JNS – ISRASWISS

(www.jnews.ch)

Switzerland & USA Connections

Google, AOL, Skype, Facebook, Apple, Hotmail, Skype und Yahoo geben routinemässig Regierungen unsere Internet-Aktivitäten und Passwörter

Nachrichtendienstlicher Austausch mit dem Ausland

Versus

Rechtstaatlichkeit in der Schweiz

The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)

By James Bamford, 03.15.12, 7:24 PM

Photo: Name Withheld; Digital Manipulation: Jesse Lenz

The spring air in the small, sand-dusted town has a soft haze to it, and clumps of green-gray sagebrush rustle in the breeze. Bluffdale sits in a bowl-shaped valley in the shadow of Utah's Wasatch Range to the east and the Oquirrh Mountains to the west. It's the heart of Mormon country, where religious pioneers first arrived more than 160 years ago. They came to escape the rest of the world, to understand the mysterious words sent down from their god as revealed on buried golden plates, and to practice what has become known as "the principle," marriage to multiple wives.

Today Bluffdale is home to one of the nation's largest sects of polygamists, the Apostolic United Brethren, with upwards of 9,000 members. The brethren's complex includes a chapel, a school, a sports field, and an archive. Membership has doubled since 1978—and the number of plural marriages has tripled—so the sect has recently been looking for ways to purchase more land and expand throughout the town. secretly capturing, storing, and analyzing vast quantities of words and images hurtling through the world's telecommunications networks. In the little town of Bluffdale, Big Love and Big Brother have become uneasy neighbors.

The NSA has become the largest, most covert, and potentially most intrusive intelligence agency ever.

Under construction by contractors with top-secret clearances, the blandly named Utah Data Center is being built for the National Security Agency. A project of immense secrecy, it is the final piece in a complex puzzle assembled over the past decade. Its purpose: to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks. The heavily fortified $2 billion center should be up and running in September 2013. Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter." It is, in some measure, the realization of the "total information awareness" program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans' privacy.

But "this is more than just a data center," says one senior intelligence official who until recently was involved with the program. The mammoth Bluffdale center will have another important and far more secret role that until now has gone unrevealed. It is also critical, he says, for breaking codes. And code-breaking is crucial, because much of the data that the center will handle—financial information, stock transactions, business deals, foreign military and diplomatic secrets, legal documents, confidential personal communications—will be heavily encrypted. According to another top official also involved with the program, the NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US. The upshot, according to this official: "Everybody's a target; everybody with communication is a target."

For the NSA, overflowing with tens of billions of dollars in post-9/11 budget awards, the cryptanalysis breakthrough came at a time of explosive growth, in size as well as in power. Established as an arm of the Department of Defense following Pearl Harbor, with the primary purpose of preventing another surprise assault, the NSA suffered a series of humiliations in the post-Cold War years. Caught offguard by an escalating series of terrorist attacks—the first World Trade Center bombing, the blowing up of US embassies in East Africa, the attack on the USS *Cole* in Yemen, and finally the devastation of 9/11—some began questioning the agency's very reason for being. In response, the NSA has quietly been reborn. And while there is little indication that its actual effectiveness has improved—after all, despite numerous pieces of evidence and intelligence-gathering opportunities, it missed the near-disastrous attempted attacks by the underwear bomber on a flight to Detroit in 2009 and by the car bomber in Times Square in 2010—there is no doubt that it has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created.

In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it's all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever.

But new pioneers have quietly begun moving into the area, secretive outsiders who say little and keep to themselves. Like the pious polygamists, they are focused on deciphering cryptic messages

that only they have the power to understand. Just off Beef Hollow Road, less than a mile from brethren headquarters, thousands of hard-hatted construction workers in sweat-soaked T-shirts are laying the groundwork for the newcomers' own temple and archive, a massive complex so large that it necessitated expanding the town's boundaries. Once built, it will be more than five times the size of the US Capitol.

Rather than Bibles, prophets, and worshippers, this temple will be filled with servers, computer intelligence experts, and armed guards. And instead of listening for words flowing down from heaven, these newcomers will be.

UTAH DATA CENTER

When construction is completed in 2013, the heavily fortified $2 billion facility in Bluffdale will encompass 1 million square feet.

1 VISITOR CONTROL CENTER
A $9.7 million facility for ensuring that only cleared personnel gain access.

2 ADMINISTRATION
Designated space for technical support and administrative personnel.

3 DATA HALLS
Four 25,000-square-foot facilities house rows and rows of servers.

4 BACKUP GENERATORS AND FUEL TANKS
Can power the center for at least three days.

5 WATER STORAGE AND PUMPING
Able to pump 1.7 million gallons of liquid per day.

6 CHILLER PLANT
About 60,000 tons of cooling equipment to keep servers from overheating.

7 POWER SUBSTATION
An electrical substation to meet the center's estimated 65-megawatt demand.

8 SECURITY
Video surveillance, intrusion detection, and other protection will cost more than $10 million.

Source: U.S. Army Corps of Engineers Conceptual Site plan

A swath of freezing fog blanketed Salt Lake City on the morning of January 6, 2011, mixing with a weeklong coating of heavy gray smog. Red air alerts, warning people to stay indoors unless absolutely necessary, had become almost daily occurrences, and the temperature was in the bone-chilling twenties. "What I smell and taste is like coal smoke," complained one local blogger that day. At the city's international airport, many inbound flights were delayed or diverted while outbound regional jets were grounded. But among those making it through the icy mist was a figure whose gray suit and tie made him almost disappear into the background. He was tall and thin, with the physique of an aging basketball player and dark caterpillar eyebrows beneath a shock of matching hair. Accompanied by a retinue of bodyguards, the man was NSA deputy director Chris Inglis, the agency's highest-ranking civilian and the person who ran its worldwide day-to-day operations.

A short time later, Inglis arrived in Bluffdale at the site of the future data center, a flat, unpaved runway on a little-used part of Camp Williams, a National Guard training site. There, in a white tent set up for the occasion, Inglis joined Harvey Davis, the agency's associate director for installations and logistics, and Utah senator Orrin Hatch, along with a few generals and politicians in a surreal ceremony. Standing in an odd wooden sandbox and holding gold-painted shovels, they made awkward jabs at the sand and thus officially broke ground on what the local media had simply dubbed "the spy center." Hoping for some details on what was about to be built, reporters turned to one of the invited guests, Lane Beattie of the Salt Lake Chamber of Commerce. Did he have any idea of the purpose behind the new facility in his backyard? "Absolutely not," he said with a self-conscious half laugh. "Nor do I want them spying on me."

For his part, Inglis simply engaged in a bit of double-talk, emphasizing the least threatening aspect of the center: "It's a state-of-the-art facility designed to support the intelligence community in its mission to, in turn, enable and protect the nation's cybersecurity." While cybersecurity will certainly be among the areas focused on in Bluffdale, what is collected, how it's collected, and what is done with the material are far more important issues. Battling hackers makes for a nice cover—it's easy to explain, and who could be against it? Then the reporters turned to Hatch, who proudly described the center as "a great tribute to Utah," then added, "I can't tell you a lot about what they're going to be doing, because it's highly classified."

And then there was this anomaly: Although this was supposedly the official ground-breaking for the nation's largest and most expensive cybersecurity project, no one from the Department of Homeland Security, the agency responsible for protecting civilian networks from cyberattack, spoke from the lectern. In fact, the official who'd originally introduced the data center, at a press conference in Salt Lake City in October 2009, had nothing to do with cybersecurity. It was Glenn A. Gaffney, deputy director of national intelligence for collection, a man who had spent almost his entire career at the CIA. As head of collection for the intelligence community, he managed the country's human and electronic spies.

Within days, the tent and sandbox and gold shovels would be gone and Inglis and the generals would be replaced by some 10,000 construction workers. “We’ve been asked not to talk about the project,” Rob Moore, president of Big-D Construction, one of the three major contractors working on the project, told a local reporter. The plans for the center show an extensive security system: an elaborate $10 million antiterrorism protection program, including a fence designed to stop a 15,000-pound vehicle traveling 50 miles per hour, closed-circuit cameras, a biometric identification system, a vehicle inspection facility, and a visitor-control center.

Inside, the facility will consist of four 25,000-square-foot halls filled with servers, complete with raised floor space for cables and storage. In addition, there will be more than 900,000 square feet for technical support and administration. The entire site will be self-sustaining, with fuel tanks large enough to power the backup generators for three days in an emergency, water storage with the capability of pumping 1.7 million gallons of liquid per day, as well as a sewage system and massive air-conditioning system to keep all those servers cool. Electricity will come from the center’s own substation built by Rocky Mountain Power to satisfy the 65-megawatt power demand. Such a mammoth amount of energy comes with a mammoth price tag—about $40 million a year, according to one estimate.

