is not a clear war at play, even a cold one, but an attack on the political process itself that seeks to undermine truth and trust, approaching Snyder’s chilling warning that ‘Post-truth is pre-fascism.’ Moore is also correct in his warning that the events of 2016 should be seen ‘not as anomalies, but as models for what is coming next.’”[825]

+ADD “Our effort should be accompanied by a preventive strategy that is as much, or more, political as it is military. The strategy must focus clearly on the Arab and Muslim world, in all its variety. Our strategy should also include defenses. America can be attacked in many ways and has many vulnerabilities. No defenses are perfect. **But risks must be calculated; hard choices must be made about allocating resources.** Responsibilities for America's defense should be clearly defined. Planning does make a difference, **identifying where a little money might have a large effect. Defenses also complicate the plans of attackers, increasing their risks of discovery and failure. Finally, the nation must prepare to deal with attacks that are not stopped.** Measuring Success: What should Americans expect from their government in the struggle against Islamist terrorism? **The goals seem unlimited: Defeat terrorism anywhere in the world.** But Americans have also been told to expect the worst: An attack is probably coming; it may be terrible. **With such benchmarks, the justifications for action and spending seem limitless.** Goals are good. **Yet effective public policies also need concrete objectives. Agencies need to be able to measure success.** These measurements do not need to be quantitative: government cannot measure success in the ways that private firms can. But the targets should be specific enough so that **reasonable observers-in the White House, the Congress, the media, or the general public-can judge whether or not the objectives have**

[824] Sexual Violence against men in conflict, P. 264-266
[825] Steed, p. 46.

been attained. Vague goals match an amorphous picture of the enemy. Al Qaeda and its affiliates are popularly described as being all over the world, adaptable, resilient, needing little higher-level organization, and capable of anything. **The American people are thus given the picture of an omnipotent, unslayable hydra of destruction. This image lowers expectations for government effectiveness. It should not lower them too far.** Our report shows a determined and capable group of plotters. Yet the group was fragile, dependent on a few key personalities, and occasionally left vulnerable by the marginal, unstable people often attracted to such causes."[826]

+ADD "'What we see is that in the aftermath, a lot of the concerns about the communities directly affected and what can be done for them end up being bargained away.'"[827] Reference to game theory gambling model in use in conflict resolution and reparations, article also cited under The Hacker's Arsenal

+ ADD "Relying mainly on Wikileaks cables and the websites of key CIA pass through foundations (which he reproduces in the appendix), Bensaada methodically lists every State Department conference and workshop the Arab Spring heroes attended, the dollar amounts spent on them by the State Department and key "democracy" promoting foundations3, the specific involvement of Google, Facebook, Twitter and Obama's 2008 Internet campaign team in training Arab Spring cyberactivists in encryption technologies and social media skills, US embassy visits, and direct encounters with Hillary Clinton, Condoleezza Rice, John McCain, Barack Obama and Serbian trainers from CANVAS (the CIA-backed organization that overthrew Slobodan Milosevic in 2000)."[828]

+ADD background to 1990s Bosnia, 2019 US Congressional resolution to condemn Armenian genocide without mention of current Armenian genocides (re: UN official refusal to admit knowledge of events in countries), despite Congress having already publicly condemned those Armenian massacres 120 years earlier when those massacres were ongoing. The US Congress in 1896 condemned the Ittihadist genocide of Armenians. "In response to the reports of the ongoing massacres in the 1894-96 period, the U.S. Senate unanimously passed a resolution in 22 January 1896 condemning them."[829]

On December 12, 2019, the US Congress publicly condemned the 1894-96 Armenian genocide in a redundant resolution of strategic non-binding brinksmanship: "Turkish foreign minister Mevlut Cavusoglu called the decision a 'political show' while presidential spokesman Ibrahim Kalin said Ankara strongly condemned and rejected the measure. The resolution is nonbinding. 'History will note these resolutions as irresponsible and irrational actions by some members of the US Congress against Turkey,' Fahrettin Altun, Turkey's communications director, said on Twitter in response. Congressional aides said the White House does not want the legislation to move ahead while it negotiates with Ankara on sensitive issues. However, since the visit, Erdogan repeatedly said **Turkey has no intention of dropping the Russian S-400 air defense missile systems it has bought, crushing any hopes for progress**… They have also

---

826 https://govinfo.library.unt.edu/911/report/911Report_Ch12.htm
827 https://www.independent.co.uk/news/world/middle-east/isis-sex-slaves-lamiya-aji-bashar-nadia-murad-sinjar-yazidi-genocide-sexual-violence-rape-sakharov-a7445151.html
828 https://www.globalresearch.ca/the-arab-spring-made-in-the-usa/5484950
829 Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 90.

moved to punish Turkey over its Oct. 9 incursion into Syria. **A U.S. Senate committee backed legislation on Wednesday to impose sanctions on Turkey**, pushing Trump to take a harder line on the issue, as many lawmakers blame Trump for giving a green light to Ankara for its military offensive. To become law, that legislation would have to pass the House of Representatives, which passed its own Turkish sanctions bill by an overwhelming 403-16 vote in October, and be signed by Trump."[830] [REWORD]

Since the December 2019 resolution and sanctions, armed conflict has broken out in Armenia and surrounding countries with *Armenia* being accused of aggressively using Russian missiles and committing war crimes.
+ADD relate to political sanctions, arms embargos, shifting media narrative on group guilt/victimhood, and the escalation to genocide in Bosnia in 1990s, the Bosnia Model
"Armenia and Azerbaijan: What Sparked War and Will Peace Prevail?" https://www.nytimes.com/article/armenian-azerbaijan-conflict.html?action=click&module=RelatedLinks&pgtype=Article
"Armenia's war crimes exposed at UN Congress" 8 March 2021 https://www.azernews.az/nation/176916.html ;

Armenia's Prime Minister, Nikol Pashinyan, Warns of an Attempted Coup" 3/2021 https://www.nytimes.com/2021/02/25/world/europe/armenia-coup-pashinyan.html ;
"Azerbaijan-Armenia conflict: Israeli defence system shot down Russian missile Yerevan fired at Baku" https://www.middleeasteye.net/news/azerbaijan-armenia-israel-russia-missile-fired-shot-down 3 March 2021 ; "Armenia destroyed Karabakh's cultural heritage: Azerbaijani envoy" https://www.dailysabah.com/world/europe/armenia-destroyed-karabakhs-cultural-heritage-azerbaijani-envoy 4 March 2021

"Muş Vice Consul Hampton reported that all Muslims were implicated in the massacres, which were carried out on order form 'central authorities,' and 'of the existence of which [order] I have no doubt.' Prisoners were released from prison for this task. Sivas Vice Consul Bulman reported on 4 February 1896 of having 'definite proof that the massacres were prearranged.' Harput Vice Consul Fontana provided a clue as to how massacres could be ordered form the Palace without any explicit use of the world itself, or anything similar to it… Fontana was able to reconstruct the sequence of events through the disclosures of a Turk who was connected to the state Telegraph Office. That office received a telegram from the Palace ordering Harput province authorities 'to take the necessary action' against the Armenians at Agn, who 'intended to create a disturbance.' The machinery for massacres was immediately set in motion by the Military Commandant issuing the appropriate telegraphic orders to Agn officials… Even though the Germans studiously avoided pressuring the sultan, or remonstrating against him [as WWI allies], Kaiser Wilhelm II's Ambassador Saurma reported on a widely held view that the atrocities were the result of the Muslims having been spurred on by low level local authorities… But, in a further report he told his Foreign Office in Berlin that ' the most diverse sources assure us that

[830] https://www.reuters.com/article/us-usa-turkey-armenia/u-s-senate-passes-resolution-recognizing-armenian-genocide-angering-turkey-idUSKBN1YG2DZ

the Armenian massacres were enacted mostly as a result of secret orders emanating from the Palace.'"[831]

"The Kosovo conflict looked and sounded like a war: jets took off, buildings were destroyed and people died. For the civilians and soldiers killed in air strikes and the Kosovar Albanians murdered by Serbian police and paramilitaries the war was as real – and as fraught with horror – as war can be. **For the citizens of the NATO countries, on the other hand, the war was virtual. They were mobilized, not as combatants but as spectators. The war was a spectacle: it aroused emotions in the intense but shallow way that sports do.** The events in question were as remote from their essential concerns as a football game, and even though the game was in deadly earnest, the deaths were mostly hidden, and above all, they were someone else's. **If war becomes unreal to the citizens** of modern democracies, will they care enough to restrain and control the violence exercised in their name?... The result suggests that if we won a victory, it too was virtual. It was the kind of war fought by peoples who have known fifty years of peace; the kind of war a nation fights when it wants to, not when it must, when values rather than survival are on the line; when commitment is intense but also shallow… Kosovo broke new ground. It was a war fought for a new end: the defense of a party to a civil war within a state. It was fought without ground troops, in the hope and expectation that there would be no causalities at all. And so it proved. Technological mastery removed death from our experience of war. But war without death – to our side – is war that ceases to be fully real to us: virtual war."[832]

"it appears that the [1894 Sassoun, 1885 and 1886 Istanbul, and 1895 Urfa cathedral burning] massacres were not without a subsidiary purpose, namely, as a probative effort which retrospectively may be characterized as a rehearsal for the subsequent 1915-18 cataclysm."[833]

"The British, French, and Russian Consular delegates of the Sassoun Inquiry Commission submitted a sixty-page joint report. In it, they asserted that 'the refusal of seven of eight wards' of a village to pay taxes, or 'some isolated acts of brigandage' by an Armenian band, or some Armenian 'resistance to the troops' did not constitute 'an open revolt' as claimed by Ottoman authorities. The delegates further maintained that these deeds did not warrant the disproportionately severe measures of repression that included burning victims alive, wounding and killing 'without distinction of age or sex,' and especially 'old people, the sick, and children,' who were unable to flee. In a separate memorandum, attached to the Joint Report, the British delegate Shipley dismissed Turkish charges as 'the pseudo revolt, or the pretended outrages' of the Armenians, concluding: '… it is not too much to say that the Armenians were absolutely hunted like wild beasts, being killed wherever they were met."[834]

---

[831] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 87-89.
[832] Ignatieff, Michael. *Virtual War: Kosovo and Beyond.* Metropolitan Books. 2000, p. 3-5.
[833] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 85.
[834] Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 86.

"In the west, we see a complete media darkness where it comes to Yugoslavia, because world global networks have been assigned the task of being an instrument of war and of disinforming the public."[835] Milosevic at The Hague War Crimes Trials

“Accused informed of the campaign through media reports. The Chamber also heard evidence that the sniping and shelling of civilians was widely covered in the press, and that the Accused closely followed this coverage. Events in Sarajevo were particularly well covered by the media, reporters from the international press corps were common in Sarajevo, and the media was critical of violations of international humanitarian law in the city. Sniping incidents in particular received widespread coverage in the press. Furthermore, UNPROFOR protests would be publicised through journalists and a statement would be made at the daily press point, which sometimes elicited a written response from the Bosnian Serbs or the Bosnian Muslims denying what was said.16337 [REDACTED] the Accused, Krajišnik, Plavšić, and Koljević had information from television and newspapers at their disposal, and were very well-informed about what the international media was saying about events in BiH.16338 4849. Martin Bell also thought that the Accused was well-aware of his reports on the situation in Sarajevo, including the sniping and shelling of civilians, and testified that on one occasion the Accused took issue with a specific BBC report and phoned BBC News to complain.16339 Similarly, Van Lynden testified that both the Accused and Mladić told him that they watched Sky News and other international broadcasts.16340 According to Van Lynden, the Accused was eager to speak to Sky News because he considered it important to be able to put his point of view on one of the more important news organisations.16341 Van Lynden also concluded from meetings with Mladić that Mladić followed the news and was fully aware of what was happening.16342 In September 1992, Van Lynden referred to Mladić as the “scourge of Sarajevo” in a Sky News report of an interview conducted with Mladić. 16343 Van Lynden testified that when he saw him next, Mladić “seemed very happy with the title” and “rather proud of it”. 16344 4850. According to [REDACTED], the three parties to the conflict were all “very, very concerned about the international coverage of the events” in BiH and “very, very well informed by different means about what was being said about their activities or actions in the conflict”. On the basis of the Bosnian Serbs’ comments on news stories by organisations such as BBC or CNN, and on the basis of his visits to Pale, [REDACTED] thought that the Bosnian Serbs received information through Belgrade, from all the foreign embassies of Yugoslavia, and were also well-informed in terms of press clippings and international television coverage. 16346 [REDACTED] testified that the Accused “normally had with him all these clippings and reports on the international media”.16347 According to [REDACTED], the Accused would blame the international media for being part of a “complex plot against the Bosnian Serbs”.”[836]

+ADD RAND publication 10 Common Pitfalls definition of modeling “MODELISM: We shall start by considering what is to many people, the heart and soul of Systems Analysis—the use and abuse of models. We have already explained that it is necessary to use idealized

[835] https://www.theguardian.com/world/2002/feb/14/warcrimes1
[836] https://www.icty.org/x/cases/karadzic/tjug/en/160324_judgement.pdf P. 1983-85

models which abstract essentials and make assumptions explicit." RAND's foremost founder then goes on a lengthy explicit analogy of a young (in 1957) systems analyst who may end up looking at pin-up pictures of female models rather real women, and adds an equally lengthy footnote stating that:

> There are delectable girls all around to tempt our 'mature heterosexual adult' away from this dummy, but what can our poor Systems Analyst replace his model with? Another one! Even if he wanted a war he couldn't have one. (Of course, as any psychologist will tell you, the comparison is not so unfair. Some fantasies are nicer than some real girls.)

Researchers looking at early RAND Corporation publications for information on foundations of their methodologies, concerning Modeling or otherwise, will encounter little of use on the actual topic, and instead a lot of posturing drivel meant to mean practically nothing of use. This is likely intentional in order to hide how they have in fact practiced and how they have no true methodologies at all. Except of course what is revealed – that analysts have been trained since the existence of such jobs to treat their jobs as opportunities for sexual exploitations and are trained to consider war as opportunity for personal sexual predation.

This is an example of how brazenly ridiculous think-tanks like RAND have been since their inception, and they have been encouraged and funded only by the like-minded. The highly sexualized frameworks in which their analysts have long been encouraged to view war and analysis is explained in recent US war histories. It is no mystery at all why sex crimes of human trafficking, pedophilia, rape, and sexual tortures of prisoners are so ubiquitous today in American intel-security industries; US security analysts have been trained for 70 years to treat their appetite for war as a sexual appetite and their sexual appetite as an appetite for war. I, however, do not call this orientation 'mature', 'male', nor 'heterosexual'.[837]

In the section titled The Bosnia Model, The Rumsfeld Model, I relay Congressional testimony given by RAND Board Trustee, former RAND analyst and then-Secretary of Defense Donald Rumsfeld in which he defends the Department of Defense's contracting with DynCorp despite their proven crimes in child and female human trafficking in the Balkans from 1991 to 2005 (?), when the hearing took place. The discussion on the Rumsfeld Model as termed by the RAND Corporation in their recent (ADD year) publication *The Rumsfeld Model*…. These considerations combined with further information of the nature of the revolutions (if they are called that at all any longer) in the former Yugoslavia will give the reader a picture of how the US forms foreign policy decisionmaking from the embryonic stage to the infanticide stage.

"As extremely bloody wars were being fought on the ground, a war of words took place through magazines, journals, newspapers, and books, as well as on television, the radio, and the internet. All modern means of communication were actively subordinated to the goals or ethnic nationalist leaders in Serbia and Croatia, seeking to promote revised images of the respective histories."[838] …Cont to page 2

---

[837] Kahn, Herman and Irwin Mann. *Ten Common Pitfalls.* The RAND Corporation, Santa Monica, California. 17 July 1957, p. 1-2.

[838] MacDonald, David Bruce. *Balkan holocausts?: Serbian and Croatian victim-centered propaganda and the war in Yugoslavia.* Manchester University Press, 2002, p. 1.

"Another characteristic shared by both Serbs and Croats was the frequent use of the internet to disseminate nationalist propaganda. Vast networks connected literally thousands of different sites together, may with complete online books, journals, and magazines, which could be downloaded free of charge. Most nationalist publications available as hard copies could similarly be found floating in 'cyberspace'. Many books and journals that were available only as hard copies in the first two years of the conflict were duly scanned and uploaded into various government websites, with all the scanning mistakes intact. The use of this new medium made many of the historical debates between these two sides extremely vibrant and dynamic… An interesting aspect of Croatian propaganda was how the focus of attack shifted after 1991. Before Serbia became a threat to Croatian autonomy, Croatian nationalists had little interest in Serbian leaders or Serbian history. Their only true enemies were the Communists, who were solidly in control of SFRY [Socialist Federative Republic of Yugoslavia]. It was only after Serbian machinations in eastern Slavonia and the Krajina that any coherent study of Serbian history seems to have taken place. It was only at this time that a Serbian history of evil was truly brought to the forefront."[839]

+ADD Bosnia genocide and intervention led to the intervention in Kosovo in public discourse. After backing Bosnia (while keeping arms embargo against Bosnia) failed to oust Milosevic, then… +ADD the bombing of the Belgrade television station headquarters by NATO April 1999. Re: https://www.aljazeera.com/archive/2005/11/200841015162799655 9.html "The transcript of the pair's talks during Blair's 16 April 2004 visit to Washington allegedly shows Bush wanted to attack the satellite channel's headquarters in Doha, Qatar… Aljazeera's coverage of the war in Iraq had drawn criticism from Washington after the US-led March 2003 invasion. A source told the Mirror: "The memo is explosive and hugely damaging to Bush. 'He made clear he wanted to bomb Aljazeera in Qatar and elsewhere.'… The newspaper said **that the memo "casts fresh doubt on claims that other attacks on Aljazeera were accidents".** It cited the 2001 direct hit on the channel's Kabul office in Afghanistan. In April 2003, an Aljazeera journalist died when its Baghdad office was struck during a US bombing campaign. Nabil Khoury, a US State Department spokesman in Doha, said the strike was a mistake. In November 2002, Aljazeera's office in Kabul, Afghanistan, was destroyed by a US missile. None of the crew was at the office at the time. US officials said they believed the target was a terrorist site and did not know it was Aljazeera's office."[840] [Re: information warfare]

+ADD "**As many as eight station offices may have been raided on Saturday. The Saudi-owned Al-Arabiya news channel said masked gunmen who arrived in black cars wearing black clothes had stormed the offices of the station on Saturday evening, beating up some of the employees and smashing equipment** before they fled, The Associated Press reported. The channel had been receiving threats for several days, its Baghdad correspondent, Majed Hamid, said. Unidentified gunmen **also raided the offices of Iraq's Dajla and NRT news channels** in Baghdad, according to employees at the stations, both privately owned. Iraqi analyst Hiwa Osman said **the Baghdad offices of Arabiya Hadath, Fallouja, Al-Ghad al-Araby, Al-Sharqiya and Sky News Arabia were also attacked.** 'They ransacked the offices, destroyed their equipment and broadcast facilities,' she said in a tweet on Saturday night. Sharing a testimony she said had been gathered from an employee of one of the stations, Osman wrote:

---

[839] MacDonald, David Bruce. *Balkan holocausts?: Serbian and Croatian victim-centered propaganda and the war in Yugoslavia.* Manchester University Press, 2002, p. 125.
[840] Al-Jazeera Staff. "Memo: Bush wanted Aljazeera bombed". *Al-Jazeera.* 22 November 2005.

