



Espionage: A Spooky Cooperation

Secret Services' hunger for data is enormous. The equipment feeding this appetite is provided by the software industry. This is a mega business for Silicon Valley, but also for IT companies in Europe, such as SAP in Germany and Crypto AG in Switzerland.

The people of Crypto AG are generally considered to be silent, closed and inaccessible. Some would even consider them slightly paranoid. Whenever they surf the Internet, they sit in a glass cage within their office complex in the business district of Steinhausen, Canton of Zug, strictly isolated from other offices and the production lines. Like outlawed smokers, who retire to the smoking lounge during their break.

These days the people at Crypto are no longer ridiculed. Globally among the leading encryption artists, their company is no stranger to the world of intelligence and yet it remains a mystery: no one knows who owns it. Yet demand for companies like Crypto in the secret service domain is higher than ever.

The young intelligence officer Edward Snowden has issued a wakeup call that has turned an uneasy feeling into certainty. With

PowerPoint files stolen from the lowest echelons of the super-intelligence service called the National Security Agency (NSA), Snowden has publicly described their standard eavesdropping and observation practices in words that can be understood by everyone. His revelations have not only shown how the data-grabbing NSA has been growing and how it fishes for communications among governments, businesses and citizens. For the first time ever, the

spotlight has been turned on a young industry that hitherto has received little attention: the espionage business. Along with the growth of the Internet, a relationship between government intelligence agencies and private business has developed that heretofore was only known to exist between the defense industry and the military. It is a relationship similar to the "military industrial complex", which U.S. President Dwight Eisenhower warned could become a threat to democracy in 1961. Now, a silent but rapidly growing intelligence-industry complex has emerged that potential represents a high risk.

Spy money for Start-ups

Innocent observers were astonished to find out that whistleblower Snowden was not employed by the NSA but by the consulting company Booz Allen Hamilton. To the intelligence community this was no surprise. The U.S. intelligence agencies would find it difficult to imagine doing without the services provided by Booz Allen or leading defense contractors such as Boeing, General Dynamics and Siemens. Missile supplier Raytheon currently earns almost as much revenue from their intelligence services as they do from military flying objects.

In the U.S., some 70 percent of the state security budget goes to the espionage industry, whose annual turnover is estimated at 75 billion dollars.

The Internet has become a catalyst for this development and Silicon Valley is its industrial base. In the melting pot of creative computer developers, a strangely open culture has emerged. While 20 years ago service providers, such as the Texas-based E-Systems, which supplied wiretapping devices, took meticulous care to keep their clients secret, the foreign intelligence service CIA sees no problem in

permitting its suppliers to advertise this fact on the Internet.



In 1999, for example, the CIA founded a venture capital fund named In-Q-Tel, which openly declares itself to be a contractual partner promoting start-up businesses that develop useful products. A quote from its website reads: "In-Q-Tel (IQT) was created to bridge the gap between the technology needs of the U.S. Intelligence Community (IC) and emerging commercial innovation." Unlike many secretive actors in the venture capital scene, this CIA fund publishes the names of more than 90 companies in which they have invested. Among these are specialized companies such as A4Vision, headquartered in California (with a branch in Geneva), that develops 3D images for facial recognition. Or Palantir Technologies, a software company well-known in professional circles.

The needle in the haystack

Palantir's products are also being offered to the relevant authorities in Bern. The company, which is located at the former headquarters of Facebook in Palo Alto, employs a well-known former German intelligence officer as its trade representative, and its top management also includes two Germans: the Silicon Valley legend Peter Thiel and Alexander Karp, from Frankfurt, who holds a doctorate in philosophy. Thiel is the founder of PayPal, the online payment service, and is a major investor in the Facebook project. With PayPal, Facebook and Palantir

Thiel amassed a fortune estimated at \$ 1.5 billion. Following law studies at Stanford, the philosopher Karp joined Thiel as CEO and creative spokesperson of Palantir.

After fraudulent users almost drove PayPal into bankruptcy, Thiel and computer scientists from Stanford University, together with several co-investors, developed software to detect abnormal patterns in transactions. An additional investor in the project was a trust domiciled in Vaduz, Principality of Liechtenstein, with a Zurich lawyer as trustee. This project has since become Palantir's major business: analyzing huge collections of unstructured data, detecting abnormalities, discovering trends and relationships and identifying patterns of behavior. In other words: looking for the needle in the haystack.

Palantir's name was inspired by the "seeing stones" in Tolkien's novel "The Lord of the Rings". Palantir's website has been influenced by cool start-up freaks: photos show students in bathing suits and T-shirts, lounging around a conference table. You can follow them on Facebook, Twitter, YouTube and Quora and their company motto suggests a do-gooder initiative: "We are here to solve the toughest problems of the world." Their mission: "To make the world a better place."

Princely accolade

Palantir's products have an excellent reputation and patents are being accorded on a regular basis, such as the latest for managing bulk data within a changing software environment. Then there are analytical tools that allow hedge funds to improve their trading strategies, obviously a useful by-product of the investigative applications. The services Palantir offers to the authorities in their fight against fraud were praised three

years ago by no less a person than U.S. Vice President Joe Biden. A princely accolade: the company doubles its turnover every year. However, Palantir does not release any financial data, nor does the company communicate the number of its employees or any other data. World-wide, it counts many governmental institutions among its customers, including intelligence and investigative agencies, as well as banks and hedge funds. The Palantir people help in the fight against terrorism and in combating financial crimes; they were successful in cyber warfare, unmasking Chinese cyber spies for the U.S. authorities.