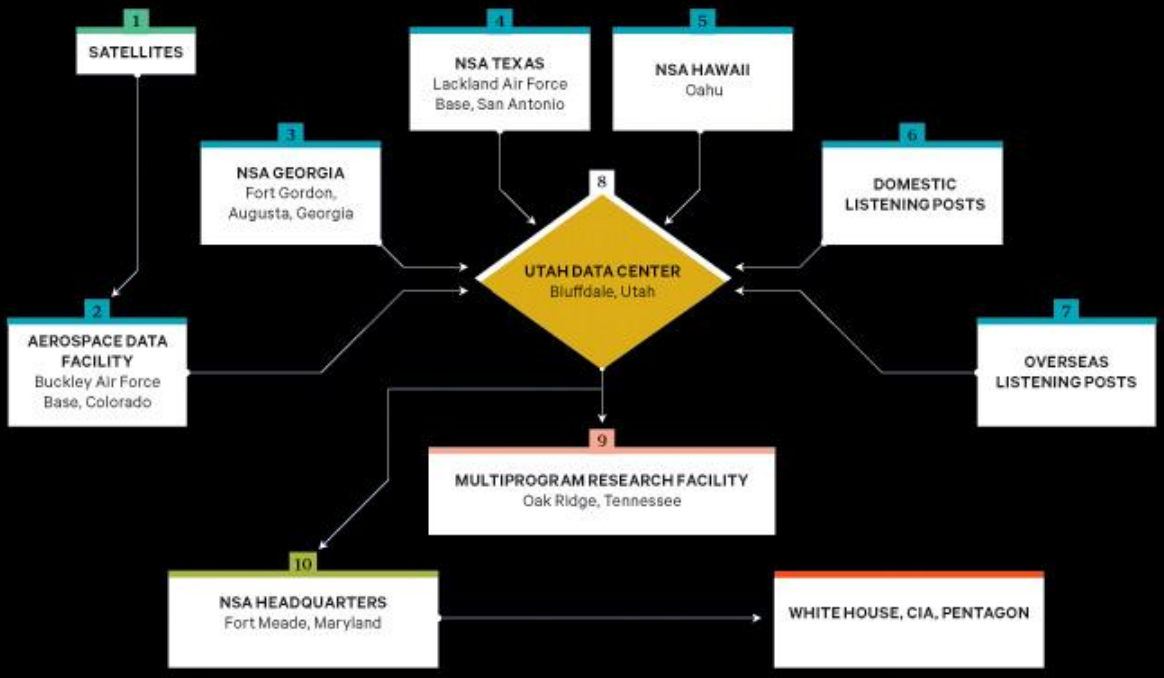
Given the facility’s scale and the fact that a terabyte of data can now be stored on a flash drive the size of a man’s pinky, the potential amount of information that could be housed in Bluffdale is truly staggering. But so is the exponential growth in the amount of intelligence data being produced every day by the eavesdropping sensors of the NSA and other intelligence agencies. As a result of this “expanding array of theater airborne and other sensor networks,” as a 2007 Department of Defense report puts it, the Pentagon is attempting to expand its worldwide communications network, known as the Global Information Grid, to handle yottabytes (10^{24} bytes) of data. (A yottabyte is a septillion bytes—so large that no one has yet coined a term for the next higher magnitude.)

It needs that capacity because, according to a recent report by Cisco, global Internet traffic will quadruple from 2010 to 2015, reaching 966 exabytes per year. (A million exabytes equal a yottabyte.) In terms of scale, Eric Schmidt, Google’s former CEO, once estimated that the total of all human knowledge created from the dawn of man to 2003 totaled 5 exabytes. And the data flow shows no sign of slowing. In 2011 more than 2 billion of the world’s 6.9 billion people were connected to the Internet. By 2015, market research firm IDC estimates, there will be 2.7 billion users. Thus, the NSA’s need for a 1-million-square-foot data storehouse. Should the agency ever fill the Utah center with a yottabyte of information, it would be equal to about 500 quintillion (500,000,000,000,000,000,000) pages of text.

The data stored in Bluffdale will naturally go far beyond the world’s billions of public web pages. The NSA is more interested in the so-called invisible web, also known as the deep web or deepnet—data beyond the reach of the public. This includes password-protected data, US and foreign government communications, and noncommercial file-sharing between trusted peers. “The deep web contains government reports, databases, and other sources of information of high value to DOD and the intelligence community,” according to a 2010 Defense Science Board report. “Alternative tools are needed to find and index data in the deep web … Stealing the classified secrets of a potential adversary is where the [intelligence] community is most comfortable.” With its new Utah Data Center, the NSA will at last have the technical capability to store, and rummage through, all those stolen secrets. The question, of course, is how the agency defines who is, and who is not, “a potential adversary.”

The NSA'S SPY NETWORK

Once it's operational, the Utah Data Center will become, in effect, the NSA's cloud. The center will be fed data collected by the agency's eavesdropping satellites, overseas listening posts, and secret monitoring rooms in telecom facilities throughout the US. All that data will then be accessible to the NSA's code breakers, data-miners, China analysts, counterterrorism specialists, and others working at its Fort Meade headquarters and around the world. Here's how the data center appears to fit into the NSA's global puzzle.—J.B.



1 GEOSTATIONARY SATELLITES

Four satellites positioned around the globe monitor frequencies carrying everything from walkie-talkies and cell phones in Libya to radar systems in North Korea. Onboard software acts as the first filter in the collection process, targeting only key regions, countries, cities, and phone numbers or email.

2 AEROSPACE DATA FACILITY, BUCKLEY AIR FORCE BASE, COLORADO

Intelligence collected from the geostationary satellites, as well as signals from other spacecraft and overseas listening posts, is relayed to this facility outside Denver. About 850 NSA employees track the satellites, transmit target information, and download the intelligence haul.

3 NSA GEORGIA, FORT GORDON, AUGUSTA, GEORGIA

Focuses on intercepts from Europe, the Middle East, and North Africa. Codenamed Sweet Tea, the facility has been massively expanded and now consists of a 604,000-square-foot operations building for up to 4,000 intercept operators, analysts, and other specialists.

4 NSA TEXAS, LACKLAND AIR FORCE BASE, SAN ANTONIO

Focuses on intercepts from Latin America and, since 9/11, the Middle East and Europe. Some 2,000 workers staff the operation. The NSA recently completed a $100 million renovation on a mega-data center here—a backup storage facility for the Utah Data Center.

5 NSA HAWAII, OAHU

Focuses on intercepts from Asia. Built to house an aircraft assembly plant during World War II, the 250,000-square-foot bunker is nicknamed the Hole. Like the other NSA operations centers, it has since been expanded: Its 2,700 employees now do their work aboveground from a new 234,000-square-foot facility.

6 Domestic listening posts

The NSA has long been free to eavesdrop on international satellite communications. But after 9/11, it installed taps in US telecom "switches," gaining access to domestic traffic. An ex-NSA official says there are 10 to 20 such installations.

7 Overseas listening posts

According to a knowledgeable intelligence source, the NSA has installed taps on at least a dozen of the major overseas communications links, each capable of eavesdropping on information passing by at a high data rate.

8 Utah Data Center, Bluffdale, Utah

At a million square feet, this $2 billion digital storage facility outside Salt Lake City will be the centerpiece of the NSA's cloud-based data strategy and essential in its plans for decrypting previously uncrackable documents.

9 Multiprogram Research Facility, Oak Ridge, Tennessee

Some 300 scientists and computer engineers with top security clearance toil away here, building the world's fastest supercomputers and working on cryptanalytic applications and other secret projects.

10 NSA headquarters, Fort Meade, Maryland

Analysts here will access material stored at Bluffdale to prepare reports and recommendations that are sent to policymakers. To handle the increased data load, the NSA is also building an $896 million supercomputer center here.

Before yottabytes of data from the deep web and elsewhere can begin piling up inside the servers of the NSA's new center, they must be collected. To better accomplish that, the agency has undergone the largest building boom in its history, including installing secret electronic monitoring rooms in major US telecom facilities. Controlled by the NSA, these highly secured spaces are where the agency taps into the US communications networks, a practice that came to light during the Bush years but was never acknowledged by the agency. The broad outlines of the so-called warrantless-wiretapping program have long been exposed—how the NSA secretly and illegally bypassed the Foreign Intelligence Surveillance Court, which was supposed to oversee and authorize highly targeted domestic eavesdropping; how the program allowed wholesale monitoring of millions of American phone calls and email. In the wake of the program's exposure, Congress passed the FISA Amendments Act of 2008, which largely made the practices legal. Telecoms that had agreed to participate in the illegal activity were granted immunity from prosecution and lawsuits. What wasn't revealed until now, however, was the enormity of this ongoing domestic spying program.