'Armed men... lined up the staff on the floor. **They beat the staff up, took their wallets & phones. They took all the computers and the safe. They broke all the video walls and all the built-in equipments. They burnt down the studios we presented our programmes from and left. They did the same with the other channels.'** No group has claimed responsibility for the raids, but **press freedom advocates have placed the blame on the Iraqi government**, either for explicitly ordering the attacks or failing to intervene. **Critics say the attacks are part of a government plan to suppress local coverage of the protests.** Internet restored: Iraq on Sunday morning lifted a block on internet **and social media access, an internet monitor said**. Access to social media sites including Facebook and Twitter was blocked on Wednesday, according to watchdog NetBlocks, with internet access sporadic until a complete net blackout on Thursday. **The internet shutdown had prohibited most of the country - barring the autonomous Iraqi Kurdistan region - from going online**… The mostly **leaderless protests** have been concentrated in Baghdad and in predominantly Shia areas of southern Iraq, bringing out jobless youths and university graduates who are suffering under an economy reeling from graft and mismanagement."[841]

+The Libya Model https://thehill.com/homenews/administration/460921-trump-bolton-wasnt-in-line-with-my-agenda
https://www.youtube.com/watch?v=M6QIopgwuIU&feature=youtu.be Bosnia: Cradle of modern jihadism? BBC News 4 July 2015

"Moreover, **in most cases, as we have seen in the Balkans and now in Libya, NATO-led operations** can count on only a limited number of member nations to contribute forces that will assume combat or strike roles in any given operation."[842]

Brookings Institute Michael O'Hanlon in 2015 *Defense News* commentary "Who Will Hold Together the Future Syria?": "In conflicts like this, when hatreds have been so inflamed by brutality on all sides, when distrust is rampant, when many so-called moderates have been either killed or radicalized, and when there is likely to be no clear battlefield winner…", "**Much more realistic is something like a Bosnia model of federalism, along the lines of what Joe Biden proposed for Iraq in 2006. Syria would have a central government, but a weak one**. Al-Assad would be gone, and ISIL, as well as the al-Nusra Front defeated. Most governance would occur regionally. The Kurds would have a zone in the northeast; Alawites would create an autonomous area where many live now along the Mediterranean coast. Two or three Sunni-majority regions would form in the nation's south as well as its north/central zones. A final region, and the most difficult to police, would include much of the intermixed population belt running from Damascus through Homs and Hama up to Aleppo. Ideally, most parts of it would remain intermixed, with Sunnis and Alawites and Christians living together, though some soft partition might become necessary. International peacekeeping forces could concentrate their efforts along the borders separating the autonomous zones and within the central multi-sectarian area, where **they would seek to build a new Syrian security force. The Bosnia mission started with some 60,000 NATO troops in a country with one-fifth Syria's population. But**

[841] https://www.albawaba.com/news/masked-men-attack-offices-satellite-tv-stations-iraq-1313065
[842] Francois, Isabelle. "NATO and the Arab Spring", p. 3.

it was almost surely oversized, since NATO militaries had few competing demands at the time. So a Syria mission might require 100,000 or so foreign peacekeeping troops at first. Perhaps 10,000 to 20,000 of the troops would have to be American, in order to provide adequate military muscle and logistical capabilities.", "Envisioning an enforceable peace deal based on the declared goal of confederation makes more sense than throwing another Hail Mary in the peace talks in Geneva."[843]

Brookings' O'Hanlon in 2013: "We need a debate about the right exit strategy in Syria before we enter into the war. The right model is neither Iraq, nor Afghanistan nor Libya, but the country of Bosnia and Herzegovina."[844]

Brookings' O'Hanlon in 2007: "As Bosnia expert Edward P. Joseph and I have recently argued, building on the ideas of Sen. Joe Biden and Leslie Gelb, something akin to a Bosnia model for Iraq would make more sense."[845]

[move this section?] The Brookings Institute's O'Hanlon has also issued advice to the 2006 House Armed Services Subcommittee on satellite warfare, urging increased research and development for *surveillance of reconnaissance satellites*: + ADD "**If the US does not protect its Earth-orbiting satellites, the equivalent of a car bomb in space could take the economy back to the 1950s**, according to witnesses testifying in Washington DC earlier this week. **'We are at an unusually good moment for the US in space, and it won't last,' Brookings Institution fellow Michael O'Hanlon told the US House armed services subcommittee on Tuesday. 'It can't last.'** US Global Positioning System satellites and commercial telecommunications satellites already face jamming from low-tech weapons on the ground. **But a looming threat, said witnesses, is a weapon launched into space to directly attack a satellite or to detonate a nuclear device that could fry the electronics of many satellites at once. Such an attack could cripple US military capability and also affect day-to-day civilian life. For example, credit card transactions are authorised through satellite communications links, and most cable channels are beamed down to Earth through satellites**. 'We don't worry as much about nuclear attacks on our satellites as we used to, and I think that's a mistake,' O'Hanlon says. Radiation belts: The Outer Space **Treaty of 1967** bans nuclear weapons in space. **But in a wartime situation, a country might put a bomb into low Earth orbit and detonate it with a timer or remote control. Any satellite within tens of kilometres would probably be destroyed and any unprotected satellites within hundreds of kilometres would risk being damaged or disabled. Over time, the blast would feed additional charged particles into the Van Allen radiation belts that surround Earth, ruining the operation of most satellites in low Earth orbit within a month, O'Hanlon argues in written testimony. 'I think most countries could pull off an anti-satellite strike on the first try,' O'Hanlon says. 'You don't**

---

[843] O'Hanlon, Michael. "Commentary: Who Will Hold Together the Future Syria?". *Defense News*. 8 September 2015.

[844] https://www.brookings.edu/opinions/bosnia-lends-clue-to-syria-strategy/

[845] https://www.twincities.com/2007/01/16/its-prospects-are-mediocre-but-bushs-plan-has-logic-behind-it/

have to get that close to destroy something.' But it would be considerably more difficult to explode a nuclear weapon in the higher geosynchronous orbit, where many communications and military satellites orbit. Another potential threat is small satellites that could ram into larger satellites or carry conventional explosives. 'Some countries have had anti-satellite weapons in the past,' said air force lieutenant-general Robert Kehler. 'We're watching that today.' Hardened satellites: A potential response to the threat of attack is to 'harden' satellites to make their electronics less vulnerable. **The US military already hardens some of its satellites. But if US companies were asked to harden their satellites, they would have a tougher time competing with international companies that did not have such a requirement, noted Edward Morris, director of the office of space commercialisation** for the National Oceanic and Atmospheric Administration. **O'Hanlon recommended improved monitoring of satellites so the US would know whether its satellites were being attacked.**"[846]

"While the West wants to help transitions succeed, its financial crises mean there can't be a big wave of new assistance, such as that which helped the Central Europeans or Balkan countries make it through their transitions. This may not be a bad thing, as it will require assistance to be focused on areas where it can do the most good. We will need to learn how to structure security assistance and rule of law training in ways that help, rather than hinder, democratic transitions."[847]

That US policy makers consider the outcome in Bosnia as a model for anything other than what-not-to-do is blood-chilling and reveals US policymakers' monopoly of violence in their ability to consciously recreate specific models of genocide anywhere at will. Many facts on the ground in several Arab Spring countries created by international consensus, and lack thereof, have created a devastation very similar to the Yugoslav war, so much so that one can see the inspiration from the earlier NATO success (by their measure) in the Bosnian genocide that Biden and Brookings analysts have admittedly been working to replicate.

"Some view the breakdown of order in Somalia as the first modern instance of state failure; others, the collapse of political order in the Balkans. Whichever benchmark is chosen, attempts to investigate the phenomenon systematically are but two decades old."[848]

+ All-sides-are-to-blame-now international discourse (Biden article w This Time We Knew); Area ethnically cleansed and segregated and borders re-drawn (Biden plan w This Time We Knew)

One does not have to go far to find intimate links between US involvement in the Yugoslav War and US involvement post-2000 across the Middle East. An article from the *International Herald Tribune*, an extinct newspaper published in conjunction with *The New York Times* and *The Washington Post*, dated March 12, 1998 reiterates to the UN the Clinton Administration's "right to launch attack at Iraq", in which "Clinton tells Annan U.S. will consult with Security Council before attacking Iraq". A Republican majority leader and then-Senator Joe Biden bipartisanly refused to meet with Annan due to the issue, but it is noted that the $1.7

---

[846] https://www.newscientist.com/article/dn9393-space-attack-on-satellites-could-be-devastating/
[847] https://www.rand.org/blog/2011/12/the-year-of-the-arab-spring.html
[848] Bates, Robert H. "State Failure". *Annual Reviews Political Science,* Vol. 11. 2008, p. 9.

billion owed by the US to the UN for peace-keeping dues was also pertinent, as "the dues question also appears tightly bound to a resolution of the Iraqi crisis. If Baghdad violates the agreement [for arms inspections], support in Congress for paying the U.S. debt [to the UN] would likely suffer."[849]

A separate article in the same March 12, 1998 issue details $40 million given to Iraqi "Kurdish groups" by US NGOs and the Pentagon, $10 million "in political support to democratic opposition to Saddam", $5 million for an Arabic station Radio Free Iraq broadcast from US owned equipment in Kuwait, and $3 million "to fund an effort to get the United Nations to approve an international criminal tribune for 'indicting, prosecuting and punishing Saddam Hussein and other Iraqi officials responsible for crimes against humanity.'" An unnamed Republican source remarks in the article that, "This is only a first step toward the longer-term plan for ousting Saddam Hussein."[850]

In the same March 12, 1998 issue, Chris Hedges publishes an article about the Red Cross leaving Kosovo due to threats to foreign staff, leaving the Albanian areas "cordoned off by police and paramilitary". Milosevic was given 10 days to comply with removing these forces as two million Albanians became refugees. This led "The Contact Group of overseers" from Britain, France, Italy, US, Canada and Russia to reimpose sanctions on Yugoslavia.[851]

The planned deportation of Iraqis from the US who worked for the CIA is also covered in detail in this March 12, 1998 issue. Having worked out of "a CIA base in northern Iraq", "the six jailed men were among a group of 600 Iraqis who fled to Turkey in August and September 1996. The group, along with 5,500 other Iraqis and Kurds, was evacuated to the island of Guam. When they went to California, the Iraqis were imprisoned…". These "six Iraqis who apparently worked in concert for the CIA in failed plots against Saddam Hussein have been declared threats to US national security in a court ruling so secret that their lawyers cannot read it." They "were offered refuge by the United States when two CIA plots against the Iraqi leader collapsed in 1996. Then after arriving in California they were placed in detention centers run by the Immigration and Naturalization Service."[852]

Guam, Puerto Rico, and Guantanamo Bay of Cuba were, of course, all bequeathed to the US through the Spanish-American War. In 1999, shortly before the events of September 11, 2001 that would lead to the Bay becoming a prison camp for prisoners in the War on Terror, Guantanamo Bay, according to TIME Magazine, was earmarked to become a refugee camp for some 20,000 people fleeing the Yugoslav War.[853] The plans for a post-Kosovo refugee camp were not realized, and Guantanamo Bay was repurposed as a perpetual US detention facility

---

[849] Knowlton, Brian. "Clinton Tries to Reassure UN Leader". *International Herald Tribune*. 12 March 1998.
[850] Pincus, Walter. "U.S. Senators Push for Aid to Opponents of Saddam". *International Herald Tribune*. 12 March 1998.
[851] Hedges, Chris. "Heeding Death Threats, Red Cross Leaves Kosovo". *International Herald Tribune*. 12 March 1998.
[852] Weiner, Tim. "U.S. May Deport Iraqis Who Worked for CIA". *International Herald Tribune*. 12 March 1998.
[853] Rothman, Lily. "Why the United States Controls Guantanamo Bay". *TIME Magazine*. 22 January 2015.

notorious for torture, secrecy and other human rights abuses against accused but unconvicted Muslim "terrorists".
https://www.newenglishreview.org/Ares_Demertzis/Bill_Clinton%27s_Bastard_Army/
"Former U.S. National Security Advisor Zbigniew Brzezinski stated that a "political awakening" is taking place in this region which may be an indicator of the multi-polar world that is now developing. **He alluded to the Greater Middle East as the "Global Balkans",** and as a control lever on an area he refers to as Eurasia.[7]"[854]

Research and Arrested Development
A political problem thought of in military terms eventually becomes a military problem.
Gen. George C. Marshall

[TOPIC – on strategic arms races meant to deplete opponent's resources (military deception), to control policy through terror, to increase surveillance (including human trafficking, espionage), to arm with *tactical* nuclear weapons for *covert Special operations* (including assassinations, human trafficking & experimentation), to receive funding for R&D]
"Our amendment calls for a mutual and verifiable freeze on the testing, production, and deployment of nuclear weapons. It is premised on the essential nuclear parity that exists today… Since the Senate first voted on the Kennedy-Hatfield nuclear freeze and reductions resolution last October [1984], both the INF and the START negotiations have broken off… Both sides should renounce forever the pursuit of the phantom of nuclear superiority. We must free our diplomacy from the myth that more megatons mean bigger bargaining chips… We must ask a simple question of them. Instead of piling overkill upon overkill, why not start now with a freeze?... The freeze can halt new technologies that are dangerous and destabilizing, technologies that may be impossible to stop once they are started… Opponents also claim that a freeze is not a practical idea, because it will be too difficult to verify. Just the opposite is true. In fact, a freeze may well be easier to verify than a complex arms reduction treaty. **One critical aspect of the freeze, the deployment of new nuclear weapons systems, can be verified with high confidence through national technical means – that is, satellites and listening posts equipped with sensors – and through data exchange and restrictions on concealment.** A **second element of the freeze, testing, can also be verified by national technical means, together with unmanned seismic stations and opportunities for onsite inspection**… **The third aspect of the freeze, production, may be more difficult to verify, but our intelligence is so highly developed that, according to former Under Secretary of Defense William Perry, we have been able to 'monitor** Soviet activity at the design bureaus and production plans well enough so that we have been able to predict ever ICBM before it began its tests.'… But **on the question of verification, we should remember one important aspect of the nuclear freeze that was described be the former Deputy Director of CIA, Herbert Scoville: A Freeze is Actually Easier to Verify than A Treaty** Like SALT I or Salt II. Such treaties contain complicated limits on numbers and on modifications of missiles and planes; to detect a violation requires continuing and exact measurements of a vast array of possible prohibited activity. **With a freeze, however, a violation would occur and be discovered the instant the other side does**

[854] https://en.wikipedia.org/wiki/Greater_Middle_East

anything new at all… Our overriding goal should be to secure **a nuclear weapons freeze** that prevents any further escalation of the nuclear arms race – across the board – not only in Europe but **in <u>every</u> region of the world.** Moreover, the opponents who make this **argument against the freeze seem to imply that the United States could not, or world not, call on its entire nuclear arsenal in response to a Soviet nuclear attack on NATO… Any suggestion that the United States no longer relies on this avenue of retaliation signals a major and destabilizing change to NATO policy, in which Europe can no longer depend upon America's nuclear umbrella**… In fact, a bilateral freeze is the best way to protect against the effects of that buildup**. It would halt an entire new generation of nuclear weapons** which the Soviets are now **developing** – including the Blackjack bomber, a new submarine-launched ballistic missile and land-based mobile missiles. The cries of alarm about Soviet plans for the future actually constitute a compelling reason to freeze the present balance of forces – and to prevent future destabilizing <u>im</u>balances. The Administration instead prefers to respond with billions of dollars in more military spending and a massive American military buildup. But **we should know by now that the Soviets will not accept a status of military inferiority**, that they will match us bomber for bomber, missile for missile, warhead for warhead. Finally, we are told that a freeze at this time would keep us from perfecting our own deterrent – for example, by creating a new type of bomber which, for at least a while, will be less vulnerable to Soviet defenses. But at any time, there will always be some imperfections in the military forces on either side**. That reality can be used every time to justify just one more round in the arms race. 'This is all we want,' they say, 'and <u>then</u> we will have enough.' But the Soviets have learned to make that same argument.** And so we drift, as Einstein said, 'toward unparalleled catastrophe.' We must reject policies which claim for the moment to make the world a little more secure, but in the end make the world a more unsafe and unstable place. In closing, let me respond briefly to those who have questioned the idea of offering the freeze as an amendment to the Debt Ceiling Act**. The freeze is hardly irrelevant to the Debt Ceiling Act**. If a nuclear weapons freeze is successfully negotiated, it can make a bigger difference than any other single proposal I have heard for reducing the dangerous federal deficit. A freeze will save America $100 billion over the next five years – an average of $20 billion a year. Under the circumstances, the freeze is not only appropriate, it is also timely and relevant as an amendment to the Debt Ceiling Act. There is no morality in the mushroom cloud. The black rain of nuclear ashes will fall alike on the just and unjust. And **then it will be too late to wish that we had done the real work of this atomic age** – which is to seek a world that is neither red nor dead, to prevent a planet divided from becoming a planet destroy. I urge the Senate to vote for the nuclear weapons freeze and reduction resolution, as a clear sign of our commitment to stop the nuclear arms race before it stops the human race."[855]

A freeze, reduction, and stockpiling led to an increase in spending and deployment of newer, smaller scale "national technical means" for nuclear/atomic weapons systems. Through radar satellite technology, acoustic surveillance "listening posts", vibrational seismic sensors, and an unverifiable intelligence force - described as existing somewhere between the DOD, the CIA, and violations enforcement agencies, – the threat of strategic weapons set the stage to approve international and domestic policy for the use of covert tactical nuclear weapons intelligence.

---

[855] Kennedy, Sen. Edward M. "Statement of Senator Edward M. Kennedy on the Nuclear Weapons Freeze Amendment to the Debt Ceiling". *Office of Senator Edward M. Kennedy of Massachusetts*. 5 October 1984.

[TOPIC - Surveillance Density, Voter Turnout and Economic Performance in East Germany: The existence of a surveillance state is proven to have a strong negative impact on the state's economic performance, creating a negatively reinforcing cycle.]

Marcus Jacob and Marcel Tyrell find in "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany" that:

> the differences in the intensity of Stasi surveillance and repression across the regions in the former GDR [German Democratic Republic] have significant bearing on the social capital patterns observed in these regions today, which in turn inform economic outcomes. Our approach is motivated by the considerable body of scholarly work that attributes the persistence of differences in economic development to social capital, referred to as the connections among individuals, and the norms of reciprocity and trustworthiness that arise from them… We posit that people's experience of living in a regime with the world's most pervasive and intrusive surveillance apparatus has resulted in a strong and lingering sense of mistrust of members of society outside the immediate family circle in post-communist East Germany. **To ensure that the people would become and remain submissive, the ruling party in the GDR saturated its realm with more spies than had any other totalitarian regime in history… To be specific, we find that a one standard deviation increase in the Stasi informer density (about 2.73 informers per thousand people) is associated with a 0.6 percentage point decrease in current electoral turnout, a 10% decrease in organizational involvement, and a 50% reduction of the number of organs donated post mortem** in the districts in our sample… **our results suggest that scale and depth of penetration of people's private lives, and the ensuing social capital erosion in East Germany, may be an important explanatory factor for the persistent differences in economic prosperity between East and West Germany.** Our regression evidence suggests that surveillance via social capital may **explain approximately 7% of the East-West differential in income per capita and 26% of the unemployment gap**… Ostrom (2005) argues that **despotic or authoritarian policies deteriorate social capital by a) inducing individuals to be narrowly self-interested and to wait for externally imposed inducement of sanctions before voluntarily contributing to collective action, and by b) undermining citizens' ability to experiment solutions to their problems and learn from experimentation over time**.[856]

"There is hereby established within the **Department of Justice an Office of Science and Technology** (hereinafter in this title referred to as the ''Office''). (a) MISSION.—The mission of the Office shall be— … (6**) To carry out research, development,** testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to— (A) weapons capable of preventing use by unauthorized persons, including personalized guns; (B) protective apparel; (C) bullet-resistant and explosion-resistant glass; (D) monitoring systems and alarm systems capable of providing precise location information; (E) wire and wireless interoperable communication technologies; (F) tools and techniques that

---

[856] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010, p. 3-4; 7.

facilitate investigative and forensic work, including computer forensics; (G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices; (H) guides to assist State and local law enforcement agencies; (I) DNA identification technologies; and (J) tools and techniques that facilitate investigations of computer crime.