There are very tight connections between the company and the government. At its headquarters in Palo Alto, California, Palantir co-founders have launched the Institute for Security & Analysis as a tax-exempt, non-profit organization. The Institute has declared its mission to be the support of the U.S. government in the development of new technologies, helping it to take a leading role in the utilization of Silicon Valley software. However, when software developers were hired to investigate the WikiLeaks revelations, a shit storm broke out across the Internet; bright spark Alex Karp apologized to the Internet community.

In May 2011 the managers of Palantir gained a powerful European ally. Together with SAP, the world's leading company for business software, they are now jointly offering their information analysis application to national security and intelligence services under the name of "SAP Intelligence Analysis for the Public Sector by Palantir". They state that "with this product our customers can gather information efficiently, evaluate it and thus increase public safety." The application supports the authorities in "sovereign security tasks."

Through the Snowden revelations, a more critical light has been shed on such joint ventures as this, in which CIA's service-provider Palantir joins up with SAP, the world's largest supplier of business applications, which processes the data of 248 500 customers in 188 countries. Critics cannot ignore the weekly PowerPoint slides, which Snowden publishes with the help of the American documentary filmmaker Laura Poitras. The slides report how the NSA and CIA access the databases of internet giants such as Facebook, Google and Yahoo, or of telecom companies such as Verizon and AT & T, how they read emails at Internet hubs, spy out credit card transactions, listen in on telephone conversations or decrypt smart phones like BlackBerrys and iPhones, things they sometimes carry out legally, in accordance with secret agreements, at other times using trickery and by-passing American laws.

Controversial «Clouds»

SAP would unquestionably be a desirable goal. Clandestine access to the group would provide U.S. intelligence services insights into a huge economic universe – a nightmare scenario for many companies. "Palantir normally works directly with the client on a project and uses only such data that the customer has submitted to it for the agreed purposes," says a spokesman for SAP: "So far we have not received a request by the NSA to transmit data."

Nonetheless, IT security engineers have been turning up their noses for some time at a trend that SAP and many other IT companies are pushing: cloud storage. Such clouds store customer programs and databases in virtual clouds, huge server farms that are installed somewhere out there. "SAP Cloud" for example is already being used by 30 million SAP customers. "The

Cloud is the most dangerous stupidity of all time," rants an experienced security man. You might as well place your hard disks on the pavement and stick a piece of paper on them with a friendly invitation to 'help yourself'."

**Society for Worldwide Interbank Financial
Telecommunication**



Palantir and SAP, as well as Snowden's ex-employer Booz Allen, are among the top service providers to the intelligence services. However, the range the espionage industry covers is broad and encompasses everything that the services require: encryption and decryption, investigators' databases and visualization software for crime research, pattern recognition, speech recognition, face recognition, network analysis, as well as all sorts of modern hardware, whether for the use of covert espionage or for judicially authorized scanning of computers.

"We live in a golden age of espionage," says the cryptographer Paul Kocher, who has been involved in the encryption technology for the SSL protocol, which is intended to secure e-mail communications. He has had to realize that, with the help of their service providers, the NSA has managed to weaken the SSL key to such an extent that it can filter out any information it desires. The same applies to VPN connections, which many companies use both internally and externally. The NSA spends \$250 million annually for their "Sigint Enabling Project" program, in order to find loopholes to hack encrypted networks. And, if you believe the Snowden revelations, the NSA does not differentiate between friend and

foe, between private and government matters. Whether it is tourist and airline reservation systems, telecom companies or the European monetary transaction network Swift, nothing seems to be safe from the reach of the eavesdroppers. Fundamental trust is being destroyed; a user no longer knows whether he's holding an Apple or an NSA phone in his hand.

The revelations have led to contradictory effects: they both promote the business of the espionage industry and also encourage distrust toward the same industry. "We are at a turning point," says Franz Grüter of Green.ch, a Swiss company that operates large data centers for clients such as Hewlett-Packard, Axpo or North Stream. "People are bound to renew their demand for sovereignty over their data." Users are asking themselves whether encryption still makes sense. Security experts answer that only those users may feel reasonably safe who encrypt their data on their own hardware using robust systems, and then decrypt it at the receiving

end, using only devices that have no connections to the outside world or to the net. Among these are the military encryption devices manufactured by Crypto AG in Zug and supplied to the Swiss Army, as well as to numerous governments and military agencies.

Mysterious owners

But can Crypto AG be trusted? The managers in Steinhausen point out that their devices may not be delivered to the United States. Permission is only given for encryption devices whose encryption algorithm is stored with the U.S. authorities. There is something else, however, which for decades has been keeping Crypto AG a mystery: no one knows who owns Crypto AG. Even the company's managers maintain they don't know who the real owner is. A single board member acts as shareholder representative on behalf of the parent Crypto Group AG and holds the bearer shares through the "European Institute Trading Company" in Liechtenstein.

Only this much is known: The company was registered in 1950 in Vaduz by Crypto-founder Boris Hagelin. Rumors about the identity of the presumed owner have been circulating for decades. Sometimes it is said that it is the German secret service, sometimes Siemens AG, at other times the Americans. Crypto AG has always vehemently denied these rumors, but it has never named its shareholders. Indisputable is the fact during WWII company founder Boris Hagelin supplied the U.S. Army with a legendary cipher machine. He worked on it together with the cryptologist William Friedman, who later became a leading NSA developer. For intelligence historians only one thing is certain: already in the 1950's, the NSA used their large Harvest computer to crack encryption devices. Maybe there is a secret service man sitting in a glass cage in "Crypto City", the headquarters of the NSA at Fort Meade, who knows precisely who owns the Trading Institute in Liechtenstein.