For the first time, a former NSA official has gone on the record to describe the program, codenamed Stellar Wind, in detail. William Binney was a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network. A tall man with strands of black hair across the front of his scalp and dark, determined eyes behind thick-rimmed glasses, the 68-year-old spent nearly four decades breaking codes and finding new ways to channel billions of private phone calls and email messages from around the world into the NSA's bulging databases. As chief and one of the two cofounders of the agency's Signals Intelligence Automation Research Center, Binney and his team designed much of the infrastructure that's still likely used to intercept international and foreign communications.

He explains that the agency could have installed its tapping gear at the nation's cable landing stations—the more than two dozen sites on the periphery of the US where fiber-optic cables come ashore. If it had taken that route, the NSA would have been able to limit its eavesdropping to just international communications, which at the time was all that was allowed under US law. Instead it chose to put the wiretapping rooms at key junction points throughout the country—large, windowless buildings known as switches—thus gaining access to not just international communications but also to most of the domestic traffic flowing through the US. The network of intercept stations goes far beyond the single room in an AT&T building in San Francisco exposed by a whistle-blower in 2006. "I think there's 10 to 20 of them," Binney says. "That's not just San Francisco; they have them in the middle of the country and also on the East Coast."

The eavesdropping on Americans doesn't stop at the telecom switches. To capture satellite communications in and out of the US, the agency also monitors AT&T's powerful earth stations, satellite receivers in locations that include Roaring Creek and Salt Creek. Tucked away on a back road in rural Catawissa, Pennsylvania, Roaring Creek's three 105-foot dishes handle much of the country's communications to and from Europe and the Middle East. And on an isolated stretch of land in remote Arbuckle, California, three similar dishes at the company's Salt Creek station service the Pacific Rim and Asia.

The former NSA official held his thumb and forefinger close together: "We are that far from a turnkey totalitarian state."

Binney left the NSA in late 2001, shortly after the agency launched its warrantless-wiretapping program. "They violated the Constitution setting it up," he says bluntly. "But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn't stay." Binney says Stellar Wind was far larger than has been publicly disclosed and included not just eavesdropping on domestic phone calls but the inspection of domestic email. At the outset the program recorded 320 million calls a day, he says, which represented about 73 to 80 percent of the total volume of the agency's worldwide intercepts. The haul only grew from there. According to Binney—who has maintained close contact with agency employees until a few years ago—the taps in the secret rooms dotting the country are actually powered by highly sophisticated software programs that conduct "deep packet inspection," examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light.

The software, created by a company called Narus that's now part of Boeing, is controlled remotely from NSA headquarters at Fort Meade in Maryland and searches US sources for target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases in email. Any communication that arouses suspicion, especially those to or from the million or so people on agency watch lists, are automatically copied or recorded and then transmitted to the NSA.

The scope of surveillance expands from there, Binney says. Once a name is entered into the Narus database, all phone calls and other communications to and from that person are automatically routed to the NSA's recorders. "Anybody you want, route to a recorder," Binney says. "If your number's in there? Routed and gets recorded." He adds, "The Narus device allows you to take it all." And when Bluffdale is completed, whatever is collected will be routed there for storage and analysis.

According to Binney, one of the deepest secrets of the Stellar Wind program—again, never confirmed until now—was that the NSA gained warrantless access to AT&T's vast trove of

domestic and international billing records, detailed information about who called whom in the US and around the world. As of 2007, AT&T had more than 2.8 trillion records housed in a database at its Florham Park, New Jersey, complex.

Verizon was also part of the program, Binney says, and that greatly expanded the volume of calls subject to the agency's domestic eavesdropping. "That multiplies the call rate by at least a factor of five," he says. "So you're over a billion and a half calls a day." (Spokespeople for Verizon and AT&T said their companies would not comment on matters of national security.)

After he left the NSA, Binney suggested a system for monitoring people's communications according to how closely they are connected to an initial target. The further away from the target—say you're just an acquaintance of a friend of the target—the less the surveillance. But the agency rejected the idea, and, given the massive new storage facility in Utah, Binney suspects that it now simply collects everything. "The whole idea was, how do you manage 20 terabytes of intercept a minute?" he says. "The way we proposed was to distinguish between things you want and things you don't want." Instead, he adds, "they're storing everything they gather." And the agency is gathering as much as it can.

Once the communications are intercepted and stored, the data-mining begins. "You can watch everybody all the time with data- mining," Binney says. Everything a person does becomes charted on a graph, "financial transactions or travel or anything," he says. Thus, as data like bookstore receipts, bank statements, and commuter toll records flow in, the NSA is able to paint a more and more detailed picture of someone's life.

The NSA also has the ability to eavesdrop on phone calls directly and in real time. According to Adrienne J. Kinne, who worked both before and after 9/11 as a voice interceptor at the NSA facility in Georgia, in the wake of the World Trade Center attacks "basically all rules were thrown out the window, and they would use any excuse to justify a waiver to spy on Americans." Even journalists calling home from overseas were included. "A lot of time you could tell they were calling their families," she says, "incredibly intimate, personal conversations." Kinne found the act of eavesdropping on innocent fellow citizens personally distressing. "It's almost like going through and finding somebody's diary," she says.

In secret listening rooms nationwide, NSA software examines every email, phone call, and tweet as they zip by.

But there is, of course, reason for anyone to be distressed about the practice. Once the door is open for the government to spy on US citizens, there are often great temptations to abuse that power for political purposes, as when Richard Nixon eavesdropped on his political enemies during Watergate and ordered the NSA to spy on antiwar protesters. Those and other abuses prompted Congress to enact prohibitions in the mid-1970s against domestic spying.

Before he gave up and left the NSA, Binney tried to persuade officials to create a more targeted system that could be authorized by a court. At the time, the agency had 72 hours to obtain a legal warrant, and Binney devised a method to computerize the system. "I had proposed that we automate the process of requesting a warrant and automate approval so we could manage a couple of million intercepts a day, rather than subvert the whole process." But such a system would have required close coordination with the courts, and NSA officials weren't interested in that, Binney says. Instead they continued to haul in data on a grand scale. Asked how many communications—"transactions," in NSA's lingo—the agency has intercepted since 9/11, Binney estimates the number at "between 15 and 20 trillion, the aggregate over 11 years."

When Barack Obama took office, Binney hoped the new administration might be open to reforming the program to address his constitutional concerns. He and another former senior NSA analyst, J. Kirk Wiebe, tried to bring the idea of an automated warrant-approval system to the attention of the Department of Justice's inspector general. They were given the brush-off. "They said, oh, OK, we can't comment," Binney says.

Sitting in a restaurant not far from NSA headquarters, the place where he spent nearly 40 years of his life, Binney held his thumb and forefinger close together. "We are, like, that far from a turnkey totalitarian state," he says.

There is still one technology preventing untrammeled government access to private digital data: strong encryption. Anyone—from terrorists and weapons dealers to corporations, financial institutions, and ordinary email senders—can use it to seal their messages, plans, photos, and documents in hardened data shells. For years, one of the hardest shells has been the Advanced Encryption Standard, one of several algorithms used by much of the world to encrypt data. Available in three different strengths—128 bits, 192 bits, and 256 bits—it's incorporated in most commercial email programs and web browsers and is considered so strong that the NSA has even approved its use for top-secret US government communications. Most experts say that a so-called brute-force computer attack on the algorithm—trying one combination after another to unlock the encryption—would likely take longer than the age of the universe. For a 128-bit cipher, the number of trial-and-error attempts would be 340 undecillion (10^{36}).

Breaking into those complex mathematical shells like the AES is one of the key reasons for the construction going on in Bluffdale. That kind of cryptanalysis requires two major ingredients: super-fast computers to conduct brute-force attacks on encrypted messages and a massive number of those messages for the computers to analyze. The more messages from a given target, the more likely it is for the computers to detect telltale patterns, and Bluffdale will be able to hold a great many messages. "We questioned it one time," says another source, a senior intelligence manager who was also involved with the planning. "Why were we building this NSA facility? And, boy, they rolled out all the old guys—the crypto guys." According to the official, these experts told then-director of national intelligence Dennis Blair, "You've got to build this thing because we just don't have the capability of doing the code-breaking." It was a candid admission. In the long war between the code breakers and the code makers—the tens of thousands of cryptographers in the worldwide computer security industry—the code breakers were admitting defeat.