(7**) To administer a program of research, development,** testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) **To serve on the** Technical Support Working Group of **the Department of Defense**, and on other relevant interagency panels, as requested.

(9) **To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.**

(10) **To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.**

(11) **To administer a program of acquisition, research, development,** and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating **cybercrime**.

(12) **To support research fellowships** in support of its mission.

(13) **To serve as a clearinghouse for information on law enforcement technologies**.

(14) **To represent the United States and State and local law enforcement agencies**, as requested**, in international activities concerning law enforcement technology**.

(15) **To enter into contracts and cooperative agreements and provide grants**, which may require **in-kind or cash matches from the recipient,** as necessary to carry out its mission.

(16) To carry out other duties **assigned by the Attorney General to accomplish the mission of the Office.**

(c) COMPETITION REQUIRED.—**Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis**."[857]

"The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1) **advising the Secretary regarding research and development efforts and priorities in support of the Department's missions**;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to **chemical, biological, radiological, nuclear, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals** for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Information Analysis and Infrastructure Protection, by **assessing and testing homeland security vulnerabilities and possible threats**;

(4) **conducting basic and applied research, development, demonstration, testing**, and evaluation activities that are relevant to any or all elements of the Department, through both

---

[857] 107th Congress. Homeland Security Act 2002, Public Law 107-296. 25 November 2002. https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf p. 26-27

intramural and extramural programs, **except that such responsibility does not extend to human health-related research and development activities**;

(5) **establishing priorities for, directing, funding, and conducting national research, development,** test and evaluation, and procurement of technology and systems for— (A) preventing the importation of **chemical, biological, radiological, nuclear, and related weapons** and material; and (B) **detecting, preventing, protecting against, and responding to terrorist attacks;**

(6) **establishing a system for transferring homeland security developments** or technologies to Federal, State, local government, and private sector entities;

(7) **entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites** and support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. 8401), as amended by section 1709(b);

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as ''select agents'' in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act (42 U.S.C. 262a);

(10) **supporting United States leadership in science and technology**;

(11**) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;**

(12) **coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;**

(13) coordinating with other appropriate executive agencies in **developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs**; and

(14) developing and overseeing the administration of guidelines **for merit review of research and development projects** throughout the Department, **and for the dissemination of research conducted or sponsored by the Department.**

In accordance with title XV, **there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of the following entities**:

(1) The following **programs and activities of the Department of Energy**, including the functions of the Secretary of Energy relating thereto (**but not including programs and activities relating to the strategic nuclear defense posture of the United States**):

(A) The **chemical and biological national security** and supporting programs **and activities of the nonproliferation and verification research and development program**.

(B) The **nuclear smuggling programs and activities within the proliferation detection program** of the nonproliferation and verification research and development program. The programs and activities described in this subparagraph may be designated by the President either for transfer to the Department or for joint operation by the Secretary and the Secretary of Energy.

(C) The nuclear assessment program and activities of the assessment, detection, and cooperation program of **the international materials protection and cooperation program**.

(D) Such life sciences activities of the biological and environmental **research program related to microbial pathogens as** may be designated by the President for transfer to the Department.
(E) The Environmental Measurements Laboratory.
(F) The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.

(2) The National Bio-Weapons Defense Analysis Center of the Department of Defense, including the functions of the Secretary of Defense related thereto. (a) IN GENERAL.—With respect to **civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities, goals, objectives, and policies** and develop a coordinated strategy for such activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed pursuant to section 302(2). (b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in such subsection."[858]

"The Secretary, acting through the Under Secretary for Science and Technology, **shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues**, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308. SEC. 306. MISCELLANEOUS PROVISIONS. (a) CLASSIFICATION.—To the greatest extent practicable, **research conducted or supported by the Department shall be unclassified.** (b) CONSTRUCTION.—**Nothing in this title shall be construed to preclude any Under Secretary of the Department from carrying out research, development, demonstration, or deployment activities**, as long as such activities are coordinated through the Under Secretary for Science and Technology. (c) REGULATIONS.—The Secretary, acting through the Under Secretary for Science and Technology, **may issue necessary regulations with respect to research, development, demonstration, testing, and evaluation activities of the Department, including the conducting, funding, and reviewing of such activities**. (d) NOTIFICATION OF PRESIDENTIAL LIFE SCIENCES DESIGNATIONS.—Not later than 60 days before effecting any transfer of Department of Energy life sciences activities pursuant to section 303(1)(D) of this Act, the President shall notify the appropriate congressional committees of the proposed transfer and shall include the reasons for the transfer and a description of the effect of the transfer on the activities of the Department of Energy.
SEC. 307. HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY. (a) DEFINITIONS.—In this section: (1) FUND.—The term ''Fund'' means the **Acceleration Fund for Research and Development of Homeland Security Technologies** established in subsection (c). (2) HOMELAND SECURITY RESEARCH.—**The term ''homeland security research'' means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.** (3) HSARPA.—The term ''HSARPA'' means the Homeland Security Advanced Research

[858] 107th Congress. Homeland Security Act 2002, Public Law 107-296. 25 November 2002. https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf P. 30-31

Projects Agency established in subsection (b). (4) UNDER SECRETARY.—The term ‘‘Under Secretary’’ means the Under Secretary for Science and Technology. (b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.— (1) ESTABLISHMENT.— There is established the Homeland Security Advanced Research Projects Agency. (2) DIRECTOR.—HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary. (3) RESPONSIBILITIES.—The Director shall administer the Fund **to award competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including businesses, federally funded research and development centers, and universities**. The Director shall administer the Fund to— (A) **support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security**; (B) **advance the development, testing and evaluation, and deployment of critical homeland security technologies**; and (C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities. (4) TARGETED COMPETITIONS.—The Director may solicit proposals to address specific vulnerabilities identified by the Director. (5) COORDINATION.—The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies. (6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section. (7) DEMONSTRATIONS.—The Director, periodically, shall hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel. (c) FUND.— (1) ESTABLISHMENT.—There is established the Acceleration Fund for Research and Development of Homeland Security Technologies, which shall be administered by the Director of HSARPA.”[859]

“IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the responsibilities under section 302(4) through both extramural and intramural programs. (b) EXTRAMURAL PROGRAMS.— (1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, **shall operate extramural research, development, demonstration, testing, and evaluation programs** so as to—

(A) **ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practicable participate**;

(B) **ensure that the research funded is of high quality, as determined through merit review** processes developed under section 302(14); and

(C) **distribute funds through grants, cooperative agreements, and contracts**.

(2) **UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY**.— (A) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish within 1 year of the date of enactment of this Act a university-based center or centers for homeland security. The purpose of this center or centers shall be to establish a coordinated, university-based system to enhance the Nation’s homeland security. (B) CRITERIA FOR SELECTION.—**In selecting colleges or universities as centers for homeland security**, the Secretary shall consider the following criteria: (i) **Demonstrated expertise in the**

[859] 107th Congress. Homeland Security Act 2002, Public Law 107-296. 25 November 2002 https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf P. 34-35

training of first responders. (ii) **Demonstrated expertise in responding to incidents involving weapons of mass destruction and biological warfare**. (iii) **Demonstrated expertise in emergency medical services.** (iv) **Demonstrated expertise in chemical, biological, radiological, and nuclear countermeasures**. (v) **Strong affiliations with animal and plant diagnostic laboratories**. (vi) **Demonstrated expertise in food safety**. (vii) **Affiliation with Department of Agriculture laboratories or training centers**. (viii) **Demonstrated expertise in water and wastewater operations**. (ix) **Demonstrated expertise in port and waterway security**. (x**) Demonstrated expertise in multi-modal transportation**. (xi) **Nationally recognized programs in information security**. (xii) **Nationally recognized programs in engineering**. (xiii) **Demonstrated expertise in educational outreach and technical assistance.** (xiv) **Demonstrated expertise in border transportation and security**. (xv) **Demonstrated expertise in interdisciplinary public policy research and communication** outreach regarding science, technology, and public policy. (C) DISCRETION OF SECRETARY.—The Secretary shall have the discretion to establish such centers and to consider additional criteria as necessary to meet the evolving needs of homeland security and shall report to Congress concerning the implementation of this paragraph as necessary. (D) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this paragraph. (c) INTRAMURAL PROGRAMS.—
(1) CONSULTATION.—In carrying out the duties under section 302, the Secretary, acting through the Under Secretary for Science and Technology, may draw upon the expertise of any laboratory of the Federal Government, whether operated by a contractor or the Government.
(2) LABORATORIES.—The Secretary, acting through the Under Secretary for Science and Technology**, may establish a headquarters laboratory for the Department at any laboratory or site** and may establish additional laboratory units at other laboratories or sites.
(3) CRITERIA FOR HEADQUARTERS LABORATORY.—If the Secretary chooses to establish a headquarters laboratory pursuant to paragraph (2), then the Secretary shall do the following: (A) Establish criteria for the selection of the headquarters laboratory in consultation with the National Academy of Sciences, appropriate Federal agencies, and other experts. (B) Publish the criteria in the Federal Register. (C) Evaluate all appropriate laboratories or sites against the criteria. (D) Select a laboratory or site on the basis of the criteria. (E) Report to the appropriate congressional committees on which laboratory was selected, how the selected laboratory meets the published criteria, and what duties the headquarters laboratory shall perform. (4) LIMITATION ON OPERATION OF LABORATORIES.—No **laboratory shall begin operating as the headquarters laboratory of the Department** until at least 30 days after the transmittal of the report required by paragraph (3)(E).”[860]

+ADD “There’s a lot of excitement around self-driving cars, delivery drones, and other intelligent, autonomous systems, but **before they can be deployed at scale**, they need to be both reliable and safe. That’s why Gurdeep Pall, CVP of Business AI at Microsoft, and Dr. Ashish Kapoor, who leads research in Aerial Informatics and Robotics, are using a simulated environment called AirSim to reduce the time, cost and risk of the testing necessary to get autonomous agents ready for the open world. Today, Gurdeep and Ashish discuss life at the intersection of machine learning, simulation, and autonomous systems, and talk about the

[860] 107th Congress. Homeland Security Act 2002, Public Law 107-296. 25 November 2002 https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf P. 36-38

challenges we face as we transition from a world of automation to a world of autonomy. They also tell us about **Game of Drones, an exciting new drone racing competition where the goal is to imbue flying robots with human-level perception and decision making skills**… on the fly. …
Ashish Kapoor: So AirSim aspires to be a **near realistic simulation for AI and robotics systems. So, in a nutshell it's a video game on steroids that softwares are playing**. And **the game** comprises of a robotic agent that's operating in an environment which is akin to reality. So Gurdeep just mentioned about technology such as reinforcement learning and imitation learning, which are trying to solve this **decision-making problem. So, as an autonomous agent**, you need to make decisions, and decisions are not just about now, but it also needs to factor into account the future consequences as well. And that's what makes them hard. So, for instance, when you're playing games, so **things like Go or Atari games or Pac Man or any other video game, right? As a gamer, you have a sense of what your actions, right now, have a consequence in future.** And, **in order to bake that effect into your machine learning, you need to play millions and millions of times**. So for instance, you know, Atari games. You know, we've been hearing about how machine learning can solve some of these video games at superhuman level, almost getting perfect score. For instance, some of the **recent work at Microsoft Research in Montreal talks about PacMan**. But one thing you need to realize is that you are trying to **play these games several hundred millions of times before something reasonable starts to appear as a policy**. We do not have such luxury in real world. I cannot have a robot bonk into things a million times before I start to learn something new. So consequently, simulation… Host: Well, I want to talk about **Game of Drones**. And this is a competition that's coming up for NeurIPS 2019. Ashish, before I talked to you this week, I was actually unaware that **drone racing was a thing, let alone a hugely popular thing**. And then I went down the YouTube rabbit hole and saw what it was, and it's amazing. And we talked about simulated drone racing. They actually have live drone racing… Ashish Kapoor: **Live drone racing, yeah**…! Host: …in empty arenas. These guys are in cages and **then the drones going like Harry Potter in Quidditch**, kind of thing. I was blown away. So, talk about what you're doing in this arena, no pun intended, of drone racing, and how **Game of Drones** is playing into that and what you **hope to accomplish from like a research and science perspective on it.** …
Kapoor: So **Game of Drones** is a competition that is being held at NeurIPS 2019, and this was jointly proposed by **Microsoft, Stanford University and University of Zurich**. So, yeah, you know, this is in collaboration with academia and it's trying to solve, I would say, one of the hardest problems in **autonomy**… So there are courses that are built in AirSim where competitors can try their algorithms and see how well they fare. **There is an ongoing leader board** where, you know, you can track your progress **against your opponents and then there are prizes as well**… Host: **Everything you come up with brings up new things is like, this is research forever, right? Momma needs a new pair of shoes!**
Gurdeep Pall: **Totally**. Host: Well, there's another competition that I'd like to talk about. Ashish, you and a team of collaborators just employed your AirSim technology to win a pretty amazing competition called the **DARPA** SubT Challenge, SubT standing for subterranean. And you won it rather decisively. … Ashish Kapoor: So the simulation environment helps them by validating their methodologies, as well as collecting training data for their perception models. So the competition itself was to identify several of these objects that were lying in a real cave. And you had to send your robots and you had to identify. So the objects, for instance, were a survivor, a backpack, a cell phone, a drill and, I believe, a flashlight. Host: So this was a real cave?

Ashish Kapoor: This was a real cave. Host: And real robots? Ashish Kapoor: And real robots and there were all these objects. And the team, whoever could go and detect maximum number of these objects, won."[861] https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html

"**According to the [Pentagon] video, tomorrow's vast urban jungles will be replete with 'subterranean labyrinths' governed by their 'own social code and rule of law.**' They'll also enable a proliferation of 'digital domains' that facilitate 'sophisticated illicit economies and decentralized syndicates of crime to give adversaries global reach at an unprecedented level.' If the photo montage in the video is to be believed, hackers will use outdoor electrical outlets to do grave digital damage, such as donning Guy Fawkes masks and filming segments of 'Anonymous News.' **This, we're told, will somehow 'add to the complexities of human targeting** as a proportionally smaller number of adversaries intermingle with the larger and increasing number of citizens.'"[862]

"'One major issue is the lack of publicly available data to measure progress, as well as a system that has led government agencies and other organizations to fudge statistics to make themselves look better… "**First they classified the data, then they stopped reporting it**," he said. "**You as members of Congress have no public metrics to rate the billions of dollars we are spending in Afghanistan'**… 'Despite the U.S. Air Force doing 'a wonderful job' working with their Afghan counterparts, the Afghan military and police have been a 'hopeless nightmare and a disaster'… **'As much as you hate the Taliban, and I do, to the average Afghan it's better than the justice provided by the national unity government.**'," **John Sopko, Special Inspector General for Afghanistan Reconstruction said before the House Foreign Affairs Committee hearing held January 16, 2020**.[863]

Because the US created and armed the Taliban as the *mujahidin*, it is a suggestion that the Cold War US-created militia is preferable to the current US-sponsored Afghan government. This is a fine example of wargaming logic in real situations – the US plays against the multiple versions of itself it has trained. It is an endorsement for the US Air Force deployment of aerial weaponry and its proliferation among forces of a highly unstable nation.

It is also a call for more research and development – part of the $133 billion dollars lamented already spent on the Afghan War. Inevitably, this recent 'embarrassing' development before the House and public will result in more demand for research and development to respond to the embarrassing testimony. This exemplifies one part of the entropic mechanism at work detailed in the final section Research and Arrested Development.

[REWORD above – repeated]

+ADD "The bombs may be available in 1965. Unless research is slowed down, nuclear weapons will not be inexpensive – they will be cheap. There should be models available which can just about be manufactured by any high-quality ordnance manufacturer. (Other models will require every resource of technology.) Presumably, the designs of those bombs which are easily made

---

[861] Autonomous systems, aerial robotics and Game of Drones with Gurdeep Pall and Dr. Ashish Kapoor November 27, 2019 | By Microsoft blog editor. Microsoft webpage. https://www.microsoft.com/en-us/research/blog/autonomous-systems-aerial-robotics-and-game-of-drones-with-gurdeep-pall-and-dr-ashish-kapoor/

[862] https://theintercept.com/2016/10/13/pentagon-video-warns-of-unavoidable-dystopian-future-for-worlds-biggest-cities/

[863] Blitzer, Ronn. "" https://www.foxnews.com/politics/afghanistan-watchdog-testimony

will still be classified, and the materials restricted. It should be another five or ten years before this knowledge gets widely disseminated, and it may be even longer before the materials become generally available."[864]

+ADD "**The first prototype situation is Armageddon** – a final battle between 'good' and 'evil' in which civilization itself will receive an enormous setback no matter who wins the battle or, even more finally, a battle in which human life will be wiped out. As I pointed out in discussing the Doomsday Machine, this will not always be a completely academic notion. **While it does not seem technically feasible today, unless R&D is controlled**, it most likely will be technically feasible in 10 to 20 years. A central problem of arms control – perhaps *the* central problem – is to delay the day when Doomsday Machines or near equivalents become practical, and when and if **Doomsday Machines or near equivalents** are feasible to **see to it that none are built**. In the long run there is presumably no question that Armageddon is the major issue. **To say that this catastrophe must be avoided, no matter what compromises this entails, seems to be a humorous or stupid understatement.** Unfortunately, there seems to be no practical way to eliminate this possibility entirely. **The best available policy** seems to be one that would involve some **world supervision of permissible weapons systems**."[865]

During the Congressional 2005 Fiscal Year Defense Budget Hearing, the official connections between US national debt, the Yugoslav War, September 11th attacks, post-2000 wars in the Middle East, Defense Department ICT, and human trafficking became abundantly clear during a fairly concise exchange over four and a half minutes between Pentagon officials and an examining member of Congress, as follows:

Representative Cynthia McKinney: Mr. Secretary, I watched President Bush deliver a moving speech at the United Nations in September 2003 in which he mentioned the crisis of the sex trade. The president called for the punishment of those involved in this horrible business. But at the very moment of that speech, DynCorp was exposed for having been involved in the buying and selling of young women and children. While all of this was going on, DynCorp kept the Pentagon contract to administer the smallpox and anthrax vaccine and is now working on a plague vaccine through the Joint Vaccine Acquisition Program. Well, how do you explain the fact that DynCorp and its successor companies have received and continue to receive government contracts? …

Mr. Secretary, is it policy of the U.S. government to reward companies that traffic in women and little girls? That's my first question… My second question, Mr. Secretary, [is]: According to the comptroller general of the United States, there are serious financial management problems at the Pentagon, to which Mr. Cooper alluded. Fiscal year 1999, $2.3 trillion missing; fiscal year 2000, $1.1 trillion missing. And DOD is the number-one reason why the government can't balance its checkbook...The Pentagon has claimed year after year that the reason it can't account for the money is because its computers don't communicate with each other. My second question, Mr. Secretary, is, who has the contact today to make those systems communicate with each other? How long have they had those contracts? And how much have the taxpayers paid for them?...