So the agency had one major ingredient—a massive data storage facility—under way. Meanwhile, across the country in Tennessee, the government was working in utmost secrecy on the other vital element: the most powerful computer the world has ever known.

The plan was launched in 2004 as a modern-day Manhattan Project. Dubbed the High Productivity Computing Systems program, its goal was to advance computer speed a thousandfold, creating a machine that could execute a quadrillion (10^{15}) operations a second, known as a petaflop—the computer equivalent of breaking the land speed record. And as with the Manhattan Project, the venue chosen for the supercomputing program was the town of Oak Ridge in eastern Tennessee, a rural area where sharp ridges give way to low, scattered hills, and the southwestward-flowing Clinch River bends sharply to the southeast. About 25 miles from Knoxville, it is the "secret city" where uranium- 235 was extracted for the first atomic bomb. A sign near the exit read: WHAT YOU SEE HERE, WHAT YOU DO HERE, WHAT YOU HEAR HERE, WHEN YOU LEAVE HERE, LET IT STAY HERE. Today, not far from where that sign stood, Oak Ridge is home to the Department of Energy's Oak Ridge National Laboratory, and it's engaged in a new secret war. But

this time, instead of a bomb of almost unimaginable power, the weapon is a computer of almost unimaginable speed.

In 2004, as part of the supercomputing program, the Department of Energy established its Oak Ridge Leadership Computing Facility for multiple agencies to join forces on the project. But in reality there would be two tracks, one unclassified, in which all of the scientific work would be public, and another top-secret, in which the NSA could pursue its own computer covertly. “For our purposes, they had to create a separate facility,” says a former senior NSA computer expert who worked on the project and is still associated with the agency. (He is one of three sources who described the program.) It was an expensive undertaking, but one the NSA was desperate to launch.

Known as the Multiprogram Research Facility, or Building 5300, the $41 million, five-story, 214,000-square-foot structure was built on a plot of land on the lab’s East Campus and completed in 2006. Behind the brick walls and green-tinted windows, 318 scientists, computer engineers, and other staff work in secret on the cryptanalytic applications of high-speed computing and other classified projects. The supercomputer center was named in honor of George R. Cotter, the NSA’s now-retired chief scientist and head of its information technology program. Not that you’d know it. “There’s no sign on the door,” says the ex-NSA computer expert.

At the DOE’s unclassified center at Oak Ridge, work progressed at a furious pace, although it was a one-way street when it came to cooperation with the closemouthed people in Building 5300. Nevertheless, the unclassified team had its Cray XT4 supercomputer upgraded to a warehouse-sized XT5. Named Jaguar for its speed, it clocked in at 1.75 petaflops, officially becoming the world’s fastest computer in 2009.

Meanwhile, over in Building 5300, the NSA succeeded in building an even faster supercomputer. “They made a big breakthrough,” says another former senior intelligence official, who helped oversee the program. The NSA’s machine was likely similar to the unclassified Jaguar, but it was much faster out of the gate, modified specifically for cryptanalysis and targeted against one or more specific algorithms, like the AES. In other words, they were moving from the research and development phase to actually attacking extremely difficult encryption systems. The code-breaking effort was up and running.

The breakthrough was enormous, says the former official, and soon afterward the agency pulled the shade down tight on the project, even within the intelligence community and Congress. “Only the chairman and vice chairman and the two staff directors of each intelligence committee were told about it,” he says. The reason? “They were thinking that this computing breakthrough was going to give them the ability to crack current public encryption.”

In addition to giving the NSA access to a tremendous amount of Americans’ personal data, such an advance would also open a window on a trove of foreign secrets. While today most sensitive communications use the strongest encryption, much of the older data stored by the NSA, including a great deal of what will be transferred to Bluffdale once the center is complete, is encrypted with more vulnerable ciphers. “Remember,” says the former intelligence official, “a lot of foreign government stuff we’ve never been able to break is 128 or less. Break all that and you’ll find out a lot more of what you didn’t know—stuff we’ve already stored—so there’s an enormous amount of information still in there.”

The NSA believes it’s on the verge of breaking a key encryption algorithm—opening up hoards of data.

That, he notes, is where the value of Bluffdale, and its mountains of long-stored data, will come in. What can't be broken today may be broken tomorrow. "Then you can see what they were saying in the past," he says. "By extrapolating the way they did business, it gives us an indication of how they may do things now." The danger, the former official says, is that it's not only foreign government information that is locked in weaker algorithms, it's also a great deal of personal domestic communications, such as Americans' email intercepted by the NSA in the past decade.

But first the supercomputer must break the encryption, and to do that, speed is everything. The faster the computer, the faster it can break codes. The Data Encryption Standard, the 56-bit predecessor to the AES, debuted in 1976 and lasted about 25 years. The AES made its first appearance in 2001 and is expected to remain strong and durable for at least a decade. But if the NSA has secretly built a computer that is considerably faster than machines in the unclassified arena, then the agency has a chance of breaking the AES in a much shorter time. And with Bluffdale in operation, the NSA will have the luxury of storing an ever-expanding archive of intercepts until that breakthrough comes along.

But despite its progress, the agency has not finished building at Oak Ridge, nor is it satisfied with breaking the petaflop barrier. Its next goal is to reach exaflop speed, one quintillion (10^{18}) operations a second, and eventually zettaflop (10^{21}) and yottaflop.

These goals have considerable support in Congress. Last November a bipartisan group of 24 senators sent a letter to President Obama urging him to approve continued funding through 2013 for the Department of Energy's exascale computing initiative (the NSA's budget requests are classified). They cited the necessity to keep up with and surpass China and Japan. "The race is on to develop exascale computing capabilities," the senators noted. The reason was clear: By late 2011 the Jaguar (now with a peak speed of 2.33 petaflops) ranked third behind Japan's "K Computer," with an impressive 10.51 petaflops, and the Chinese Tianhe-1A system, with 2.57 petaflops.

But the real competition will take place in the classified realm. To secretly develop the new exaflop (or higher) machine by 2018, the NSA has proposed constructing two connecting buildings, totaling 260,000 square feet, near its current facility on the East Campus of Oak Ridge. Called the Multiprogram Computational Data Center, the buildings will be low and wide like giant warehouses, a design necessary for the dozens of computer cabinets that will compose an exaflop-scale machine, possibly arranged in a cluster to minimize the distance between circuits. According to a presentation delivered to DOE employees in 2009, it will be an "unassuming facility with limited view from roads," in keeping with the NSA's desire for secrecy. And it will have an extraordinary appetite for electricity, eventually using about 200 megawatts, enough to power 200,000 homes. The computer will also produce a gargantuan amount of heat, requiring 60,000 tons of cooling equipment, the same amount that was needed to serve both of the World Trade Center towers.

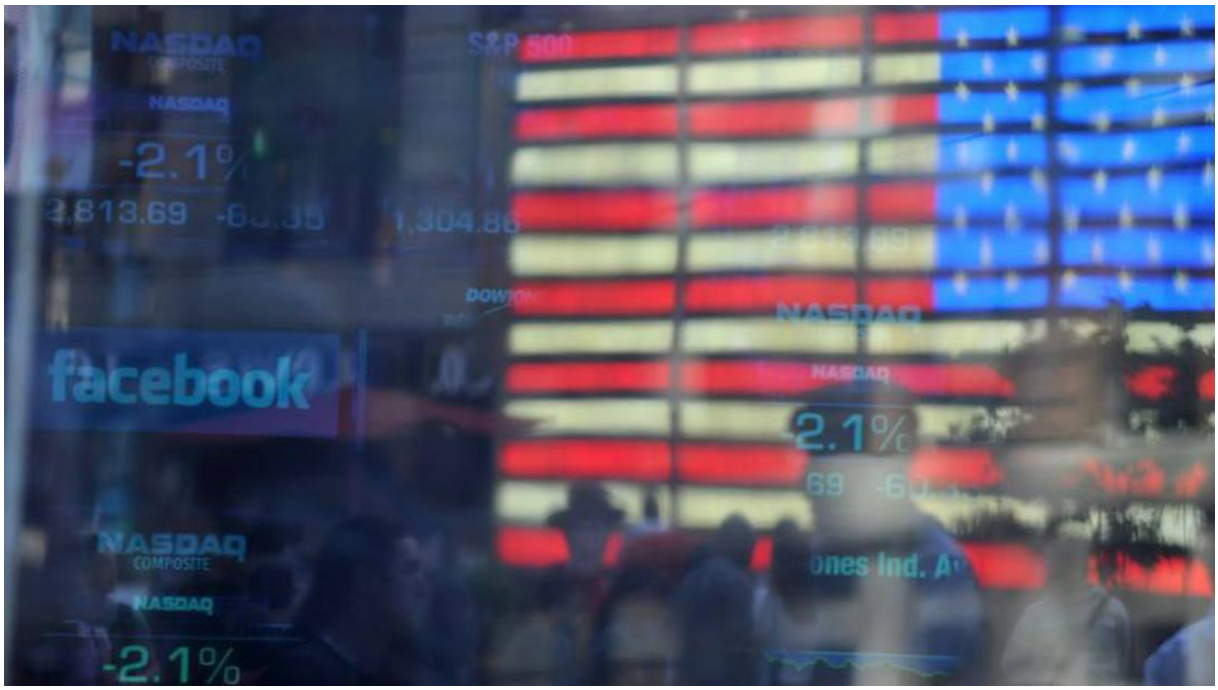
In the meantime Cray is working on the next step for the NSA, funded in part by a $250 million contract with the Defense Advanced Research Projects Agency. It's a massively parallel supercomputer called Cascade, a prototype of which is due at the end of 2012. Its development will run largely in parallel with the unclassified effort for the DOE and other partner agencies. That project, due in 2013, will upgrade the Jaguar XT5 into an XK6, codenamed Titan, upping its speed to 10 to 20 petaflops.