---

[864] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 479.
[865] Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960, p. 523-524.

Finally, Mr. Secretary, after the last hearing, I thought that my office was promised a written response to my question regarding the four war games on September 11th [2001]. I have not yet received that response…

Defense Secretary Rumsfeld: First, the answer to your first question is no, absolutely not. The policy of the United States government is clear, unambiguous and opposed to the activities that you described…

McKinney: Well, how do you explain the fact that DynCorp and its successor companies have received and continue to receive government contracts?...

Rumsfeld: I would have to go and find the facts. But there are laws and rules and regulations with respect to government contracts, and there are times that corporations do things they should not do, in which case they tend to be suspended for some period. There are times, then, that under the laws and the rules and regulations passed by the Congress and implemented by the executive branch, that corporations can get off of -- out of the penalty box, if you will, and be permitted to engage in contracts with the government. They're generally not barred in perpetuity...

McKinney: This contract -- this company was never in the penalty box...

Rumsfeld: The second question... I've forgotten what the second question was.

McKinney: I think Ms. Jonas knows it...

DoD Comptroller Tina Jonas: Thank you, Ms. McKinney. I appreciate the question. I appreciate your interest in the department's financial condition. And we are working very hard on that program. I've just come back recently -- … In general, we spend about $20 billion in the department on information technology systems. The accounting systems are part of that. I can get you the exact number for the record of what we spent on our current what we call legacy systems and those that we're moving toward."

Rumsfeld: On your first question, I'm advised by Dr. Chu that it was not the [DynCorp] corporation that was engaged in the activities you characterized, but I'm told it was an employee of the corporation, and it was some years ago in the Balkans that that took place.

McKinney: It's my understanding that that continues to take place, and --

Rumsfeld: Well, if you can give me information to that effect --

McKinney: I'm sure you are interested in all the information that I have, and I'll be more than happy to provide it to you...

McKinney: The question was - we had four war games going on on September 11th, and the question that I tried to pose before the secretary had to go to lunch was whether or not the activities of the four war games going on on September 11th actually impaired our ability to actually respond to the attacks…

General Richard Myers: The answer to the question is no, it did not impair our response. In fact, General Eberhart who was then the commander of North American Aerospace Defense Command, as he testified in front of the 9/11 Commission, I believe -- I believe he told them that it enhanced our ability to respond given that NORAD didn't have the overall responsibility for responding to attacks that day. That was an FAA [Federal Aviation Administration] responsibility.

Myers: But there were two CPXs [Command Post Exercises]. There was one Department of Justice exercise that didn't have anything to do with the other three. And there was an actual operation ongoing, because there was some Russian bomber activity up near Alaska. So we -- There's not a lot more to say, I don't think, except that there is a series of

-- I'll call them war games, that they are seminar war games where we periodically check our ability to fulfill the commitment that the secretary has made to the president in terms of our capabilities of our Department of Defense. And we can do exactly as the secretary said. We can meet our obligations, as we have, and our strategy. We always have the problems, of course, of things that are in high demand when you have a contingency, whether they're the intelligence/surveillance/reconnaissance assets, or strategic airlift -- those sorts of things. But we have ways to handle all that…

Rumsfeld: If you think about it, five years ago, ten years ago, I would go around Europe and talk to friends from back when I was ambassador to NATO, and they were worried about us. They were worried about the United States of America and wondered about the fact, for example, that in the Balkans, when somebody strayed over a line, everyone pulled back several miles. They were worried about Somalia and the problems there, where the -- the United States made decisions that left question marks in the minds of other countries in the world. We've seen intelligence where Saddam Hussein made comments about the United States won't do this, they can't sustain anything, they'll cut and run. And the world has seen in the last three and a half years the capability of the United States of America to go into Afghanistan, a landlocked country, all the way across the globe, and with 20,000, 15,000 troops, working with the Afghans, do what 200,000 Soviets couldn't do in a decade. They've seen the United States and the coalition forces go into Iraq. And the world has seen a vivid demonstration of the power and capability and agility of the armed forces of the United States. That has to have a deterrent effect on people. It's true, we're doing a lot in the world right now. But if you put yourself in the shoes of a country that might decide they'd like to make mischief, they have a very recent, vivid example of the fact that the United States has the ability to deal with mischief.[866]

When such connections appear in official government exchanges, it becomes increasingly difficult for government officials to deny that there are causations and correlations between the overarching issues I discuss here of crimes against humanity involving police, the Pentagon, NATO, information communication technology and national debts, that result in the coups and wars in the Near East. In 2018, “DynCorp, Arma Aviation and Others Awarded $25 Billion for Army Aircraft Maintenance- DoD Daily Contracts” [867]

+ADD “Computerising Vietnam: Under the pressures of a never-ending war in Vietnam, those running the US information infrastructure turned to computerised data management, launching a second American information regime. Powered by the most advanced IBM mainframe computers, the US military compiled monthly tabulations of security in all of South Vietnam's 12,000 villages and filed the three million enemy documents its soldiers captured annually on giant reels of bar-coded film. At the same time, the CIA collated and computerised diverse data on the communist civilian infrastructure as part of its infamous Phoenix Programme. This, in turn, became the basis for its systematic tortures and 41,000 "extra-judicial executions" (which,

[866] *Fiscal Year 2006 Defense Budget*. 10 March 2005. C-SPAN. Media resource.
[867] https://news.clearancejobs.com/2018/04/04/dyncorp-arma-aviation-others-awarded-25-billion-army-aircraft-maintenance-dod-daily-contracts/

based on disinformation from petty local grudges and communist counterintelligence, killed many but failed to capture more than a handfull of top communist cadres). Most ambitiously, the US Air Force spent $800m a year to lace southern Laos with a network of 20,000 acoustic, seismic, thermal and ammonia-sensitive sensors to pinpoint Hanoi's truck convoys coming down the Ho Chi Minh Trail under a heavy jungle canopy. The information these provided was then gathered on computerised systems for the targeting of incessant bombing runs. After 100,000 North Vietnamese troops passed right through this electronic grid undetected with trucks, tanks and heavy artillery to launch the Nguyen Hue Offensive in 1972, the US Pacific Air Force pronounced this bold attempt to build an "electronic battlefield" an unqualified failure. In this pressure cooker of what became history's largest air war, the Air Force also accelerated the transformation of a new information system that would rise to significance three decades later: The Firebee target drone. By war's end, it had morphed into an increasingly agile unmanned aircraft that would make 3,500 top-secret surveillance sorties over China, North Vietnam and Laos. By 1972, the SC/TV drone, with a camera in its nose, was capable of flying 2,400 miles while navigating via a low-resolution television image. On balance, all this computerised data helped foster the illusion that American "pacification" programmes in the countryside were winning over the inhabitants of Vietnam's villages and the delusion that the air war was successfully destroying North Vietnam's supply effort. Despite a dismal succession of short-term failures that helped deliver a soul-searing blow to American power, all this computerised data-gathering proved a seminal experiment, even if its advances would not become evident for another 30 years until the US began creating a third - robotic - information regime."[868]

While the news media is what has been discussed as the prime medium for propelling wartime philosophies, Jean Baudrillard wrote in 1993 on the mediated spectacularization of human suffering for legitimating intellectual-political action, i.e. research and development:

> Susan Sontag [and her staging *Waiting for Godot* in Sarajevo in 1993] is not, however, the issue. She is merely the high-society instance of what has become a generalized situation, where harmless and powerless intellectuals exchange their misery with those who are miserable, each sustaining the other through a sort of perverse contract... the one serving up its corruption and scandals, the other its artificial convulsions and inertia. Not so long ago, Bourdieu and Father Pierre were the offerings in a televisual holocaust… We must therefore replenish the preserve of our references and values. By way of that smallest of common denominators known as world suffering, we must restock our preserves with artificial game… The New Intellectual Order follows, in every way, on the heels of the New World Order. Everywhere we look distress, misery, and suffering have become the raw goods... Those who do not directly exploit it do so by proxy, and there is no dearth of middlemen skimming a financial or symbolic profit along the way. As with global debt, deficits and suffering are negotiable and have resale value on the futures markets - here, the intellectual-political markets - which are the present-day equivalents of the military-industrial complex of the sinister old days. The logic of suffering governs all commiseration. Even if we mean to confront suffering, our very reference to it gives suffering an indefinite base of objective

[868] https://www.aljazeera.com/indepth/opinion/2012/11/201211912435170883.html

> reproduction. Clearly, to combat anything, one's starting point must be the evil underlying suffering.[869]

The evil Baudrillard addresses here is the commodification of suffering. In an example of what could be studied as late phase capitalist vertical integration, he accuses intellectuals, politicians and media, the purveyors of material on global crises, of "serving up corruption and scandals", of being the same who cause global civil unrest and violence through "its artificial convulsions and inertia."

This is the same point made by Bahador in *The CNN Effect in Action.* + and in recent events involving civil strife in Hong Kong, which has been blamed by that government on subversions of American NGOs. American tourists join walking tours of Hong Kong to watch civil uprisings…[870] ADD Great Game reference

In his comparison of the more familiar military-industrial complex, so called because of military action necessitating industrialists' products and services for weaponry, transport and rebuilding, he terms this newer provider-beneficiary group the intellectual-political markets, who knowingly benefit one another (a single entity, in actuality) through "perverse contracts", such as academics, political advisors and media clamouring for political action on the crisis of one another's choosing. [reword]

By skillfully controlling their clamour and coordinating the reveal of hot-button issues between their industries, the same groups of individuals are able to choose which reaction would be of the greatest benefit at which time. This constitutes the market of irregular warfare. Max Weber in *Politics as a Vocation* calls this a "'romanticism of the intellectually interesting,' running into emptiness devoid of all feeling of objective responsibility."[871]

Baudrillard refers to social contracts in the article, with mention of financial profiteering, but the contracts that exist in the intellectual-political markets are very literally financial contracts, and the lack of published and critical information on these contracts is due to reluctance in self-reporting and the obvious benefits of not highlighting industry secrets, especially a secret that points towards international conspiracy of genocide.

For the argument made here in favor of cyber-realism, consider MAXAR Satellite Technology's Vice President of Communications Nancy Coleman's corporate statement that:

> … high-resolution satellite imagery and analytics are a powerful complement to good journalism, providing indisputable truth at a time when credibility is critical... Our imagery and expertise provide unmatched quality, currency, and veracity in the form of credentialed content to news organizations. **The visual context that we provide puts a compelling**

---

[869] Baudrillard, Jean. "No Pity for Sarajevo". *This Time We Knew*, ed. Cushman, p. 81-83; *Libération*, 7 January 1993, translated by James Petterson.

[870] https://www.msn.com/en-us/news/world/not-your-usual-day-out-for-a-tourist-in-hong-kong-curious-visitors-join-walking-tours-to-see-protests/ar-BBXTtFY?ocid=spartanntp

[871] Weber, Max. "Politics as a Vocation". *From Max Weber: Essays in Sociology*. Oxford University Press. 1958,p. 115.

spotlight on injustice and human suffering allowing decisions to be made with confidence and is an extension of Maxar's purpose.[872]

In the statement Coleman clearly outlines Maxar's production line - from injustice and human suffering to satellite imaging, to news media, to policy decision-making. She clarifies that *injustice and human suffering is the product* sold by satellite imaging companies like MAXAR. The conscious intention and work required to keep this industry functioning must be acknowledged, which is the understanding that the "raw goods" of suffering are created by the people selling images of sufferers – by radiation poisoning and weaponized surveillance – and by the same decision-making bodies that will be called on to correct the policy causing the suffering. This is the situation which I am calling for cyber realism to be applied to.

Cyber realism could be argued to the opposite effect if end-to-end information access, operational control and policy responsibility could be attributed to other industries and individuals. There are certainly other industries and factors involved in the production line of suffering that I have not named here and those that will become involved in the future.

+ADD "Satellite Surveillance Can Trace Atrocities but Not Stop Them: George Clooney's pioneering data project documented horrors in Sudan, but that wasn't enough" "SSP was largely successful in its predictive goals. The Harvard Humanitarian Initiative's report on the pilot phase of the project makes for grim but impressive reading about large-scale violence that was predicted before it happened, recorded in almost real time as it occurred, and further documented as the perpetrators, to varying degrees, attempted to conceal it. The analysis was accurate and prescient enough that the report quotes Rebecca Hamilton, a former special correspondent for the *Washington Post* in Sudan and a fellow at the Pulitzer Center on Crisis Reporting, as calling the attack on Abyei "perhaps the most clearly forecast crisis in history. But if the complex alignment of targeted tasking of satellites and expertise-based human analysis of data was successful, the impact of the project was not what its founders had hoped for. Raymond said one of the learnings from SSP was that "documentation is no substitute for political will." In one case—the attack on Kadugli in 2011—the documentation did force the U.S. government to admit there were grounds for investigation, but the groundbreaking work of SSP led to very little change in the humanitarian community's response to the documented, and even predicted, horrors. In retrospect, it seems almost naive to imagine it would. But in 2010 Bashir had just been indicted by the ICC, and Responsibility to Protect (R2P), a doctrine urging accountability for the violence of states against their own citizens, had just garnered a U.N. secretary-general report. Governments and the international community claimed that they needed evidence to act; it made sense to provide that evidence… There was another factor in that optimism as well, one that sounds very familiar today amid tech buzzwords thrown around in the promise of transformative initiatives. In a 2017 paper in Genocide Studies and Prevention, Raymond and co-author Kristin Bergtora Sandvik call this "technology optimism," an often implicit belief that the use of information and communication technologies has "an inherently Ambient Protective Effect (APE); i.e. casually transforming the threat matrix of a particular atrocity producing environment in a way that improves the human security status of targeted populations." As with surveillance cameras in public areas, there is an assumption among some sectors of the

872 SAR. "MAXAR's Initiative Focused on High-Resolution Imagery".

population that they will make the situation better by their mere existence, that the act of surveilling itself will prevent bad things from happening**. In fact, the reverse can happen. In a 2016 dissertation paper studying Amnesty International's Eyes on Darfur project, Grant Gordon found that "Amnesty's advocacy effort was associated with between a 15 and 20 percentage point increase in violence in monitored areas.**'…The success of the program also led to another insight, one that Raymond believes is even more crucial. As the team realized that they could accomplish what they set out to accomplish—a new form of data that was predictive—they also started to understand that they were working without an ethical net. The **idea of *primum non nocere*, or first, do no harm, is commonly associated with medicine, but it is also the basis for an important humanitarian principle, do no harm. However, as Raymond said, "First you must know the harm before you cannot do the harm." The kind of work SSP was doing was so far outside of the existing strands of information ethics**—primarily focused on individual privacy on the one hand and the limits established by the **Nuremberg tribunals** on violation of agency on the other—that it had no framework yet for figuring out where the limits were."[873]

Why governments choose to traffic humans and their suffering for profit, including their own citizens and subjects of occupation, in full view of the public eye is not only due to a ubiquitous penchant for sadism and vacuous morality. In historical precedent, another modern nation which has already risen and fallen faced major public national debts and began to engage in public kidnapping, torture, exploitation and ransoming of its citizens and visitors from other nations, the German Democratic Republic of East Germany.

Although it is mostly viewed now as a humanitarian and political subject, the kidnapping and financial exploitation of captives or prisoners by East Germany, known as *haeftlingsfreikauf* "purchasing to free prisoners", was done explicitly as an economic project. As a major supplement to the East German GDP of 3.5 billion Deutschmarks (or $500 million every year), and in exchange for commodities such as coffee, copper and oil, the "purchasing to free prisoners" program was an East German presence in the international economy.[874] In 1979, *The New York Times* reported that East Germany had declared the practice ended, but in fact it continued until the collapse of the country. "The ransom payments were begun under Chancellor Konrad Adenauer in 1962, the year after the construction of the Berlin Wall sealed the East German border between East and West Berlin."[875]

The 'purchasing to free prisoners' system also served a tool of political leverage.

+ADD https://www.nytimes.com/1986/02/12/world/shcharansky-wins-freedom-in-berlin-in-prisoner-trade.html ; *boston globe* "shcharansky freed" February 12 1986 [printed]; *NYT*

[873] https://foreignpolicy.com/2020/01/21/sudan-clooney-satellite-surveillance-can-trace-atrocities-but-not-stop-them/

[874] https://www.bbc.com/news/magazine-29889706 ; https://www.nytimes.com/1993/06/22/books/books-of-the-times-the-trade-in-spies-not-all-black-or-white.html ; https://www.reuters.com/article/oukoe-uk-germany-prisoners/west-germanys-cold-war-ransoming-of-prisoners-encouraged-fraud-research-idUKBREA3A09620140411; https://www.pri.org/stories/2014-11-06/during-cold-war-buying-people-east-germany-was-common-practice

[875]https://www.nytimes.com/1979/10/28/archives/east-germanys-prisonerransom-deals-appear-ended.html

"Shcharansky May Go Free in Deal Today" 2/11/1986; *NYT* "Plan for Shcharansky's Release: the Soviet Union's Motives" 2/11/1986; *Baltimore Sun* "East bloc agent pleads guilty in return for inclusion in swap" 2/11/86, similar political plot turned into Hollywood movie *Bridge of Spies* in 2015 grossing $165.5 million

+ADD from The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany

Conclusions

+ADD On human security threats transforming into insurgencies: "Unchecked corruption and any further expansion of the cartels' ability to coerce political processes and citizen participation can fuse their lucrative illicit economy into the normal functioning of the state, requiring the government to co-opt these groups as the only means to reduce violence."[876]

+ADD "Potential state collapse in Mexico or the long-term social and economic consequences of illicit narcotics use in the US will undermine the US's ability to sustain a favorable balance of power across the globe. Drug use and addiction reduce human productivity and reduce the available labor pool and intellectual capacity that underpins a society's sustained economic growth and quality of life. The cartels create regional instability that foreign competitors can leverage to gain access to the Western hemisphere. The human security threat draws the attention of nearly every international and nongovernmental entity in the world. The high levels of violence and lack of human security in Mexico are a global responsibility. The US and Mexico cannot kill or arrest their way out of the problem, and this paper presents an explicit warning to legalization advocates lest that policy mutate from a human security threat into a war."[877]

If my personal testimony can be considered as part of the argument for cyber realism, after I began researching and writing on the topic of Anonymous and its involvement with the federal government and US corporations in the Arab Spring, I received a written threat on my door while working in Washington, DC and experienced physical stalking for years to follow. My personal devices began displaying evidence of hacking, such as Internet connection being disrupted for long periods of time, phone calling service being cut for weeks without explanation, messages and calls not delivered or received, and my social media accounts being closed or suspended. My unshared writing and activities have regularly been commented on in Anonymous members, journalists, and tech corporations' social media posts.

In the fall of 2017, an entire coherent poem about war apparently titled "a poem for the masses" appeared in the drop-down Google search bar on my personal laptop.