Yottabytes and exaflops, septillions and undecillions—the race for computing speed and data storage goes on. In his 1941 story "The Library of Babel," Jorge Luis Borges imagined a collection

of information where the entire world's knowledge is stored but barely a single word is understood. In Bluffdale the NSA is constructing a library on a scale that even Borges might not have contemplated. And to hear the masters of the agency tell it, it's only a matter of time until every word is illuminated.

James Bamford (washwriter@gmail.com) is the author of *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.*

Die geheimen Mächte im Internet



Hinter vielen grossen Playern im Netz steht der US-Geheimdienst CIA. Gemeinsam mit dubiosen Investoren haben es die Spione geschafft, das grösste soziale Netzwerk der Welt zu unterwandern

Geheimdienste, Investoren, Regierungen: Viele Strippenzieher hinter Facebook, PayPal & Co. bleiben lieber im Verborgenen. CHIP bringt Licht ins Dunkel. Fast eine Milliarde Menschen posten bei Facebook mittlerweile, wen sie kennen, was ihnen gefällt, was sie gerne tun, welche Pläne sie für die Zukunft haben und was sie über aktuelle Entwicklungen in Politik und Gesellschaft denken. Das ist ein Siebtel der Menschheit. Facebook besitzt also die grösste Ansammlung privater Daten aller Zeiten – und jeder Nutzer gibt diese Daten freiwillig her. Vielen dürfte inzwischen bewusst sein, dass dies der eigentliche Preis ist, den sie für das soziale Netzwerk und andere Dienste im Netz bezahlen. Und solange Firmen wie Facebook und Google die exklusiven Informationen nur dazu nutzen, individuell zugeschnittene Werbung zu produzieren, scheint dies für viele Nutzer ein angemessener Preis zu sein.

Doch was, wenn es nicht bei Werbung bliebe? Was, wenn die Facebook-Daten in die falschen Hände gerieten? Zum Beispiel in die Hände staatlicher Einrichtungen und Sicherheitsbehörden. Würden die meisten Menschen einem Geheimdienst genauso freiwillig über ihr Privatleben berichten, wie sie es gegenüber Facebook und Google tun? Wohl kaum. Doch genau das geschieht bereits.

Die Facebook-CIA-Connection

Im April 2006, da war Facebook noch nicht mal zwei Jahre alt, erhielt das Netzwerk eine Finanzspritze in Höhe von rund 27 Millionen US-Dollar. Unter den Geldgebern war damals auch die Investmentfirma Greylock Partners, die bis heute zu den Top-10-Aktionären von Facebook gehört. Die Greylock Partners sind einflussreiche Geldgeber im Silicon Valley: Neben Facebook haben sie unter anderem in LinkedIn, Instagram und Dropbox investiert.

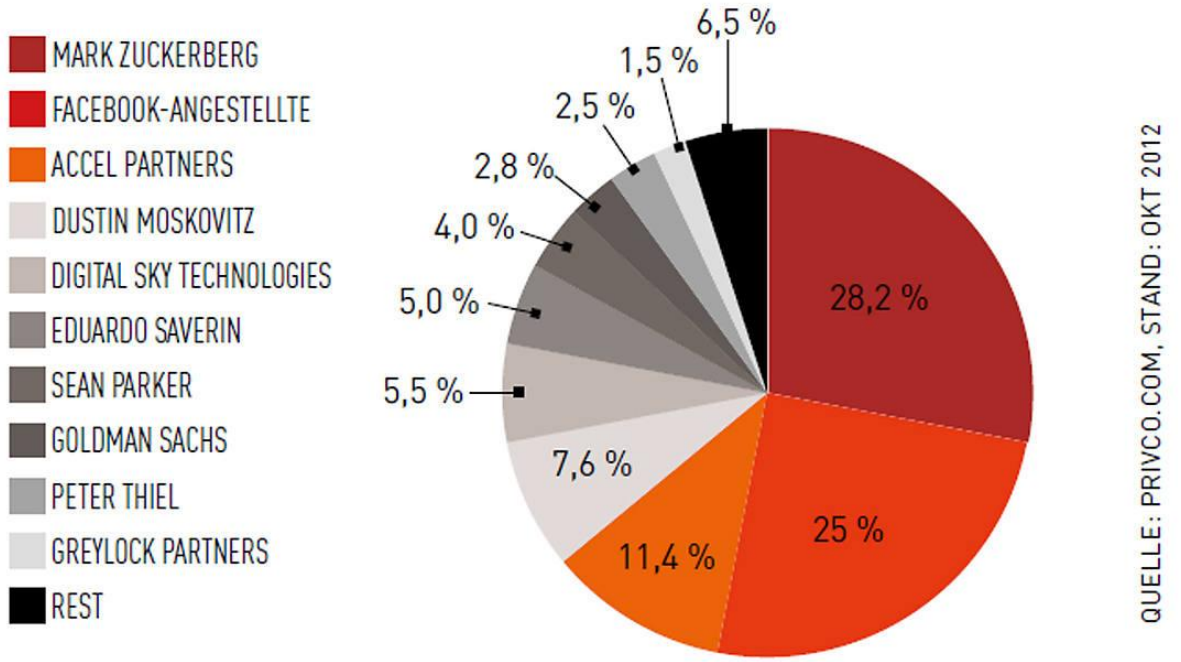
Einer der erfahrensten Mitarbeiter bei Greylock ist Howard E. Cox. Er ist dort bereits seit über 40 Jahren im Geschäft. Seine langjährige Tätigkeit als Investor macht ihn zu einem alten Hasen im Business. Allein bei Greylock hatte er in den letzten vier Jahrzehnten mehrere Aufsichtsratsposten inne. Cox mag zwar schon etwas in die Jahre gekommen sein, untätig ist er deshalb aber nicht: Heute arbeitet er als beratender Partner bei Greylock.

Beste Beziehungen in die Politik

Cox war jedoch nie einfach nur Investor. Auch in die Politik hat er beste Beziehungen: Bevor er zu Greylock kam, arbeitete Cox im Büro des US-Verteidigungsministers und sass darüber hinaus bis 2009 im Business Board des Pentagon. Auch heute hat Cox mehrere Jobs: Neben seiner Tätigkeit bei Greylock ist er Mitglied im Direktorium von In-Q-Tel, einer Firma, die in Technologie-Start-ups investiert. Im Portfolio von In-Q-Tel finden sich junge, zumeist unbekannte Unternehmen wie Biomatrica, Recorded Future oder T2 Biosystems.

Neben den vielsagenden Namen und demselben Investor verbindet diese Firmen vor allem eines: die Art ihrer Produkte. Sie alle stellen Technologien her, die der US-Geheimdienst für nützlich hält. Denn In-Q-Tel wurde von der CIA gegründet und agiert heute als ihr Investment-Arm.

Über In-QTel betreiben die Geheimdienstler Outsourcing von Forschungsarbeit. Geschickte Investitionen erlauben es der CIA, mit der rapiden technologischen Entwicklung mitzuhalten, ohne selbst eine Armada von Wissenschaftlern beschäftigen zu müssen. Ein prominentes Beispiel dafür, welche Art von Technologie die CIA über In-Q-Tel fördert, ist Google Earth. Die Software hinter dem Kartendienst wurde von der Firma Keyhole programmiert, die vor der Übernahme durch Google von In-Q-Tel finanziert wurde. Durch den Verkauf an die Suchmaschine besass die CIA-Firma eine Zeit lang Google-Aktien im Wert von über 2,2 Millionen US-Dollar.



Wer besitzt Facebook? Auf diese Frage lautet die Antwort meistens: Mark Zuckerberg. Doch im Hintergrund gibt es viele weitere Parteien, die bei der Führung von Facebook ein Wörtchen mitzureden haben

Bei der Facebook-CIA-Connection gibt es zwar keine direkte finanzielle Verbindung wie zwischen In-Q-Tel und Google, doch es existiert eine personelle Brücke, die das soziale Netzwerk mit dem Geheimdienst verbindet: Howard E. Cox. Er sitzt an einem strategisch wichtigen Punkt. Denn die CIA hat ein grosses Interesse an den Daten der Facebook-Nutzer – und daraus machen die Geheimdienstler auch gar kein Geheimnis. In einer In-Q-Tel-Broschüre heisst es: „Die Überwachung von sozialen Medien wird für Regierungen zunehmend zu einem essenziellen Bestandteil, wenn es darum geht, aufkeimende politische Bewegungen im Auge zu behalten."

Das heisst im Klartext: Westliche Regierungen wollen sich nicht von einer Facebook-Revolution wie dem Arabischen Frühling überraschen lassen. Denn dabei spielten soziale Netzwerke eine ebenso zentrale Rolle wie bei der antikapitalistischen Protestbewegung Occupy. Um Strömungen wie Occupy auch effektiv überwachen zu können, braucht es jedoch noch eine zweite Komponente – Software, mit der sich riesige Datenmengen wie die von Facebook gezielt verknüpfen und visualisieren lassen.

Strategische Investitionen

Auch hierfür hat die CIA bereits eine strategische Investition getätigt: Palantir Technologies, eine weitere Firma, die von In-Q-Tel mit Geld versorgt wird, stellt so eine Software her. In einem Werbevideo zeigt Palantir anhand eines fiktiven Lebensmittelskandals, was die Software kann: Mit ihr lassen sich unzählige Daten wie Lieferscheine, Kundenlisten, Kreditkarteninformationen sowie Krankenakten aus Kliniken zusammenführen und auswerten.

Die Seuche kann so schnell zu ihrem Ursprung zurückverfolgt und eine weitere Ausbreitung verhindert werden. Ein Muster, das sich auch auf Protestbewegungen übertragen lässt.

Die mächtigen Freunde des Mark Z.

Der Firmensitz von Palantir in Palo Alto ist gerade mal zehn Autominuten von der Facebook-Zentrale entfernt – lediglich der Campus der Stanford University trennt die beiden Gebäude voneinander. Doch nicht nur räumlich sind die Firmen nah beieinander.

Noch stärker ist die Verbindung durch eine Person, bei der im Silicon Valley viele Fäden zusammenlaufen: Peter Thiel. Der in Frankfurt am Main geborene Investor ist nicht nur Hauptgeldgeber und Vorstandsvorsitzender von Palantir, sondern auch Mitglied im Vorstand von Facebook. Er war 2004 einer der Ersten, der das gerade gegründete Unternehmen von Mark Zuckerberg mit Geld versorgte. Gerade einmal zwei Monate nach Gründung des sozialen Netzwerks bekam es von Thiel eine halbe Million US-Dollar.

Heute ist dieser eine der wenigen Einzelpersonen unter den wichtigsten Facebook-Aktionären. Thiels Einfluss im Silicon Valley reicht weit über den Facebook-Vorstand hinaus. Über seine Investmentfirma Founders Fund verhalf er Spotify zu einer Startfinanzierung von 11,6 Millionen Euro.

Das Unternehmen ist heute einer der weltweit führenden Musikstreaming-Anbieter. Der erste grosse Coup gelang Thiel jedoch ein paar Jahre vor dem Einstieg bei Spotify: Im Jahr 1998 gründete er mit einigen seiner Stanford-Kommilitonen den Online-Bezahldienst PayPal. Nach dem Verkauf an eBay im Jahr 2002 verliessen die meisten PayPal-Gründungsmitglieder das Unternehmen.

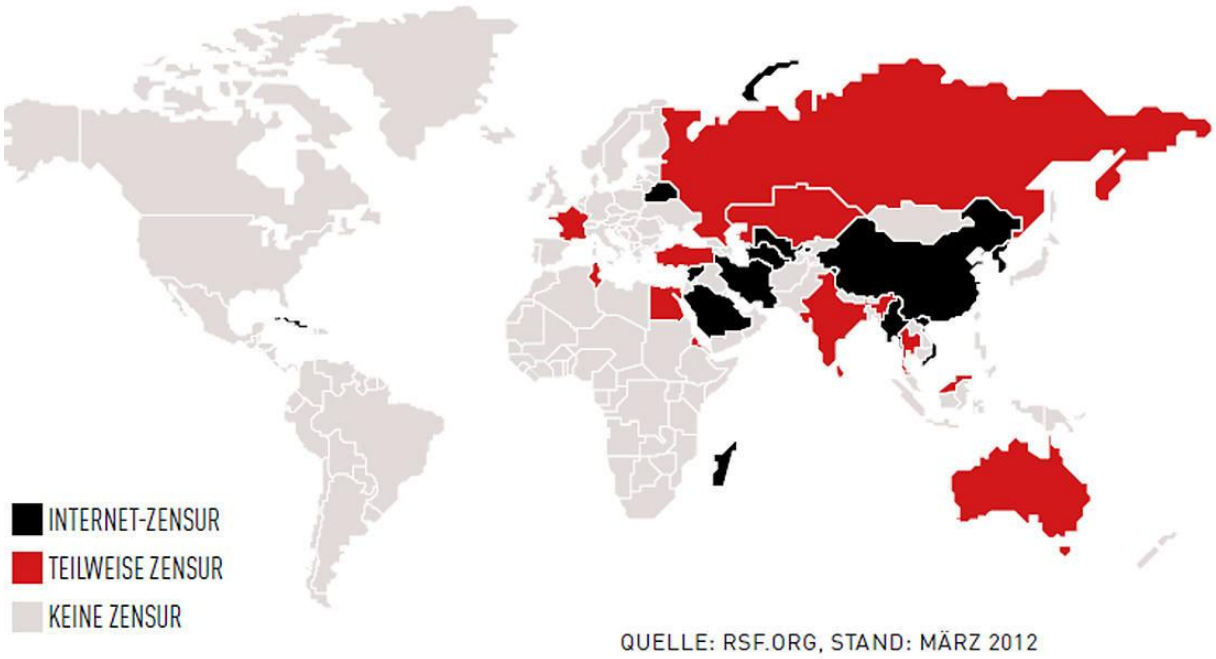
Die „PayPal-Mafia"

Mit den Erlösen aus dem eBay-Deal begannen sie damit, ein eng verzahntes Firmengeflecht aufzubauen, das sie mit gegenseitigen Finanzierungen stützten. Diese Gründungstätigkeit brachte ihnen im Silicon Valley den Namen „PayPal-Mafia" ein, ein Name, dem das Fortune Magazine

2007 mit einem Artikel zu grösserer Bekanntheit verhalf. Eines der Mitglieder in der „PayPal-Mafia“ – Reid Hoffman – ist heute bei Greylock Partners tätig, ebenso wie CIA-Investor Howard E. Cox.

Die „PayPal-Mafia“ ist jedoch nicht die zwielichtigste Vereinigung, der Peter Thiel angehört. Er ist auch Mitglied im Lenkungsausschuss der Bilderberg-Gruppe. Dieser Versammlung gehören hochrangige Vertreter aus Wirtschaft, Politik, Forschung und Medien an, die sich einmal im Jahr unter höchster Geheimhaltungsstufe in einem Luxushotel treffen, um die wichtigsten Probleme der Welt zu besprechen.

Die Gästeliste, eines der wenigen öffentlichen Dokumente der Gruppe, offenbart, dass sich Thiels Verbindungen auch bei den Bilderbergern widerspiegeln: So waren 2012 Persönlichkeiten wie „PayPal-Mafia“-Mitglied und LinkedIn-Mitgründer Reid Hoffman von Greylock Partners, Alexander Karp, der CEO von Thiels Unternehmen Palantir, und Googles Aufsichtsratsvorsitzender Eric Schmidt geladen.