In 2019, two individuals impersonating Secret Service agents came to my family home and attempted to coerce me into releasing my personal medical records to them and questioned family members about my activities, language skills, and academic writings. They claimed to represent "some of their protectees" and named the RAND Corporation, the Clintons, and the

[876] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 32.

[877] Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020, p. 33.

Obamas. Local police and the FBI once again refused to take report or respond to my communications about this harassment, and the vexatious conditions surrounding my security research continue to be perpetuated through overzealous secrecy and *ad hoc* law enforcement.

In fact, I have reported these incidents for four years to the FBI and to various local and campus law enforcement departments. I have reported to employers, and was even forced to leave a position at a major Ivy League technical university after reporting the hacking to police. I was hung up on mid-sentence by an FBI agent while attempting to report the incidents by phone.

In sum, the topic is violently suppressed. All of this only confirmed my initial suspicions and research findings.

Anonymous is far from their projected image of a small group of (no longer) young men hacking emails and websites. Functionally, it is as if there has been a shadow coup and the entire system in the United States is made up of members of Anonymous, a cyber-mafia state. For this reason, it is important for Americans to pay close attention to the coups in the Middle East for which Anonymous has already claimed responsibility. Confessed Anonymous members have claimed to be "gang-bangers", human traffickers, neo-Nazis, military members, spies, FBI informants, Internet providers, people of "significant positions in media, industry, and the sciences", and provokers of foreign coups and wars. The National Intelligence Council has fulfilled its prophecy to designate Anonymous a terrorist organization by 2025, which has meant allowing that organization to fester until said point in time.

Despite the seriousness of the threats and pressures, which have resulted mainly from law enforcement's incompetence and complicity in terrorism, I have found many of the group's actions and attitudes throughout foolishly Quixotic, politically naïve, and totally transparent. I do not hesitate to call the loose network that has previously designated itself Anonymous a terrorist organization, and I would cast serious doubt on the qualifications of any professional that challenges the designation of its makeup and nature. It is clear, however, that this designation was not born in a vacuum, but was perpetuated and planned by the US Intelligence directorates. Malicious and inscrutable does not describe the 'public-facing' methods of Anonymous of Internet forums. It does, however, describe the history of US Intelligence agencies and their repurposing of an early Web 2.0 hacktivist group.

The current Prime Minister of the UK Boris Johnson described another cyber-terrorist group this way in 2015, **citing an internal British intelligence report:**

> **If you look at all the psychological profiling about bombers, they typically will look at porn. They are literally wankers. Severe onanists... tortured... very badly adjusted in their relations with women**, a symptom of their feeling of being a failure and that the world is against them... They are not making it with girls... They are just young men in desperate need of self-esteem who do not have a particular mission in life, who feel that they are losers and this thing makes them feel strong – like winners... The crucial thing is that these are young men, principally young men who are growing up without much sense of success in their lives…[878]

[878] Perraudin, Frances and Shiv Malik. "Boris Johnson: jihadis are porn-watching 'wankers'". *The Guardian.* 30 January 2015.

Then-Mayor Johnson was speaking about so-called jihadis that practice domestic terrorism in the UK or travel to join the Islamic State. I apply the quote here because **I do not make the distinction**, outside of a theological discussion, **between secularists and religionists living in the West who feel called to make war in the Middle East**. Most jihadists are recruited as non-practicing or secular individuals who become religionists upon joining a religion-based terrorist organization, hence the psychological profile describing the deviant pervert turned terrorist.

It is a strange form of terroristic organization that exists beyond the basic puppymill war college classroom label of "leadered vs. leaderless" terrorist organization. I have argued a state-sponsored terrorist organization, that claims responsibility for violent acts and denies the violence…. [reword, elaborate]

No extradition or demands for extradition for espionage and assisting in attempted coups of US allies (compare to CIA, militaries,
Activities of wiretapping, spying, racially and politically motivated media hoaxes/hacks (compare to legacy of FBI, counterterrorism agencies) + "Sabu believed Anonymous's greatest power was its lack of hierarchy. He pointed to a U.S. government counterintelligence program in the 1960s and 1970s called COINTELPRO, which saw the FBI quietly subvert activist and political organizations. They had used HBGary-like tactics of subterfuge and misinformation to erode the power of organizations from the Black Panthers to the Puerto Rican FLN to the KKK to Mexican gangs, often doing it from the outside. The reason many of these organizations died out, Sabu believed, was that they had a structured hierarchy."[879]
Evading prosecution and apparent immunity for cyber-attacks against US agencies and corporations

A state willing to publicly traffic in human life could not afford to hire and pay the staff required for the scale of surveillance and trafficking it conducts. **The existence of a surveillance state is proven to have a strong negative impact on the state's economic performance, creating a negatively reinforcing cycle.[880]**

The monstrosity that is the reality of hackers' wars and their possible effect on much of the world could be summed up in the following passage:

> By the time East Germany collapsed in 1989, the Stasi payroll had grown to 91,015 full-time employees. On top came a network of civilian informants, regular informers, and part-time snoopers which grew rapidly in the 1960s and 1970s, and remained nearly constant from the second half of the 1970s. This 'main weapon in the fight against the enemy' was nothing short of monstrous: approximately 173,081 unofficial informers probed every aspect of citizens' lives, carried out concrete assignments for their control officers, made their flats

[879] Olsen. *We Are Anonymous*, p. 235.
[880] Jacob, Marcus and Marcell Tyrell. "The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany". *Mediengruppe Thüringen Verlag*. 10 June 2010.

> available for meetings or observations, searched flats and workplaces, and shadowed suspects with bugs and cameras and through telephone, radio and postal surveillance.[881]

Fortunately, there is always some sphere on the globe that does not take part in the destruction caused by surveillance states and their consequent industries, even if it is affected. This is a state and society that does not make that social and economic destructivity a part of itself. [ADD MORE]

If global connectedness is any indicator, the scourge of telecommunication shadow governments rivals early modern colonialism in scale, and could forewarn of global power shifts. These global power shifts may expand surveillance-colonial governance models, or, power shifts via hackers' wars may forewarn of the collapse of the US 'satellite empire' and surveillance States.

+ADD more on 'Satellite Empire'

The Greater Middle East Plan

And ye shall hear of wars and rumours of wars: see that ye be not troubled: for all these things must come to pass, but the end is not yet.
The Bible, Book of Matthew 24:6

+ADD "Putting this more concretely, a good deal of the **deterrence-oriented analysis of strategic problems and a fair amount of the containment-oriented work in area studies** and in comparative political systems have **served more apocalyptic military** as well as various other **elite, hard-line enthusiasts**. By summoning expert opinion, and by displaying data gathered or estimates projected by experts, those who helped to foster and maintain the Cold War (whether located on the Western or Communist side) were able to defend and extend their case. And thus they were able to exert significant and continuing control over policy. It is a matter of instructive paradox that, at the same time, those at the elite level who so disported themselves were further impassioned and motivated by their experts' readings of international and strategic reality. **A situation of mutual reinforcement between the experts and their most powerful clients**, between the proposers and the disposers, **helped to keep the Cold War dynamic going** – perhaps even after it had reached its own intrinsic culmination. All of this is elaboration upon the simple theme that **establishment policy intellectuals** operate within an institutional matrix that maximizes the likelihood that **their interpretations and projections will become self-fulfilling prophecies**."[882]

+ADD Zbigniew Brzezinski, "The Grand Chessboard: American Primacy and Its Geo-strategic Imperatives"

Any series of human tragedy elicits the desire in us as humans to know why. To find the rationale behind seemingly irrational events is the role of analysts, as opposed to reporters or commentators. While there are clear financial incentives behind the activities of the FBI,

---

[881] Jacob. "The Legacy of Surveillance", p. 5.
[882] Rosenberg, Milton J. (ed.). *Beyond Conflict and Containment: Critical Studies of Military and Foreign Policy.* Transaction Books. 1972, p. 16-17.

Pentagon, NATO and technologists in the Arab Spring and what has followed, the risk of so much evidence floating around in libraries and the Internet is high, and perhaps by some calculations the yield does not exceed what could be made without criminal tactics. One also has to assume that these actors have some human feeling that is disturbed by their own actions.

Nevertheless, a political explanation is elicited from political arguments, and, as I will argue in a separate research paper still in the planning phase tentatively titled The Historicism of the Greater Middle East Plan, I suggest that the political philosophy driving these actions of total and fairly quick-paced destabilization and destruction in the Middle East arises from a school of political thought known as political messianism, or millenarianism. Highly informed by religious eschatology, it has a well-documented history in American political thought, and was the driving force behind Manifest Destiny, Nazism, Zionism, and much of Puritanical British colonialism. Political messianism is often connected with an intense interest in the occult, as it was for the most infamous millenarian political party, the Third Reich, so named for its belief in a thousand-year reign until the end-times.

Contrary to what the name may indicate, political messianism is not what could be called moralistic, as most religious political philosophies are argued. It is events-driven and is practiced by people belonging to many religions. It is practiced in its desire to commit actions that bring about portended apocalyptic 'signs' of the end-of-times. As 'apocalypse' would indicate, the events brought about are what most people would popularly describe as apocalyptic, meaning catastrophic and dystopian. In this school of thought, the means justify the ends, which is the second or final coming of the Messiah and the arrival of the kingdom of God on Earth.

So, there is a moralistic element to political messiansism, but the 'moral good' necessitates an eon of causing events like the destruction of the Holy Lands, widespread war and 'rumors of war', the starvation and imprisonment of the Jewish people followed by 'the nations showing favor to Israel' followed by genocide of all but 144,000 Jews who convert to Christianity, and the torturous death of most of mankind.

If one studies eschatological texts, recent global catastrophic events do bear a striking resemblance to events described as portending signs of 'the end', for example in *The Book of Tribulations: The Syrian Muslim Apocalyptic Tradition* (trans. 2017), and the books of the Bible *Revelations*, and *Daniel*. But of course, there are people planning, executing and funding these tragic events and calling them signs of the apocalypse. Unfortunately, mythologizing mass murder has been fairly effective to date.

Oddly enough, the 2017 English translation of *The Book of Tribulations: The Syrian Muslim Apocalyptic Tradition* was translated by robotics professor David Cook of Rice University. My highly unusual experiences while employed at that NASA research university inform me that there likely is much greater mutual informing between this contribution to 'the end of the world' studies and the space science industry than many would initially presume.

Of course, the 'prophecies' are never interpreted to require personal suffering or sacrifice from these leaders. They are always behind the scenes directing their genocidal 'passion plays'

while political strategists struggle to remember their childhood Sunday school lessons, as they listen to obvious apocalyptic allusions.

Many of those attributing continuous 20th-21st century genocide, and earlier, to political messianism are met with mumbles of "conspiracy theory" when fielding the theory to non-experts. There is a further element of irony in such dismissals because 'genocide' implicitly denotes 'conspiracy'. A theory on deliberate motives not publicly known would be, in any case, integral to explaining a single cause behind one or more genocides. As Dadrian writes in *Warrant to Genocide,* inscrutable systems in secret states are a key element to the implementation of genocide.

***Theories that apply to motives of military action, meaning war or military occupation, do not cross-apply to genocide just because some elements are shared between them*. For example, in a stateless country experiencing genocide (a 'failed' state) there exist policies toward genocide that cannot be enacted or devised in the absence of a state. Genocides are by definition systematic, and could not be conducted by a 'failed' state. This is further evidence for the existence of the 'Satellite Empire' and its primacy in coups, wars, and resulting genocides.**

Genocide is, however, possible in war between states or in occupations of states by states. Therefore, there must be open facts and theories to explain *which* existing state is devising and enacting the pogrom policies. In specific historic example, the Nazi pogroms halted upon collapse of the Nazi State, completely ceasing and liberating those people, or, became persecutions led by the Allied and Soviet States.

Usually those dismissive people do not have truly alternate theories that explain holistically and specifically to the modern age. Some may apply an evolutionary theory which states that it is an accident of nature that humans continuously plan the systematic torture and extermination of portions of their own species decades in advance of each enaction. Usually such people stand to benefit in some way from the systems of genocide, too.

A deconstructionist dismissal in such matters will be met with another deconstructionist dismissal - that is, on how frameworks work properly: this section is an attempt at structuring a theory in a field overly populated by genocidal perpetrators attempting to distract the focus away from fostering conditions for genuine expert analyses. Furthermore, the issue discussed is not Derrida *or* Orwell's speak-write dilemma; **a proper understanding of how war and genocide occur is a matter greater than life and death. It is a matter of extinction.**

Genocides are by legal definition systematic. In the absence of a nation-state, where there is genocide occurring not attributed a state system, some system must be responsible for systematizing the events. In this essay, I have presented many facts that suggest that technology systems have regularly supplemented genocides by states in the past, and may be up to the 'auto-pilot' level of conducting genocides with relatively little apparent state involvement. I agree with author Dadrian that any such change is intentionally done to obfuscate reality of conspiracy to genocide between human planners and systematization.

The drastic increase of genocides in the 20th to 21st centuries, along with international organizations coming into being in the 20th and 21st centuries, and earlier colonial use of global mercantilist enterprises, suggests that <u>the metropole-periphery relationship of empire is essential to the perpetration of genocide, especially in failed states.</u> The distributed guilt possible in global collectives is also essential to this system.

The prevailing political philosophy that conflict in the Middle East is inevitable represents a secular form of political messianism, exemplified in the theory put forth in the paradigmatic work *The Clash of Civilizations and the Remaking of World Order* by Samuel Huntington. Political messianism is unfortunately not an antiquated philosophy. It is espoused today by many prominent American strategists, politicians, academics and clerics of many faith traditions, and is in fact so nearly inextricable from American policy as to be synonymous with it, especially regarding so-called Holy Lands. Many analysts may work under precepts of the philosophy by another name not realizing its origin and ultimate aim.

The National Intelligence Council, as it infringed and imagined itself in a **scenarioist *Financial Times* article**, describes projected future events, saying,

> A crisis atmosphere prevailed. Indeed it was one of those moments in history in which **a new millennium or apocalyptic atmosphere was operating—as if the end of the world was nigh—and immediate action was needed. In a sense, we have reached the Promised Land in which global cooperation is more than a 'conspiracy' among elites** but bubbles up from the grassroots across historic national and cultural divides… International politics is forever changed even though I doubt these networks can be as effective on other issues. **The environment was tailor-made because the widespread commonality of interest in avoiding Armageddon**.[883]

+ADD Carlotta Gall "'It's Like the End of the World'"[884] *The New York Times* 2/18/2020

+ADD RAND publication *Ready for Armageddon* introduction paragraph[885]

+ADD *Doomsday Scenario* secular and religious citations[886]

Some examples of political messianism can be found in George W. Bush's rhetoric of US wars in the Middle East as "crusades"; in Bush White House advisor Hamza Yusuf's and UN peace-keeping instructor and imam to UN headquarters in Manhattan Imran Hosein's equation of ISIS with the army of "the black flags of Khorasan" in Islamic eschatological hadith[887] [888] (see also the emergence of ISIS Khorasan, known as ISIS-K); the insurgencies of jihadism and "holy warriors"; in former Iranian President Ahmedinijad's statement that his hard-liner policy "will

---

[883] National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. 90-91.

[884] https://www.nytimes.com/2020/02/18/world/europe/turkey-syria-idlib.html

[885] Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002.

[886] Bertalsky, Noah (ed.). *Doomsday Scenarios*. Greenhaven Press. 2011. PAGES

[887] Zaytuna College entitled "The Crisis of ISIS: A Prophetic Prediction. A Sermon by Hamza Yusuf" on 19 September 2014

[888] "Black Flags Army | Khurasan Afghanistan from Hadiths || Sheikh Imran Hosein" earlier speech published online 6 April 2014 < https://www.youtube.com/watch?v=REsIbkfOSDs>.

create the conditions for the arrival of the Twelfth Imam'" [889]; and in Secretary of State & former CIA Director Mike Pompeo's statement to Israel that President Trump is "possibly a modern Ester… meant to save the Jewish people."[890]

An Islamic View of Gog and Magog Imran Hosein: "when Dajjal is killed and Gog and Magog are destroyed, after the *malhama* [Armageddon] takes place, electronic warfare is not possible. No, your cellphones aren't going to work anymore. No, you probably won't have electricity after that. No, so it's going to be conventional warfare, with horses. It is at that time the Prophet said (*asws*) that the army will be unstoppable from Khorasan, marching in a straight line… until it reaches… Jerusalem."[891]

Not only is the rhetoric unmistakably political messianism, as well as the geographic centers of the violence, but those committing many of the crimes photographed in the war zones discussed here use what could be called graphic messianic symbolism. Examples include actual crucifixions under ISIS, desecration of churches and statues of the Virgin Mary by ISIS, and the so-called 2014 "Caesar" photographs of tortured victims in poses that are clearly meant to evoke renaissance-era European imagery of the crucifixion, down to the detail of red sashes placed over the genitals of emaciated male victims in Syria.[892]

Literature on the topic of political messianism as the overarching driving force behind the widespread conflicts and genocides in the Middle East is the topic of a following paper on the historicism of the Greater Middle East Plan.

+ADD from https://en.wikipedia.org/wiki/Millennialism#cite_note-16

---

[889] Kazemzadeh, Masoud. "Ahmadinejad's Foreign Policy." *Comparative Studies of South Asia, Africa and the Middle East*, Vol. 27, No. 2. 2007, p. 437.

[890] https://www.washingtonpost.com/religion/2019/03/22/pompeo-perhaps-trump-is-like-bibles-esther-meant-save-jewish-people-iran/

[891] https://www.youtube.com/watch?v=REsIbkfOSDs

[892] https://img.thedailybeast.com/image/upload/c_crop,d_placeholder_euli9k,h_1439,w_2560,x_0,y_0/dpr_1.5/c_limit,w_1044/fl_lossy,q_auto/v1492197587/articles/2014/07/31/syrian-defector-assad-poised-to-torture-and-murder-150-000-more/140731-rogin-syria5_tdgfpy

*The citation style used here takes into account computer query language, and therefore reduces traditional citation punctuation marks and limiting modifiers, such as colon marks, parentheses, and place of publication names.

Bibliography

107th Congress. “S. Rept. 107-125 - AUTHORIZATION OF ‘RADIO FREE AFGHANISTAN’”. Senate Report: Foreign Relations. US Congress. 14 December 2001. Electronic resource. <https://www.congress.gov/congressional-report/107th-congress/senate-report/125/1>.

115th Congress. “Senate Hearing 115-439 - Authority to Order the Use of Nuclear Weapons”. United States Senate Committee on Foreign Relations. U.S. Government Publishing Office. 14 November 2019. Electronic resource. <https://www.foreign.senate.gov/imo/media/doc/11%2014%2017%20Authority%20to%20Order%20the%20Use%20of%20Nuclear%20Weapons1.pdf>.

Abbott, Ernest B. and Otto J. Hetzel, eds. *A Legal Guide to Homeland Security and Emergency Management for State and Local Governments.* American Bar Association. 2005.

Abella, Alex. *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*. Harcourt Publishing. 2008.

Ackerman, Spencer. “US has trained only 'four or five' Syrian fighters against Isis, top general testifies”. *The Guardian*. 16 September 2015. Electronic resource. <https://www.theguardian.com/us-news/2015/sep/16/us-military-syrian-isis-fighters>.

Akmen, Tolga. “CIA is world’s most dangerously incompetent spy agency”. *RT*. 16 May 2017. Internet resource. <https://www.rt.com/news/388595-cia-assange-incompetent-spy/>.