Weltweite Zensur im Netz Jährlich gibt die Organisation Reporter ohne Grenzen eine Liste der „Feinde des Internets“ heraus. Die aktuelle Ausgabe zeigt, wo besonders stark in die freie Meinungsäusserung im Netz eingegriffen wird

Das starke Interesse am Internetverhalten seiner Bürger ist kein US-amerikanisches Phänomen. Auch in Deutschland kontrolliert der Staat, was seine Bürger im Netz anstellen. Hiesige Strafverfolgungsbehörden und auch der Bundesnachrichtendienst haben direkten Zugriff auf den Datenverkehr der Internetserviceprovider (ISPs) wie Telekom, Vodafone und 1&1. Dass kaum jemand darüber Bescheid weiss, hat seinen Grund: Die Telekommunikations-Überwachungsverordnung (TKÜV) verbietet Providern ausdrücklich, mit Unbefugten über die Umsetzung der Überwachungsverordnung zu sprechen.

Sie verpflichtet die Provider, dauerhafte Schnittstellen in ihre Server-Infrastruktur einzubauen, auf die die Strafverfolgungsbehörden bei entsprechendem Verdacht und mit richterlicher

Genehmigung zugreifen können. Das Abgreifen der Daten nehmen die Mitarbeiter der Behörden vor Ort in den Rechenzentren vor, und zwar an sogenannten „Horchposten“. Diese grauen Kästen sind Serverschränke, die mit Schlössern vor dem Zugriff Unbefugter abgeschottet werden.

„Ein paar Mal im Monat kommt jemand mit einer richterlichen Genehmigung und einem Laptop und zapft Daten ab“, verriet ein Provider CHIP hinter vorgehaltener Hand. So wurden 2010 rund 37 Millionen Mails vom Bundesnachrichtendienst herausgefiltert, die eines oder mehrere Signalwörter enthielten.

Ist das freie Internet in Gefahr?
Während die staatliche Kontrolle des Webs in den USA und Deutschland über geschickte Investitionen und nationale Gesetzgebung realisiert wird, wollen repressive Regierungen in Russland, China und im Iran einen Schritt weitergehen: Sie möchten das Netz komplett unter staatliche Aufsicht stellen – weltweit.

„Die Zahl der Regierungen, die das Internet zensieren, ist seit 2002 von vier auf 40 gestiegen. Und diese Zahl wächst ständig weiter an“, schrieb Vint Cerf, einer der Väter des Internets, im Mai 2012 in der New York Times. Ihr Vorhaben wollen die treibenden Staaten mit einer Novelle der Internationalen Telekommunikationsregulierungen umsetzen. Damit würden sie die Hoheit über das Web von der gemeinnützigen Internet Corporation for Assigned Names and Numbers (ICANN) auf die Internationale Fernmeldeunion (ITU) übertragen, eine UN-Organisation, in der nur Regierungsvertreter stimmberechtigt sind.

Zensur von Inhalten möglich
Grundlegende Elemente der Netzinfrastruktur wie das Domain Name System, die Vergabe von Top-Level-Domains und IP-Adressräumen – all das soll künftig unter der Kontrolle der Nationalstaaten stehen. Sollte es so kommen, könnten solche „Feinde des Internets“ (Reporter ohne Grenzen) künftig darüber entscheiden, wie das Web funktioniert. Kein Provider dürfte mehr ohne staatliche Genehmigung den Betrieb aufnehmen, betroffen wären auch Netzknoten oder wissenschaftliche Netzwerke. Die Staaten könnten so tatsächlich Abschaltknöpfe für das Internet schaffen – was auch bereits Politiker in Deutschland forderten.

Einige Vorschläge der Neuregelung, die im Dezember 2012 beschlossen werden soll, sehen gar Zensur von Inhalten vor. Die Lobbyorganisation der europäischen Netzbetreiber ETNO drängt zudem darauf, dass Anbieter wie Skype oder YouTube für den Zugriff auf ihre Inhalte an die Provider zahlen sollen – Gebühren, die am Ende die User tragen müssten. Vint Cerf: „Das Internet, wie wir es kennen, könnte es bald nicht mehr geben.“

Google, AOL, Skype, Facebook, Apple, Hotmail, Skype und Yahoo geben routinemässig Regierungen unsere Internet-Aktivitäten und Passwörter

Activist Post 10 June 2013: Main-Core ist der Codename einer Datenbank, die seit den 1980er Jahren von der Bundesregierung der Vereinigten Staaten gehalten wird. Main-Core enthält persönliche und finanzielle Daten von 8 Millionen US-Bürgern, die angenommen werden, Bedrohungen der nationalen Sicherheit zu sein. Die Daten, die von der

NSA, CIA und dem FBI sowie anderen Quellen kommen, werden gesammelt und ohne Haftbefehl oder Gerichtsbeschlüsse gespeichert.
Im Falle eines nationalen Notstandes, könnten diese Menschen von allem von erhöhter Überwachung und Fahndung, Vernehmen bis hin möglicherweise sogar zu Haft betroffen werden. Laut Christopher Ketchum, ist genau die Art der NSA-Schnüffelei, die Edward Snowden gerade beschrieben hat, verwendet worden, um Daten in die Main-Core-Datenbank zu füttern. The Northeast Intelligence Network 7 June 2013 bestätigt.

EUbusiness 11. Juni 2013: Am Freitag wird die EU den Vereinigten Staaten eine starke Verpflichtung abverlangen, um die Rechte der europäischen Bürger zu respektieren, nachdem bekannt geworden war, dass Washington ein weltweites Internet-Überwachungsprogramm, das das Grundrecht auf Privatsphäre und Datenschutz der EU-Bürger "potenziell gefährdet, verwaltet "

Die US-amerikanische National Security Agency (NSA) will Ihre Seele um jeden Preis: Sie will jeden ihrer Gedanken kennen lernen, sie kontrollieren und Sie zu einem kleinen Bit in ihrem nationalen, sogar globalen Megacomputer der gleichgeschalteten, kontrollierten Seelen machen. Die Nutzer ist die übliche satanistische Bankster Elite der NWO. Durch ihren Computer wollen sie totale Gesinnungskontrolle über eine gehirngewaschene, sogar hirnchip-implantierte Weltbevölkerung, wie es Nicholas Rockefeller sagte. Sie werden dann "von oben" - oder in Wirklichkeit von sehr tief unten - in allem gelenkt.
Aber bis der NSA-Big Brother diesen Wunschtraum verwirklichen kann, muss er andere Methoden verwenden, um uns zu kontrollieren: das ECHELON und weitere 40 ausgefeilte Methoden, u.a. ein Netzwerk von CCTV-Kameras, die entscheiden, ob Sie kriminelle Gedanken haben! Die NSA hat eine lange *Geschichte der Verletzungen der Verfassung und Lauschangriffe gegen die* US-Bevölkerung

***NSA´s** Bluffdale Center **(rechts):** Ein Projekt von grosser Geheimhaltung. Sein Zweck: grosse Schwaden der weltweiten Kommunikationen, wie sie sich aus Satelliten zappen und durch die U-Bahn und Seekabel internationaler, ausländischer und inländischer Vernetzungen zippen, abzufangen, zu entschlüsseln, zu analysieren und zu speichern. Das stark befestigte Zentrum sollte im September 2013 laufen. Fliessend durch seine Server und Router und in nahezu bodenlosen Datenbanken werden alle Formen der Kommunikation, einschliesslich des vollständigen Inhalts der privaten E-Mails, Handy-Telefonate und Google-Suchanfragen, sowie aller Arten von personenbezogenen Daten, Parkschein-Quittungen, Bucheinkauf Reisepläne, und anderer digitaler "Taschen-Abfälle (aus der ganzen Welt)."*

Der jüngste Trick heisst PRISMA
The Daily Mail 10 June 2013: Der 29-jährige Informant, Snowden, der $200,000 im Jahr verdiente, enthüllte erschütternde Details, wie die geheime Agentur, private Informationen über Menschen - Amerikaner und Ausländer - weltweit einsammelt – darunter auch in Grossbritannien – durch das so-genannte Prisma-Programm.

Snowden sagte: "Ich möchte nicht in einer Welt leben, wo alles, was ich tue und sage aufgezeichnet wird. Das ist nicht etwas, was ich bereit bin, zu unterstützen." Nun ist er ein Geächteter.

The Telegraph 6 June 2013: Der *Erfinder des World Wide Webs, Tim Berners Lee, sagte, das Internet stehe vor einer "grossen" Bedrohung* durch "Menschen, die es im Geheimen durch "besorgniserregende Gesetze" lenken möchten".

"Wenn man [das Internet] steuern kann, ist es die Art von Macht, wobei man ihr die Möglichkeit gibt, für immer an der Macht zu bleiben", wenn man sie *einer korrupten Regierung* gibt.