AHT Staff. “Picture shows ISIS Yazidi sex slaves sold in horrifying auctions to Saudi Arabia”. *American Herald Tribune*. 25 September 2016. Electronic resource. <https://ahtribune.com/world/north-africa-south-west-asia/1221-yazidi-sex-slaves.html>.

The a-Infos Radio Project. “US Army Whistleblower says Arab Spring was a RAND Corporation ‘Product’”. 21 April 2017. *State of the City Reports*. Media resource. <http://www.radio4all.net/index.php/program/92007>.

Alito, Associate Supreme Court Justice Samuel, ed. Josh Blackman. “Video and Transcript of Justice Alito's Keynote Address to the Federalist Society”. Reason. 12 November 2020. Internet resource. <https://reason.com/volokh/2020/11/12/video-and-transcript-of-justice-alitos-keynote-address-to-the-federalist-society/>.

American Jihad. Showtime. 2017. Media resource.

Anonymous. “Opinion: Anonymous and the global correction: A loosely organised group of hackers is targeting oppressive regimes and says this is just the beginning.” *Al-Jazeera*. 16 February 2011. Internet resource. <https://www.aljazeera.com/indepth/opinion/2011/02/201121321487750509.html>.

Anonymous representative of Anonymous. “A hacktivist message announcing at ‘Anonymous Operation Last Resort at the United States Congress plan to censour any internet website’”. 5 November 2013. Internet resource. <https://en.wikiquote.org/wiki/Anonymous_(group)>.

Asher, Jeff. “US Murder Rate Remains Elevated as New Reporting System Begins”. *The New York Times*. 16 March 2021. Electronic resource. <https://www.msn.com/en-us/news/us/us-murder-rate-remains-elevated-as-new-reporting-system-begins/ar-BB1eDhEI?ocid=Peregrine>.

Associated Press. “Army investigates psyops officer for role in Washington on day of Capitol riot”. *The Guardian*. 11 January 2021. Electronic resource. <https://www.theguardian.com/us-news/2021/jan/11/army-investigates-psyops-officer-officer-emily-rainey-capitol-riot>.

Atlamazoglou, Stavros. “How Putin's favorite mercenaries are using secretive operations to tip the balance in Africa”. *Business Insider*. 9 September 2020. Electronic resource. <https://www.businessinsider.com/how-secretive-operations-by-wagner-group-mercenaries-benefit-russia-2020-9>.

Bahador, Babak. *The CNN Effect in Action: How the News Media Pushed the West Toward War in Kosovo*. New York. Palgrave Macmillan. 2007.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace”. Electronic Frontier Foundation webpage. 8 February 1996. Accessed 27 September 2020. Internet resource. <https://www.eff.org/cyberspace-independence>.

Barlow, Nathaniel S. and Steven J. Weinstein. "Accurate Closed-Form Solution of the Sir Epidemic Model". *Physica D: Nonlinear Phenomena*. Vol. 408. 2020. Electronic resource. <DOI: 10.1016/j.physd.2020.132540>.

Barr, Alan W. “Clausewitz, Nuclear War and Deterrence”. National War College; Defense Technical Information Center. 1 January 1991. Electronic resource. <https://archive.org/details/DTIC_ADA437609>.

Bartels, Elizabeth M. “Getting the Most Out Of Your Wargame: Practical Advice for Decisionmakers”. *The RAND Blog*. 26 January 2016. <https://www.rand.org/blog/2016/01/getting-the-most-out-of-your-wargame-practical-advice.html>

Bates, Robert H. “State Failure”. *Annual Reviews Political Science, Vol. 11.* 2008. Electronic resource. <10.1146/annurev.polisci.11.060606.132017>.

Begley, Sharon. “Influential COVID-19 model uses flawed methods and shouldn’t guide U.S. policies, critics say”. *STAT*. 17 April 2020. Internet resource. <https://www.statnews.com/2020/04/17/influential-covid-19-model-uses-flawed-methods-shouldnt-guide-policies-critics-say/>.

Berkeley Center for Religion, Peace & World Affairs. “Threats to Religious and Ethnic Minorities under the Islamic State”. Conference held at Georgetown University. 28 July 2016. Internet media. <https://berkleycenter.georgetown.edu/events/threats-to-religious-and-ethnic-minorities-under-the-islamic-state>.

Bertalsky, Noah (ed.). *Doomsday Scenarios*. Greenhaven Press. 2011.

Betz, Michelle. “Justice in Egypt: My so-called ‘trial’”. 23 June 2014. *Index On Censorship*. Internet resource. <https://www.indexoncensorship.org/2014/06/called-trial-egypt/>.

Bevans, Charles I., comp. “Renunciation of War as an Instrument of National Policy (Kellogg-Briand Peace Pact or Pact of Paris)”. *Treaties and other international agreements of the United States of America, 1776-1949.* Vol. 2, p. 732-736. Department of State. U.S. Government Printing Office. 1968-76. Electronic resource. <https://www.loc.gov/law/help/us-treaties/bevans/m-ust000002-0732.pdf>.

Black, Edwin. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Crown Books, 2001.

Black, Edwin. “IBM and the Holocaust”. Presentation at Yeshiva University, New York, NY. 26 February 2012. Internet resource. <https://www.youtube.com/watch?v=kQPiub5Qyqw&t=1531s>.

Bloom, Robert M. *Searches, Seizures, and Warrants: A Reference Guide to the United States Constitution.* Westport, Connecticut: Praeger, 2003.

Boms, Nir. “Virtual Reality: New Media, the Arab Spring and the Democratic Revolution”. Rābī, ‘Ūzī, and ‘Abd -I. Bū‘asrīyah. *Lost in Translation: New Paradigms for the Arab Spring*. Sussex Academic Press. 2017. Electronic resource. <http://web.b.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzE1MzE2NzBfX0FO0?sid=495ae052-185a-4f11-b510-b55a95ed720b@pdc-v-sessmgr05&vid=0&format=EB&lpid=lp_298&rid=0>.

Bose, Meena and Rosanna Perotti. *From Cold War to New World Order: The Foreign Policy of George H.W. Bush*. Hofstra University Contributions in Political Science, No. 393. Greenwood Press. 2002.

Boseley, Sarah. “Female refugees from Syria 'blighted by gynaecological illness and stress'”. *The Guardian*. 19 February 2014. Internet resource. <https://www.theguardian.com/world/2014/feb/20/female-refugees-syria-gynaecological-stress-illness>.

Brimelow, Ben. “Syria Is Now 'The Most Aggressive Electronic Warfare Environment On The Planet,' SOCOM Says”. 26 April 2018. *Task and Purpose.* Internet resource. <https://taskandpurpose.com/syria-aircraft-disabled-electronic-warfare>.

The Brookings Institution. “Middle East Crises and Conflicts - The Way Ahead”. Washington, D.C. 5 October 2017. Transcript. <https://www.brookings.edu/wp-content/uploads/2017/10/fp_20171005_mideast_crises_transcript.pdf>.

Brown, Barrett. “Why FBI Agent Robert Smith Has Two Weeks To Send my Property Back”, parts 1-3. *YouTube.* 11 September 2012. Internet media. <https://www.youtube.com/watch?v=klvP1Xx6OH4>.

Brueck, Hilary. “Dr. Fauci said he's 'so sorry' the worst-nightmare pandemic scenario he outlined a year ago has become reality”. *Business Insider.* 9 July 2020. Internet resource. <https://www.businessinsider.com/fauci-sorry-nightmare-pandemic-scenario-was-right-2020-7>.

Burrough, Brian, Sarah Ellison and Suzanna Andrews. “The Snowden Saga: a shadowland of secrets and light”. *Vanity Fair*. May 2014. Electronic resource. <https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview>.

Casey-Maslen, Stuart. *Non-kinetic-energy weapons termed ‘non-lethal’ A Preliminary Assessment under International Humanitarian Law and International Human Rights Law*. Geneva Academy of International Humanitarian Law and Human Rights. October 2010. Electronic resource. <https://www.geneva-academy.ch/joomlatools-files/docman-files/Non-Kinetic-Energy%20Weapons.pdf>.

Center for Health Security. Event 201 Players: Avril Haines. Center for Health Security webpage. Accessed 20 January 2021. Internet resource. <https://www.centerforhealthsecurity.org/event201/players/haines.html>.

Chafkin, Max. “How to Take Back Your Email”. *Bloomberg Businessweek: How To Fight Big Tech*. 12 August 2019.

Chastain, Mary. “Amnesty International: ISIS Driving Yazidi Women to Suicide Through Rape, Sex Slavery”. *Breitbart.* 23 December 2014. Electronic resource. <https://www.breitbart.com/national-security/2014/12/23/amnesty-international-isis-driving-yazidi-women-to-suicide-through-rape-sex-slavery/>.

Clark, Neil. “Op-Ed: Slave Markets in ‘Liberated’ Libya and the Silence of Humanitarian Hawks”. *RT*. 1 December 2017. Electronic resource. <https://www.rt.com/op-ed/411562-libya-slave-markets-nato/>.

Clark, General Wesley and Amy Goodman. “Global Warfare: ‘We’re Going to Take out 7 Countries in 5 Years: Iraq, Syria, Lebanon, Libya, Somalia, Sudan & Iran...’: Video Interview with General Wesley Clark”. *Global Research.* 14 June 2019; *Democracy Now!*. 2 March 2007. Internet resource. <https://www.globalresearch.ca/we-re-going-to-take-out-7-countries-in-5-years-iraq-syria-lebanon-libya-somalia-sudan-iran/5166>.

Clarke, Colin P. "ISIS Is So Desperate It's Turning to the Drug Trade”. The RAND Blog. 25 July 2017. Internet resource. <https://www.rand.org/blog/2017/07/isis-is-so-desperate-its-turning-to-the-drug-trade.html>.

Clarity, James F. “BREIFING; Come In, Afghanistan”. *The New York Times.* 1 October 1985. Internet resource. https://www.nytimes.com/1985/10/01/us/briefing-come-in-afghanistan.html

Clow, Ryan. “Psychological Operations: The Need To Understand The Psychological Plane of Warfare”. *Canadian Military Journal (CMJ), Vol. 9, No. 1.* 2008. <http://www.journal.forces.gc.ca/vo9/no1/05-clow-eng.asp>.

Cohen, Alexander H., John Alden and Jonathan J. Ring. *Gaming the System: Nine Games to Teach American Government through Active Learning.* NY: Routledge. 2020.

Collman, Ashley. “Meet Trump's new coronavirus adviser Dr. Scott Atlas, a Stanford physician who frequently criticized lockdown measures and believes in the full reopening of schools”. Business Insider. 13 August 2020. Electronic resource. <https://www.businessinsider.com/scott-atlas-new-medical-adviser-anti-lockdown-pro-schools-reopening-2020-8>.

Compton, Jon. “The Obstacles on the Road to Better Analytical Wargaming”. *War on the Rocks.* 9 October 2019. < https://warontherocks.com/2019/10/the-obstacles-on-the-road-to-better-analytical-wargaming/>

Conti, Mauro et al. “Analyzing Android Encrypted Network Traffic to Identify User Actions.” *IEEE Transactions on Information Forensics and Security,* Vol. 11. 2016. Electronic resource. <https://www.semanticscholar.org/paper/Analyzing-Android-Encrypted-Network-Traffic-to-User-Conti-Mancini/e46b0fe8d8be88617494c58a0f5c5cea9e0f37fb>.

Constine, Josh. “Facebook announces Libra cryptocurrency: All you need to know. The use cases, technology and motive behind the new digital money”. *Tech Crunch.* 18 June 2019. Internet resource. <https://techcrunch.com/2019/06/18/facebook-libra/>.

Cooper, Michael. “THE 2000 CAMPAIGN: THE REPUBLICAN RUNNING MATE; Cheney Urges Rethinking Use of U.S. Ground Forces In Bosnia and Kosovo”. *The New York Times*. 1 September 2000. Electronic resource. <https://www.nytimes.com/2000/09/01/us/2000-campaign-republican-running-mate-cheney-urges-rethinking-use-us-ground.html>.

“Cory Doctorow: EFF Special Advisor”. *EFF: Electronic Frontier Foundation*. Accessed 8 August 2019. Internet resource. <https://www.eff.org/about/staff/cory-doctorow>.

Crabtree, Susan. “On Trump's ICC Win, Dems and Republicans See Eye to Eye”. *Real Clear Politics.* 15 April 2019. Internet resource. <https://www.realclearpolitics.com/articles/2019/04/15/on_trumps_icc_win_dems_and_republicans_see_eye_to_eye_140052.html>.

Cull, Nicholas J. *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989.* Cambridge University Press. 2008.

Cushman, Thomas and Stjepan G. Mestrovic. “Introduction”. *This Time We Knew: Western Responses to Genocide in Bosnia.* New York University Press. 1996.

Dadrian, Vahakn N. *Warrant for Genocide: Key Elements of Turko-Armenian Conflict*. Transaction Publishers. 1999, p. 100-101.

Davey, Melissa, Stephanie Kirchgaessner and Sarah Boseley. “Surgisphere: governments and WHO changed Covid-19 policy based on suspect data from tiny US company”. *The Guardian.* 3 June 2020. Electronic resource. <https://www.theguardian.com/world/2020/jun/03/covid-19-surgisphere-who-world-health-organization-hydroxychloroquine>.

Dobson, J.E, and P.F Fisher. "Geoslavery." *IEEE Technology and Society Magazine*, Vol. 22, No.1. 2013. pp. 47-52. Electronic resource. <https://msu.edu/~kg/874/geoslavery.pdf>.

Doctorow, Cory. “Cyberwar guide for Iran elections”. *Boing Boing*. 16 June 2009. Internet resource. <https://boingboing.net/2009/06/16/cyberwar-guide-for-i.html>.

Doyle, Michael W. *Empires.* Ithaca, NY: Cornell University Press, 1986.

Dubin, Ran et al. “I Know What You Saw Last Minute—Encrypted HTTP Adaptive Video Streaming Title Classification.” *IEEE Transactions on Information Forensics and Security,* Vol. 12. 2017. Electronic resource. <https://www.semanticscholar.org/paper/I-Know-What-You-Saw-Last-Minute—Encrypted-HTTP-Dubin-Dvir/2aa3ce79cc14b93a38e3ae6246ba34ccac91035b>.

Dunnigan, James F. and Albert A. Nofi. *Dirty Little Secrets: Military Information You’re Not Supposed to Know*. William Morrow and Company, Inc. 1990.

Durant, Will and Ariel. *The Story of Civilization, Part X: Rousseau and Revolution*. Simon and Schuster. New York, 1967, p. 665-66. Electronic resource. <https://archive.org/stream/TheStoryOfCivilizationcomplete/Durant_Will__The_story_of_civilization_3#page/n715/mode/2up/search/failing+trade>.

Ernst, Falko. “’The training stays with you’: the elite Mexican soldiers recruited by cartels”. The Guardian. 10 February 2018. Electronic resource. <https://www.theguardian.com/world/2018/feb/10/mexico-drug-cartels-soldiers-military>.

Eskeline, Pekka.“The Story Behind Finnish Telecommunications Industry: Military Radio Systems and Electronic Warfare in Finland during World War I1 (1939-1945)”. *IEEE AES Systems Magazine*, Vol. 11, No.8. August 1996, pp. 6-7. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=533747>

Eskander, Saad. “The Tale of Iraq's 'Cemetery of Books'”. *Information Today*, Vol. 21 No. 11. 11-12 October 2004. Electronic resource. <http://www.infotoday.com/it/dec04/eskander.shtml>.

“Face of Egypt's 2011 revolution asks el-Sisi to repent in video: Wael Ghonim says the president should apologise to widow of Mohamed Morsi, Egypt's first democratically elected leader.” *Al-Jazeera.* 11 September 2019. Electronic resource. <https://www.aljazeera.com/news/2019/09/face-egypt-2011-revolution-asks-el-sisi-repent-video-190911162025694.html>.

Federal Bureau of Investigation. “The FBI’s Role in a War Zone”. U.S. Department of Justice FBI webpage. 18 April 2011. Media resource. <https://www.fbi.gov/video-repository/newss-the-fbis-role-in-a-war-zone/view>.

Fiscal Year 2006 Defense Budget. 10 March 2005. C-SPAN. Media resource. <https://www.c-span.org/video/?185842-1/fiscal-year-2006-defense-budget>.

Francis, Jeff. “Police say human traffickers are turning to Bitcoin”. *Bitcoinist.* 15 October 2017. Internet resource. <https://bitcoinist.com/police-say-human-traffickers-are-turning-to-bitcoin/>.

Freedberg, Sydney J., Jr. “Can Army Afford The Electronic Warfare Force It Wants?”. *Breaking Defense*. 19 November 2018. Electronic resource. <https://breakingdefense.com/2018/11/can-army-afford-electronic-warfare-force-it-wants/>.

Friedman, Uri. “Why Venezuela's Revolution Will Be Tweeted The country's street protests are playing out dramatically on the social network.” *The Atlantic.* 19 February 2014. Electronic resource. <https://www.theatlantic.com/international/archive/2014/02/why-venezuelas-revolution-will-be-tweeted/283904/>.

Freelon, Deen. “The MENA protests on Twitter: Some empirical data”. *Dfreelon.org*. 19 May 2011. Internet resource. <http://dfreelon.org/2011/05/19/the-mena-protests-on-twitter-some-empirical-data/>.

"Former US envoy calls for military action against Sudan". 17 June 2011. *Sudan Tribune*. Electronic resource. <http://www.sudantribune.com/Former-US-envoy-calls-for-military,39243>.

Ghandour, Christel. *ISIS's Use of Sexual Violence in Iraq.* Washington: Academica Press. 2019.

Gilmour, David. "Twitter lifts 'permanent' suspension of activist Barrett Brown Twitter says the suspension was an 'error.'" *The Daily Dot.* (24 June 2019). Internet resource. <https://www.dailydot.com/layer8/barrett-brown-twitter-suspension/>.

Glenn, Russell W., et al. *Ready for Armageddon: Proceedings of the 2001 RAND Arroyo-U.S. Army ACTD-CETO-USMC Non-Lethal and Urban Operations Program Urban Operations Conference*, 22-23 March 2001. The RAND Corporation. 2002. Electronic resource. <https://www.rand.org/pubs/conf_proceedings/CF179.html>.

de Goede, Marieke, Esmé Bosma and Polly Pallister-Wilkins. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork.* NY: Routledge. 2020.

Goldstein, Emmanuel. *The Theory and Practice of Oligarchical Collectivism*. The Ministry of Truth: Airstrip 1. 1984.

Goode, Erich. *Paranormal Beliefs: A Sociological Introduction.* Waveland Press. Illinois. 2000.

Goodin, Dan. "Use of Tor and e-mail crypto could increase chances that NSA keeps your data". *Ars technica.* 20 June 2013. Internet resource. <https://arstechnica.com/tech-policy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-data/>.

Goodman, Peter S. "Brexit's Advance Opens a New Trade Era". *The New York Times.* 13 December 2019. Electronic resource. <https://www.nytimes.com/2019/12/13/business/economy/uk-election-brexit-trade.html>.

GT Staff Reporters. "Wuhan pathogen biologist addresses six conundrums about deadly novel coronavirus". *Global Times*. 16 February 2020. Electronic resource. <https://www.globaltimes.cn/content/1179745.shtml>.

Guzman, Genevieve de. ""Smart" Contact Lenses: Spy Gadget or Formidable Threat to Privacy?". *The Richmond Journal of Law and Technology.* 16 January 2017. University of Richmond School of Law. Electronic resource. <https://jolt.richmond.edu/2017/01/16/smart-contact-lenses-spy-gadget-or-formidable-threat-to-privacy/>.

The Hacker Wars. United States: Phase4, 2015. Media resource.

Hafner, Marco, Erez Yerushalmi, Clement Fays, Eliane Dufresne, and Christian Van Stolk, *COVID-19 and the Cost of Vaccine Nationalism.* The RAND Corporation. 2020. Electronic resource. <https://www.rand.org/pubs/research_reports/RRA769-1.html>.

Hall, Mathison. "Patrolling in the Infosphere". Future Warfare Writing Program. The Army University Press. 2017. Electronic resource. <https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/Patrolling-in-the-Infosphere/>.

O'Hanlon, Michael. "Commentary: Who Will Hold Together the Future Syria?". *Defense News*. 8 September 2015. Electronic resource. <https://www.defensenews.com/opinion/commentary/2015/09/08/commentary-who-will-hold-together-the-future-syria/>.

Harper, Reginald. "Strategic Joint Wargame Challenges Future Leaders Ability to Think Multidimensional". *Maxwell Air Force Base News.* 29 March 2017. <https://www.maxwell.af.mil/News/Commentaries/Display/Article/1134598/strategic-joint-wargame-challenges-future-leaders-ability-to-think-multidimensi/>

Harrison, Weber. “How the NSA & FBI made Facebook the perfect mass surveillance tool”. *Venture Beat*. 15 May 2014. Internet resource. <https://venturebeat.com/2014/05/15/how-the-nsa-fbi-made-facebook-the-perfect-mass-surveillance-tool/>.

Harvey, Fiona. “Record-size hole opens in ozone layer above the Arctic”. *The Guardian.* 7 April 2020. Electronic resource. <https://www.theguardian.com/environment/2020/apr/07/record-size-hole-opens-in-ozone-layer-above-the-arctic>.

Hazelwood, Robert R., Park Elliott Dietz and Janet Warren. “The Criminal Sexual Sadist”. *FBI Law Enforcement Bulletin*, Vol. 61, No. 2. February 1992. United States Department of Justice Federal Bureau of Investigation. Electronic resource. <https://www.ncjrs.gov/pdffiles1/Digitization/134598NCJRS.pdf>.

Heath, Garrett and Oleg Svet. “We Run Wargames Programs for the Joint Staff. Here’s What We’ve Learned”. Modern War Institute at West Point website. 19 October 2018. Internet resource. < https://mwi.usma.edu/run-wargames-programs-joint-staff-heres-weve-learned/>.

Hedges, Chris. “Heeding Death Threats, Red Cross Leaves Kosovo”. *International Herald Tribune*. 12 March 1998.

Higgins, John. “Raven Claw Augments Battle Management for Electronic Warfare Operations”. *Army.mil.* 22 January 2018. Electronic resource. <https://www.army.mil/article/199368/raven_claw_augments_battle_management_for_electronic_warfare_operations>.

Hodgson, Quentin E. et al. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.* The RAND Corporation. 2019. Electronic resource. < https://www.rand.org/pubs/research_reports/RR2961.html>.

Hoehn, Andrew R., Albert A. Robbert, and Margaret C. Harrell. *Succession Management for Senior Military Positions: The Rumsfeld Model for Secretary of Defense Involvement*. The RAND Corporation. 2011. Electronic resource. <https://www.rand.org/pubs/monographs/MG1081.html>.

Hoehn, John R. *Defense Primer: Electronic Warfare.* Congressional Research Service. 29 October 2020. Electronic resource. <https://fas.org/sgp/crs/natsec/IF11118.pdf>.

Hyde, Charles K. *Arsenal of Democracy: The American Automobile Industry in World War II*. Detroit: Wayne State University Press, 2013.

Ignatieff, Michael. *Virtual War: Kosovo and Beyond.* Metropolitan Books. 2000.

“Iraq: Yezidi women and girls face harrowing sexual violence”. *Amnesty International News.* 23 December 2014. Electronic resource. <https://www.amnesty.org/en/latest/news/2014/12/iraq-yezidi-women-and-girls-face-harrowing-sexual-violence/>.

Jacob, Marcus and Marcell Tyrell. “The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany”. *Mediengruppe Thüringen Verlag*. 10 June 2010. Electronic resource. <http://www.zgtonline.de/portal/download/studie_jacob_tyrell.pdf >.

JASON. *Artificial Intelligence for Health and Health Care*. JASON The MITRE Corporation. December 2017. Electronic resource. <https://www.healthit.gov/sites/default/files/jsr-17-task-002_aiforhealthandhealthcare12122017.pdf>.

JASON. *Managing the Risk From COVID-19 During a Return to On-Site University Research*. JASON The MITRE Corporation. 10 July 2020. Electronic resource. <https://fas.org/irp/agency/dod/jason/covid-19.pdf>.

Al-Jazeera Staff. “Memo: Bush wanted Aljazeera bombed”. Al-Jazeera. 22 November 2005. Internet resource. <https://www.aljazeera.com/archive/2005/11/20084101516279965 59.html>.

Ji-wei, Colonel Guo and Xue-sen Yang. “Ultramicro, Nonlethal, and Reversible Looking Ahead to Military Biotechnology”. *Military Review*. July-August 2005. Electronic resource. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Dir-Select/nano-technology.pdf>.

Johnson, Chalmers. “A Litany of Horrors: America’s University of Imperialism”. *Tomgram: Chalmers Johnson, Teaching Imperialism 101*. TomDispatch. 29 April 2008. Internet resource. <http://www.tomdispatch.com/post/174925/chalmers_johnson_teaching_imperialism_101>.

Johnston, Trevor, et al. *Could the Houthis Be the Next Hizballah? Iranian Proxy Development in Yemen and the Future of the Houthi Movement*. The RAND Corporation. 2020. Electronic resource. <https://www.rand.org/pubs/research_reports/RR2551.html>.

Joy, William. “New video reveals more about Texas connections to attack on US Capitol”. WFAA-ABC. 17 January 2021. Internet resource. <https://www.wfaa.com/article/news/crime/new-video-reveals-more-about-texas-connections-to-attack-on-us-capitol/287-1daf429a-736d-4ad5-b57a-b19bd4643c09>.

Kahn, Herman. *On Thermonuclear War*. Princeton University Press. 1960.

Karanth, Sanjana and Roque Planas. “Trump On Turkey And Kurds: ‘You Have To Let Them Fight Like 2 Kids’”. *The Huffington Post.* 17 October 2019. Internet resource. https://www.huffpost.com/entry/trump-turkey-kurds-let-kids-fight-dallas-rally_n_5da90201e4b0e0f037890e43

Karolak, Magdalena. *The Social Media Wars: Sunni and Shia Identity Conflicts in the Age of the Web 2.0 and the Arab Spring*. Academica Press. 2014

Katkov, Mark. “Biden Pick For Intel Chief: 'Biggest Challenge Is Building Trust And Confidence'”. *NPR*. 19 January 2021. Electronic resource. <https://www.npr.org/sections/biden-transition-updates/2021/01/19/958293679/biden-pick-for-intel-chief-avril-haines-goes-before-senate-committee>.

Kazemzadeh, Masoud. "Ahmadinejad's Foreign Policy." *Comparative Studies of South Asia, Africa and the Middle East*, Vol. 27, No. 2. 2007, p. 423-449. Electronic resource. <muse.jhu.edu/article/220766>.

Kende, Michael. “The Digital Handshake: Connecting Internet Backbones”. *OPP Working Paper*, No. 32. Office of Plans and Policy, Federal Communications Commission. September 2000. Working paper. <https://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf>.

Kennedy, Sen. Edward M. “Statement of Senator Edward M. Kennedy on the Nuclear Weapons Freeze Amendment to the Debt Ceiling”. *Office of Senator Edward M. Kennedy of Massachusetts*. 5 October 1984.

King, Lieutenant Colonel James. “Review - Eagle Down: The Last Special Forces Fighting the Forever War”. *Small Wars Journal*. 23 February 2021. Internet resource. <https://smallwarsjournal.com/jrnl/art/review-eagle-down-last-special-forces-fighting-forever-war>.

Korybko, Andrew. “RAND Corporation Proves Link Between US Military And Hybrid War”. *Oriental Review*. 27 February 2018. Electronic resource. <https://orientalreview.org/2018/02/27/rand-corporation-proves-link-us-military-hybrid-war/>.

Kovach, Nicholas S., Alan S. Gibson, and Gary B. Lamont. “Hypergame Theory: A Model for Conflict, Misperception, and Deception.” *Game Theory*, Vol. 2015. 19 August 2015. Electronic resource. < https://doi.org/10.1155/2015/570639>.

Knowlton, Brian. “Clinton Tries to Reassure UN Leader”. *International Herald Tribune*. 12 March 1998. **PAGE**

Kurtz, Howard. “Huffington snags N.Y. Times star”. *The Washington Post.* 21 September 2010. Electronic resource. <http://voices.washingtonpost.com/howard-kurtz/2010/09/huffington_snags_ny_times_star.html>.

Larson, Carl A. “Ethnic Weapons”. *Military Review*. November 1970. Accessed at Future Warfare Writing Program. The Army University Press. Electronic resource. <https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/Non-Fiction/Ethnic-Weapons/>.

Lester, Paul. “Gil Scott-Heron: the revolution lives on”. *The Guardian*. 26 August 2015. Electronic resource. <https://www.theguardian.com/music/2015/aug/26/gil-scott-heron-the-revolution-will-not-be-televised>.

Levin, Kenneth. *The Oslo Syndrome: Delusions of a People under Siege.* Smith and Kraus, 2005.

Lindsay, James M. “The Water’s Edge: TWE Remembers Thich Quang Duc’s Self-Immolation”. *Council on Foreign Relations blog post*. 11 June 2012. Internet resource. <https://www.cfr.org/blog/twe-remembers-thich-quang-ducs-self-immolation>.

Lindsey, Richard A. “What the Arab Spring Tells Us About the Future of Social Media in Revolutionary Movements”. *Small Wars Journal*, 2013. Electronic resource. <https://smallwarsjournal.com/jrnl/art/what-the-arab-spring-tells-us-about-the-future-of-social-media-in-revolutionary-movements>.

Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R. et al. “Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning”. *Springer*. 13 May 2019. Electronic resource. <https://link.springer.com/article/10.1007/s00500-019-04030-2>.

Lyman, Will, et al.. *Frontline: United States of Secrets: The Inside Story of the Government’s Mass Surveillance Program.* 2014. Electronic media.

MacDonald, David Bruce. *Balkan holocausts?: Serbian and Croatian victim-centered propaganda and the war in Yugoslavia.* Manchester University Press, New York. 2002.

“Macron urges military action in Libya to fight human trafficking”. *RT*. 30 November 2017. Electronic resource. <https://www.rt.com/news/411428-macron-military-action-libya/>.

Magee, Tamlin. “US government can’t compete in information war, warns RAND Corporation: The RAND Corporation’s Dr Rand Waltzman speaks with Techworld on the state of ‘cognitive security’ in the world and the ‘democratization of weapons of mass disruption”. *TechWorld*. 12 February 2018. https://www.techworld.com/security/inside-rand-corporations-proposal-for-cognitive-security-center-3671929/

O'Mahony, Angela, et al. *U.S. Presence and the Incidence of Conflict*. The RAND Corporation. 2018. Electronic resource. <https://www.rand.org/pubs/research_reports/RR1906.html>.

Marinoff, Nicholas. “DOJ lawsuit over tell-all book is "good for Bitcoin," says Edward Snowden”. *Decrypt*. 18 September 2019. Internet resource. <https://decrypt.co/9365/doj-lawsuit-over-tell-all-book-good-for-bitcoin-edward-snowden>.

Martha’s Vineyard Productions. “Bill Clinton The President is Missing”. Martha’s Vineyard Author Series. 30 December 2018. Media resource. <https://www.youtube.com/watch?v=NwIldViugQA>.

Martin, Zachary. *The Hydra: the strategic paradox of human security in Mexico*. Wright Flyer Paper No. 78. Air University Press. 2020. Electronic resource. <https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_0078_MARTIN_THE_HYDRA_THE_STRATEGIC_PARADOX_OF_HUMAN_SECURITY_IN_MEXICO.pdf>.

Martinez, Luis. “DOD suspends operational training for all Saudi students in wake of Pensacola shooting”. *ABC News.* 10 December 2019. Electronic resource. <https://abcnews.go.com/Politics/dod-suspends-operational-training-saudi-students-wake-pensacola/story?id=67636356>.

Marzūqī, Abū Ya´rub. Mafhūm al-sababīyyah ‘ind al-Ghazālī. Bouslama. Tunis. 1978.

Matossian, Mary Kilbourne. “The Time of the Great Fear”. *Sciences,* Vol. 24, Iss. 2, pp. 38-41. New York Academy of Sciences. 1 March 1984. Electronic resource. <https://doi.org/10.1002/j.2326-1951.1984.tb02694.x >.

Maxar Technologies. “Maxar Technologies’ DigitalGlobe Celebrates First Year of Its News Bureau Initiative, Applying Space-Based Insights to Enhance Global Transparency”. 5 March 2018. Internet resource. <http://investor.maxar.com/investor-news/press-release-details/2018/Maxar-Technologies-DigitalGlobe-Celebrates-First-Year-of-Its-News-Bureau-Initiative-Applying-Space-Based-Insights-to-Enhance-Global-Transparency/default.aspx>.

McMillan, M.E. *From the First World War to the Arab Spring: what’s really going on in the Middle East?* Palgrave MacMillan: NY. 2016.

Melley, Timothy. *The Covert Sphere : Secrecy, Fiction, and the National Security State*. Cornell University Press. 2012, viii. Electronic resource. <https://doi.org/10.1017/S0021875814000255>.

Michaud, Stephen G. and Roy Hazelwood. *The Evil That Men Do: FBI Profiler Roy Hazelwood’s Journey into the Minds of Sexual Predators.* St. Martin’s Press: NY. 1998.

Michel, Arthur Holland. *Eyes in the Sky: the Secret Rise of Gorgon Stare and How It Will Watch Us All.* Houghton Mifflin Harcourt. 2019.

Monaci, Sarah. “Explaining the Islamic State’s Online Media Strategy: A Transmedia Approach”. *International Journal of Communication*, Vol. 11, pp. 2842–2860. 2017. Electronic resource. LINK

Morton, Jesse. “Opinion: I Invented the Jihadist Journal: I deradicalized after 3½ years in prison. Now I’m reclaiming the medium to combat violent extremism”. *Wall Street Journal.* 3 June 2019. Electronic resource. <https://www.wsj.com/articles/i-invented-the-jihadist-journal-11559602751>.

Morton, Jesse and Mitchell Silber. “NYPD vs. Revolution Muslim: The Inside Story of the Defeat of a Local Radicalization Hub”. *CTC Sentinel, Vol. 11, Issue 4.* Combating Terrorism Center at West Point. April 2018. Electronic resource. <https://ctc.usma.edu/nypd-vs-revolution-muslim-inside-story-defeat-local-radicalization-hub/>.

Almubayed, Alaeddin & Hadi, Ali & Atoum, Jalal. “A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning”. *International Journal of Computer Network and Information Security (IJCNIS)*. 2014. Electronic resource. <https://www.researchgate.net/publication/277611386_A_Model_for_Detecting_Tor_Encrypted_Traffic_using_Supervised_Machine_Learning>.

Muehlstein, Jonathan & Zion, Yehonatan & Bahumi, Maor & Kirshenboim, Itay & Dubin, R & Dvir, Amit & Pele, Ofir. “Analyzing HTTPS Encrypted Traffic to Identify User Operating System, Browser and Application”. 15 March 2016. Electronic resource. <https://www.researchgate.net/publication/301878874_Analyzing_HTTPS_Encrypted_Traffic_to_Identify_User_Operating_System_Browser_and_Application>.

Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. Free Press. 2006.

Nafeez, Ahmed. “Whistleblower exposes how NATO’s leading ally is arming and funding ISIS: ‘I am the police chief who was asked to guard ISIS terrorists’”. *Insurge Intelligence.* 16 September 2016. Electronic resource. <https://medium.com/insurge-intelligence/former-turkish-counter-terror-chief-exposes-governments-support-for-isis-d12238698f52>.

National Intelligence Council. *Global Trends 2025: A Transformed World*. U.S. Government Printing Office. November 2008, p. xi. <www.dni.gov/nic/NIC_2025_project.html>

National Sheriffs' Association. *Animal Cruelty as a Gateway Crime.* Community Oriented Policing Services U.S. Department of Justice. 2018. Electronic resource. <https://cops.usdoj.gov/RIC/Publications/cops-w0867-pub.pdf>.

O'Neill, Patrick Howell. "NATO will establish new cyber command centers". *Cyber Scoop.* 9 November 2017. Internet resource. <https://www.cyberscoop.com/nato-cyber-command-centers/>.

Nieva, Richard. "YouTube bans videos containing hacked information that could interfere with the election". *CNET.* 13 August 2020. Internet resource. <https://www.cnet.com/news/ahead-of-dnc-and-rnc-conventions-youtube-bans-videos-containing-hacked-information/>.

Nixon, Ron. "U.S. Groups Helped Nurture Arab Uprisings". *The New York Times*. 14 April 2011. Electronic resource. <https://www.nytimes.com/2011/04/15/world/15aid.html?pagewanted=1&_r=2&emc=eta1&mtrref=undefined&assetType=REGIWALL>.

"Nuclear Explosion in the Sky". Excerpt from *Electronic Armageddon*. National Geographic. *YouTube*. 2 June 2010. <https://www.youtube.com/watch?v=PPzIWsdnj0w>.

Parisi, Jessica, "Game Changers in US Defense Strategy: An Examination of the Causes Behind the Increased Emphasis on Irregular Warfare Since 9/11". *CUREJ: College Undergraduate Research Electronic Journal, University of Pennsylvania.* 08 April 2011. http://repository.upenn.edu/curej/140.

Penenberg, Alan. "The Troll's Lawyer". *Wired*. 5 January 2015. Internet resource. <https://www.wired.com/2015/01/the-trolls-lawyer/>.

Perla, Peter P. et al. "Rolling the Iron Dice: From Analytical Wargaming to the Cycle of Research". *War on the Rocks.* 21 October 2019. Internet resource. < https://warontherocks.com/2019/10/rolling-the-iron-dice-from-analytical-wargaming-to-the-cycle-of-research/>

Perraudin, Frances and Shiv Malik. "Boris Johnson: jihadis are porn-watching 'wankers'". *The Guardian.* 30 January 2015. Electronic resource. <https://www.theguardian.com/politics/2015/jan/30/boris-johnson-jihadis-are-porn-watching-wankers>.

Phillips, Peter, Lew Brown and Bridget Thornton. *US Electromagnetic Weapons and Human Rights: A Study of the History of US Intelligence Community Human Rights Violations and Continuing Research in Electromagnetic Weapons*. Rohnert Park, CA: Sonoma State University Media Freedom Foundation. December 2006. Electronic resource. <http://www.projectcensored.org/wp-content/uploads/2010/05/ElectromegnaticWeapons.pdf>.

Pincus, Walter. "U.S. Senators Push for Aid to Opponents of Saddam". *International Herald Tribune*. 12 March 1998.

Pinsker, Joe. "Here Come the COVID-19 Baby Bust". The Atlantic. 24 November 2020. Internet resource. <https://www.theatlantic.com/family/archive/2020/11/covid-19-pandemic-births-baby-bust/617149/>.

"PM Narendra Modi congratulates Google CEO Sundar Pichai on Twitter, others join in". 11 August 2015. *The Indian Express.* Electronic resource. <https://indianexpress.com/article/india/india-others/pm-narendra-modi-congratulates-sundar-pichai-on-twitter-others-join-in/>.

"Profile: Facebook Inc (FB.O)". *Reuters*. Accessed 31 July 2019. Electronic resource. <https://www.reuters.com/finance/stocks/company-profile/FB.O>.

"Profile: Twitter Inc (TWTR.N)". *Reuters*. Accessed 31 July 2019. Electronic resource. <https://www.reuters.com/finance/stocks/company-profile/TWTR.N>.

Profiles. "Scott W. Atlas: Senior Fellow at the Hoover Institute". *Stanford University webpage*. Accessed 13 August 2020. Internet resource. <https://profiles.stanford.edu/scott-atlas?tab=bio>.

Ries, Charles P. “The Year of the Arab Spring”. *The RAND Blog*. 20 December 2011. Internet resource. <https://www.rand.org/blog/2011/12/the-year-of-the-arab-spring.html>.

Roselle, Laura. *Media and the Politics of Failure: Great powers, communication strategies, and military defeats.* Palgrave Macmillian. Series in International Political Communication. 2006.

Rosenberg, Milton J. (ed.). *Beyond Conflict and Containment: Critical Studies of Military and Foreign Policy.* Transaction Books. 1972.

Rosenberger, Laura and Lindsay Gorman. “How Democracies Can Win the Information Contest”. *The Washington Quarterly, Vol. 43, No. 2.* Summer 2020. The Elliot School of International Affairs. Electronic resource. <https://doi.org/10.1080/0163660X.2020.1771045>.

Rothman, Lily. “Why the United States Controls Guantanamo Bay”. *TIME Magazine*. 22 January 2015. Electronic resource. <https://time.com/3672066/guantanamo-bay-history/>.

Roy, Oliver. *The Politics of Chaos in the Middle East*. Columbia University Press. 2008.

Ryan, Yasmine. “Anonymous and the Arab uprisings: The cyberactivists discuss their work and the broader global push for freedom of speech and freedom from oppression.” *Al-Jazeera*.
19 May 2011. Internet resource.
<https://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html>.

Saltzman Institute of War and Peace Studies. “Disruptive Technologies, Strategic Vulnerability, and the Future of Deterrence”. *Columbia University Arnold A. Saltzman Institute of War and Peace Studies webpage*. Accessed 20 August 2020. Internet resource. <https://www.siwps.org/research/disruptive-technologies-strategic-vulnerability-and-the-future-of-deterrence/>.

Said, Edward. *Orientalism*. Vintage Books: New York. 1978.

SAR. “MAXAR’s Initiative Focused on High-Resolution Imagery”. *SAR Journal*. 6 March 2018. Electronic resource. <http://syntheticaperturerадar.com/maxars-initiative-focused-on-high-resolution-imagery/>.

“Ṣaydnāyā”. *Wikipedia (Arabic).* Accessed 2 January 2020. Internet resource. <https://ar.wikipedia.org/wiki/صيدنايا>.

Schweller, Randall L. “Neorealism’s Status-Quo Bias: What Security Dilemma?” *Security Studies*, Vol. 5, No. 3. 24 December 2007. Electronic resource. DOI: 10.1080/09636419608429277.

Senate Select Committee on Intelligence. *The Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency’s Detention and Interrogation Program*. Melville House. December 2014.

Shesgreen, Deirdre. “Pompeo says US will take ‘all necessary measures’ to bar war crimes probe of military”. USA TODAY. 5 March 2020. Electronic resource. <https://www.usatoday.com/story/news/world/2020/03/05/pompeo-says-us-shield-troops-international-war-crimes-probe/4897766002/>.

“Syria's Saydnaya prison crematorium hid killings, says US”. *BBC*. 15 May 2017. Electronic resource. <https://www.bbc.com/news/world-middle-east-39926914>.

Scarito, Michael. “Build Your Own Radar System”. DEFCON. August 2011. Internet resources. <https://www.youtube.com/watch?v=8nJIeVeOeBA>; <https://www.defcon.org/html/defcon-19/dc-19-speakers.html>.

Scheyder, Ernest. “Exclusive: Pentagon to stockpile rare earth magnets for missiles, fighter jets”. *Reuters.* 20 December 2019. Electronic resource. <https://www.reuters.com/article/us-usa-rareearths-magnets-exclusive/exclusive-pentagon-to-stockpile-rare-earth-magnets-for-missiles-fighter-jets-idUSKBN1YO0G7>.

Alshammari, Riyad & Zincir-Heywood, A. . Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?. *Computer Networks*. Vol. 55, Issue 6. Elsevier. April 2011. Electronic resource. <https://www.sciencedirect.com/science/article/abs/pii/S1389128610003695?via%3Dihub>.

Specht, Robert D. *War Games.* Santa Monica, California. The RAND Corporation. 18 March 1957. Electronic resource. https://www.rand.org/pubs/papers/P1041.html
Spiller, Sarah and Callum Macrae. "Interpol: Red Alert!: How states have used Interpol alerts to persecute exiled dissidents and refugees across international borders". *Al-Jazeera*. 12 January 2017. Internet resource. <https://www.aljazeera.com/programmes/peopleandpower/2017/01/interpol-red-alert-170111133954581.html>.

Spiegel Staff. "The US and Israel Stand Alone". Der Spiegel. 15 August 2006. Electronic resource. <https://www.spiegel.de/international/spiegel/spiegel-interview-with-jimmy-carter-the-us-and-israel-stand-alone-a-431793.html>.

Steed, Daniel. "Cyber War, let's get reali(ist)". *War On The Rocks*. 14 October 2013. Internet resource. <https://warontherocks.com/2013/10/cyber-war-lets-get-realist/>.

Steed, Daniel. *The Politics and Technology of Cyberspace.* Routledge. Modern Security Studies. 2019.

Stevenson, Angus. "Social engineering". *Oxford Dictionary of English, 3rd Edition*. Oxford University Press. 2015. Electronic resource:
<https://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/m_en_gb0788050>.

Studenka, John M. "Through the Time Tunnel – Clausewitz On Nuclear Deterrence". National War College; Defense Technical Information Center. 3 October 1990, p. 3; 5-6. Electronic resource. <https://archive.org/details/DTIC_ADA437619>.

Szoldra, Paul. "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks". *Business Insider*. 16 September 2016. Electronic resource. <https://www.businessinsider.com/snowden-leaks-timeline-2016-9>.

Taddonio, Patrice. "CIA Director Nominee Supported Destruction of Torture Tapes". *Frontline.* 9 May 2018. Internet resource. <https://www.pbs.org/wgbh/frontline/article/cia-director-nominee-supported-destruction-of-torture-tapes/>.

Tanaka, Yuki, and Marilyn B. Young (eds.). *Bombing Civilians: A Twentieth-Century History.* The New Press. 2009.

Taylor, A.J.P. *How Wars Begin*. Ebenezer Baylis & Son Ltd. 1979.

Taylor, Vincent F. et al. "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic." *2016 IEEE European Symposium on Security and Privacy (EuroS&P).* 2016. Electronic resource. <https://www.semanticscholar.org/paper/AppScanner%3A-Automatic-Fingerprinting-of-Smartphone-Taylor-Spolaor/fa74491e2138dc65f1f3198c85d7269cbe42d0ab>.

Theohary, Catherine A. *Defense Primer: Information Operations*. Congressional Research Service. 14 January 2020. Electronic resource.
<https://crsreports.congress.gov/product/pdf/IF/IF10771#:~:text=Information%20Warfare&text=Strategy%20can%20be%20defined%20as,is%20information%20operations%20(IO)>.

Thompson, Derek. "The Whole Messy, Ridiculous GameStop Saga in One Sentence". *The Atlantic*. 5 February 2021. Electronic resource. <https://www.theatlantic.com/ideas/archive/2021/01/why-everybody-obsessed-gamestop/617857/>.

Tkacheva, Olesya, et al. “Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt”. *Internet Freedom and Political Space*. RAND Corporation. 2013. Electronic resource. <https://www.jstor.org/stable/10.7249/j.ctt4cgd90.10?refreqid=excelsior%3Aaa3bfe132d8fced1b013ec6b4b9c28ab&seq=1#metadata_info_tab_contents>.

Traugott, Mark. *The Insurgent Barricade*. The Regents of the University California. 2010.

Trials of War Criminals: Before the Nuernberg Military Tribunals under Control Council Law, No. 10. Vol. I, The Medical Case, p. 719-20. U.S. Government Printing Office. 1946-49. Electronic resource. <https://www.loc.gov/rr/frd/Military_Law/pdf/NT_war-criminals_Vol-I.pdf>.

Turse, Nick. “Tomgram: Nick Turse, Tomorrow's Terror Today”. *Tom Dispatch.* 29 May 2018. Internet resource. <https://www.tomdispatch.com/blog/176429/tomgram%3A_nick_turse%2C_tomorrow%27s_terror_today/>.

Ukman, Jason. “U.S. Joint Forces Command formally dissolved”. *The Washington Post.* 4 August 2011. Electronic resource. <https://www.washingtonpost.com/blogs/checkpoint-washington/post/us-joint-forces-command-formally-dissolved/2011/08/04/gIQAQbzBuI_blog.html>.

U.S. Africa Command Public Affairs. “Russia and the Wagner Group continue to be involved in ground, air operations in Libya”. United States Africa Command webpage. 24 July 2020. Internet resource. <https://www.africom.mil/pressrelease/33034/russia-and-the-wagner-group-continue-to-be-in>.

United States Court of Appeals For the First Circuit No. 15-1719 ALEXANDER YERSHOV v. GANNETT SATELLITE INFORMATION NETWORK, INC., USA TODAY. Electronic resource. 9 July 2019. <http://media.ca1.courts.uscourts.gov/pdf.opinions/15-1719P-01A.pdf>.

US-Europe Joint Investigation Team. “Notice of Crimes Against Humanity Using Energy & Neuro/Bio Weapons, Notice of Criminal Trespass, Notice of Theft of Intellectual Property, Notice of Impending Criminal Charges”. *The Everyday Concerned Citizen*. 28 August 2017. Internet resource. <https://everydayconcerned.files.wordpress.com/2017/09/notice-of-crimes-against-humanity.pdf>

“US-developed weapon system may cause global warming: govt”. *The Times of India*. 18 July 2016. Electronic resource. <https://timesofindia.indiatimes.com/city/delhi/US-developed-weapon-system-may-cause-global-warming-govt/articleshow/53266962.cms>.

U.S. Marine Corps. *Small Wars Manual*. Department of the Navy: Headquarters United States Marine Corps. 1940. Reprint 22 December 1990. Electronic resource. <https://www.marines.mil/Portals/1/Publications/FMFRP%2012-15%20%20Small%20Wars%20Manual.pdf>.

U.S. Senate Select Committee on Intelligence. “New Reports Shed Light on Internet Research Agency’s Social Media Tactics”. *Press Release of Intelligence Committee.* 17 December 2018. Internet resource. <https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency’s-social-media-tactics>.

Vanderzielfultz, Victoria. “Conspiracy Theory Trends: Qanon”. *On the Homefront: The HSDL Blog*. Homeland Security Digital Library. 4 August 2020. Internet resource. <https://www.hsdl.org/c/conspiracy-theory-trends-qanon/>.

Vane III, Russell R. “Advances in Hypergame Theory”. *General Dynamics Advanced Information Systems*. 2006. Electronic resource. <http://www.sci.brooklyn.cuny.edu/~parsons/events/gtdt/gtdt06/vane.pdf>.

Vazquez, Lucas. “Barrett Brown in New York: Barrett Brown speaking at a pro-wikileaks and pro-bradley manning press conference”. *YouTube*. 4 April 2011. Internet media. <https://www.youtube.com/watch?v=jZ-j0aRL78k>.

“Venezuela”. *Freedom in the World.* Freedom House. 2012. Electronic resource. <https://freedomhouse.org/report/freedom-world/2012/venezuela>.

The Editors of Encyclopaedia Britannica. “Wael Ghonim: Egyptian Activist and Computer Engineer”. *Encyclopaedia Britannica, Inc.* 19 December 2018. Electronic resource. <https://www.britannica.com/biography/Wael-Ghonim>.

Wainwright, Oliver. “'The worst place on earth': inside Assad's brutal Saydnaya prison Syria’s most notorious jail has been a journalistic blank spot. Now ex-detainees and architects have built an accurate model, using ‘ear-witness’ testimony, of the president’s hellish torture house”. *The Guardian*. 17 August 2016. Electronic resource. <https://www.theguardian.com/artanddesign/2016/aug/18/saydnaya-prison-syria-assad-amnesty-reconstruction>.

Watkins, Jay. Book Review of *Operation Paperclip: The Secret Intelligence Program to Bring Nazi Scientists to America*, by Annie Jacobsen. (Little, Brown & Company, 2014). *Intelligence in Public Literature*, Vol. 58 No. 3. CSI Publications. Center for the Study of Intelligence. 6 October 2014. Electronic resource. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-58-no-3/operation-paperclip-the-secret-intelligence-program-to-bring-nazi-scientists-to-america.html>.

Webb, Whitney. “The Intercept Withheld NSA Doc That May Have Altered Course of Syrian War”. *MPN News*. 30 October 2017. Electronic resource. <https://www.mintpressnews.com/intercept-withheld-nsa-doc-that-may-have-altered-course-of-syria-war/233757/>.

Web Desk. “New mathematical method to help epidemiologists map spread of COVID-19”. *The Week.* 4 June 2020. Electronic resource. <https://www.theweek.in/news/health/2020/06/04/new-mathematical-method-to-help-epidemiologists-map-spread-of-covid-19.html>.

Weber, Max. “Politics as a Vocation”. *From Max Weber: Essays in Sociology*. Oxford University Press. 1958.

Weiner, Tim. “U.S. May Deport Iraqis Who Worked for CIA”. *International Herald Tribune*. 12 March 1998.

Wilford, Hugh. *America’s Great Game: the CIA’s Secret Arabists and the Shaping of the Modern Middle East.* NY: Basic Books, 2013.

Wing, Joel. “Did Saddam Plan The Insurgency In Iraq?” *Musings on Iraq.* 26 February 2011. <https://musingsoniraq.blogspot.com/2011/08/did-saddam-plan-insurgency-in-iraq.html>

Wired Staff. “Your Own Personal Internet”. *Wired Magazine*. 30 June 2006. Electronic resource. <https://www.wired.com/2006/06/your-own-person/>.

Zenko, Micah. “Millennium Challenge: the real story of a corrupted military exercise and its legacy”. *War on the Rocks.* 5 November 2015. Internet resource. <https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/>.

Zheng, Sarah. “Chinese foreign ministry spokesman tweets claim US military brought coronavirus to Wuhan”. *South China Morning Post*. 13 March 2020. Electronic resource. <https://www.scmp.com/news/china/society/article/3075051/chinese-foreign-ministry-spokesman-tweets-claim-us-military>.

From Glasnot to Freedom of Speech: Russian Openness and International Relations, David Wedgwood Benn

The Strange Death of the Soviet Empire, David Pryce-Jones
The Last Empire: the Final Days of the Soviet Union, Serhii Plokhy

Zbigniew Brzezinski, "The Grand Chessboard: American Primacy and Its Geo-strategic Imperatives"

https://www.nato.int/cps/en/natohq/177273.htm 17 Jul. 2020 14:12 NATO's approach to countering disinformation: a focus on COVID-19

Gorbachev's Glasnost: **The Soviet Media in the First Phase of Perestroika** Joseph Gibbs, 1999

JOURNAL ARTICLE
The Spectrum of National Responsibility for Cyberattacks

Jason Healey
The Brown Journal of World Affairs
Vol. 18, No. 1 (FALL / WINTER 2011), pp. 57-70

https://www.wilsoncenter.org/publication/radio-free-europe-and-radio-liberty

Able Archer 83: **The Secret History of the NATO Exercise That Almost Triggered Nuclear War, Nate Jones (2016)**
https://books.google.com/books?id=qNExDQAAQBAJ&dq=weinberger+that+line+is+sometimes+quite+blurred&source=gbs_navlinks_s

https://www.globalresearch.ca/egypt-us-funded-agitators-on-trial-us-democracy-promotion-foreign-funded-sedition/29255?utm_campaign=magnet&utm_source=article_page&utm_medium=related_articles

Investigation into the US Role in the Arab Uprisings, Ahmed Bensaada's 2011

L'Arabesque Americaine (French edition – not available in English yet)
by Ahmed Bensaada

Davey Winder "How Organised is Organised Cybercrime?" Raconteur 17 December 2017
https://www.raconteur.net/risk-management/how-organised-is-organised-cybercrime

Lucas Kello *The Virtual Weapon and International Order, p. 4. Yale University Press (2017)*

Melvin Gutterman *Fourth Amendment Privacy and Standing: Wherever the Twain Shall Meet (1981) ref'd pg. 130 Robert M. Bloom*
Jenkins & klandermans 2005 the politics of social protest pp 2-6 journal article

Protocol politics [electronic resource] : the globalization of Internet governance DeNardis, Laura, 2009

http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=7629918.PN.&OS=PN/7629918&RS=PN/7629918
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=4456912.PN.&OS=PN/4456912&RS=PN/4456912 (two, hardware by civilian contractors, hackers themselves or targets of hackers)

https://thehackernews.com/2015/07/Italian-hacking-team-software.html (paid-for by govt hacking industry)

https://thehackernews.com/2019/08/swapgs-speculative-execution.html (Built-in Intel chip flaw)

Krahmann, Elke. *Private Security Companies and the State Monopoly on Violence: A Case of Norm Change?* Frankfurt am Main: PRIF, 2009. Print.

Leander, Anna. *Conditional Legitimacy, Reinterpreted Monopolies: Globalisation and the Evolving State Monopoly on Legitimate Violence*. Cph: Copenhagen Peace Research Institute, 2002. Print.

Pollack, Norman. *Capitalism, Hegemony and Violence in the Age of Drones*. , 2018. Internet resource.

Kaldor, Mary. *New & Old Wars: Organized Violence in a Global Era*. , 2012. Internet resource.

"From spectacle to spectacular: How physical space, social media and mainstream broadcast amplified the public sphere in Egypt's 'Revolution'". Mohamed Nanabhaya and Roxane Farmanfarmaian. http://www.roxanefarmanfarmaian.com/wp-content/uploads/2012/06/From-Spectacle-to-Spectacular.pdf

Gregg Housh (anonymous activist)

Snowden's "haven" app as RAT

Anais, Seantel. 2013. "Objects of Security/Objects of Research. Analyzing Non-lethal Weapons" pp. 195-198 Research Methods in Critical Security Methods. Routledge. [the designation 'non-lethal' can equate to tools of torture]

The military-entertainment complex

Author:Timothy Lenoir; Luke Caldwell

Publisher: Cambridge, Massachusetts ; London, England : Harvard University Press, [2018]

Davey Winder, “How Organised is Organised Crime?” *Raconteur Special Report: cyber-risk and resilience* 2017

Lucas Kello, *The Virtual Weapon and International Order*. Yale University Press. 2017.

Index