Google, AOL, Skype, Facebook, Apple, Hotmail und Yahoo sind alle auf frischer Tat ertappt ***worden, indem sie der Spionage-Agentur der Regierung, der NSA, private Nutzerdaten übergeben haben. Alle diese Unternehmen geben routinemässig an Regierungen die E-Mails, Anrufe, Text-Chats, Fotos, Dateien und sogar Logins und Passwörter ihrer Nutzer, darunter Amerikaner, weiter.***

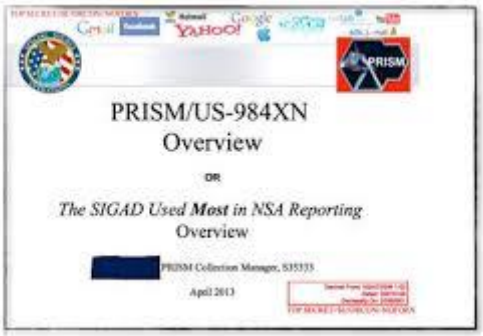
Journalist Glenn Greenwald: Ein massiver Apparat innerhalb der Regierung der Vereinigten Staaten will heimlich die Privatsphäre und Anonymität nicht nur in den Vereinigten Staaten, sondern auf der ganzen Welt zerstören".

Alle diese Unternehmen begannen sofort, jegliche Beteiligung an der NSA zu leugnen.

Was aber niemand bisher enthüllte, ist, dass ***alle diese Unternehmen gesetzlich verpflichtet sind, ihre Kunden über die geheime Regierungs-Überwachung zu belügen.*** Der Foreign Intelligence Surveillance Act macht es für jedes Unternehmen, das an der Überwachung teilnimmt, zu *Bundes-Kriminalität, die Existenz dieser Überwachung öffentlich zu bekennen.*

Director der NSA, James R. Clapper, sagte: *"Informationen, die im Rahmen dieses Programms eingesammelt sind, sind unter den wichtigsten und wertvollsten ausländischen Geheimdienst-Informationen, die wir einsammeln."*

The New York Times: ***Google, Facebook, Yahoo und andere hinterlegen einfach alle Benutzerdaten an eine andere Stelle - ein "Tor", wo die NSA sie dann kopiert.***



The Washington Post 7 June 2013: *Die National Security Agency und das FBI zapfen direkt die zentralen Server neun führender US-Internet-Unternehmen.*

The London Guardian berichtete am Freitag, das *GCHQ, Grossbritanniens Äquivalent der NSA, habe auch heimlich die Informationen aus den gleichen Internet-Unternehmen* durch eine Operation, die von der NSA konstruiert wurde, eingesammelt.

Heimlicher Zugriff auf Ihre Webcam für einen Dollar

Integrierte Webcams gefährden die Privatsphäre vieler Internet-Nutzer. Der heimliche Blick durch die Webcam einer Frau kostet auf Untergrundmarktplätzen nur einen Dollar. Bei Männern gibt es das bereits für einen Bruchteil dieses Preises.

Eine Untersuchung des britischen Radiosenders BBC 5 zeigt, dass viele Internet-Nutzer mit Hilfe ihrer Webcams bespitzelt werden. Doch es sind nicht Geheimdienste, sondern oft Jugendliche, die sich einen Spass daraus machen andere heimlich zu beobachten. Sie teilen Fotos und Videos, die sie mit fremden Webcams gemacht haben, mit anderen. Sie verkaufen sogar den Zugriff auf Webcams ahnungsloser Internet-Nutzer. Dabei kostet der Zugriff auf die Webcam einer Frau im Durchschnitt einen US-Dollar. Für den gleichen Preis kann man 100 Männer beobachten.

Ermöglicht wird dies etwa durch eingeschleuste Malware oder schlicht durch Nachlässigkeit der Benutzer. Veraltete Software-Versionen sind einmal mehr Teil des Problems. So hat Adobe bereits 2011, mit Flash Player 10.3, den Einstellungsmanager für den Flash Player von einer Seite auf der Macromedia-Website auf den lokalen Rechner verlagert (Windows Systemsteuerung). Bis dahin konnte eine präparierte Web-Seite mit einem so genannten Click-Jacking-Angriff den Zugriff auf Kamera und Mikrofon eines Benutzers unbemerkt freischalten.

In Googles Web-Browser Chrome funktionierte dieser Trick sogar noch bis vor ein paar Tagen. Google hat diese Schwachstelle im Zusammenspiel mit dem integrierten Flash Player erst am 18. Juni 2013 mit Chrome 27.0.1453.116 beseitigt.

In einem Interview der BBC mit einem jugendlichen Täter hat dieser keinerlei Unrechtsbewusstsein gezeigt. Der 17 Jahre alte Finne hat sich Zugriff auf etwa 500 Computer verschafft und die Möglichkeit deren Webcams zu steuern an andere verkauft. Das Risiko erwischt und bestraft zu werden hält er für gering. Tatsächlich handelt es um eine Straftat, die staatsanwaltliche Ermittlungen, ein Gerichtsverfahren und eine harte Strafe nach sich ziehen kann.

Ratgeber: So belauschen Hacker Sie über Ihre Webcam

Der finnische Antivirushersteller F-Secure berichtet in seinem Blog über die Untersuchung der BBC und empfiehlt das Naheliegende: decken Sie Ihre Webcam, egal ob extern oder im Notebook eingebaut, mit einem Pflaster oder Klebeband ab. Unser Zusatztipp: wenn Sie das Klebeband an einer Seite umfalten, haben Sie einen Griff, mit dem Sie die Kamera bei Bedarf leicht wieder freilegen können. Die Webcam per Software abzuschalten ist keine ausreichende Lösung, denn das kann durch andere Software, etwa Malware, wieder rückgängig gemacht werden, ohne dass Sie es bemerken.

Vergessen Sie nicht, diese Massnahme auch beim Rechner Ihres Kindes durchzuführen. Es soll ja Menschen geben, die sich besonders dafür interessieren heimlich Kinder zu

beobachten. Die sind womöglich bereit Geld dafür zu zahlen. Sprechen Sie mit Ihrem Kind darüber.

Diese Programme sperren Lauscher vom US-Geheimdienst aus

Auf einer Webseite finden Sie Alternativen zu möglicherweise vom US-Geheimdienst überwachten Programmen und Webdiensten wie Facebook, Google Chrome und der Dropbox.

Vor wenigen Tagen kam ans Licht, dass der US-Geheimdienst offensichtlich seit Jahren Daten über Internet-Nutzer sammelt. Das Projekt soll PRISM heissen und sich bei den Servern von Google, Apple, Microsoft, Facebook und vielen anderen Internetgiganten bedienen. Zwar gibt es Dementi der Internetkonzerne - doch diese sind auffallend schwach. Einige erklären, dass sie keinen "direkten Zugriff" auf die Daten ihrer Nutzer geben würden. Kritiker fragen darum, ob sie indirekten Zugriff gewähren, etwa über eine Programmierschnittstelle.

Wer den Dementi und dem US-Geheimdienst nicht traut, greift zu Alternativen von Chrome, Windows, Facebook & Co. Welche das sind, erklärt die Seite PRISM-break.org. Der Seitentitel erinnert wohl nicht zufällig an die US-Erfolgsserie "Prison Break", die zwischen 2005 und 2009 produziert wurde. Die Serie behandelt einen Ausbruch und die anschliessende Flucht aus einem Gefängnis, aber auch den Kampf gegen eine Organisation internationaler Konzerne und Regierungen.

Die meisten Tipps machen auch durchaus Sinn. So soll man etwa auf OS X, Chrome OS und Windows verzichten. Stattdessen rät die Seite zu Debian, einer Linux-Distribution oder FreeBSD. Statt Chrome, Safari oder dem IE soll man beispielsweise Firefox nutzen. Aber auch weniger offensichtliche Tipps finden sich auf der Seite. Oder wüssten Sie auf Anhieb, was man an Stelle von Google, Bing oder Yahoo Search nutzen könnte? Einige der Tipps sind aber realitätsfern - etwa die Verwendung der virtuellen Währung Bitcoin an Stelle von PayPal. Oder Diaspora statt Facebook - wo dann kaum einer der Kontakte zu finden sein dürfte. Neben reinen Alternativen verrät die Seite auch einige Verschlüsselungstools.

Auch einzelne europäische Nutzer wurden über das Prism-Programm der NSA bespitzelt.

In der vergangenen Woche sorgte die Aufdeckung des Prism-Programms der NSA für Furore. Im Rahmen des Geheimprojekts werden in den USA zahllose persönliche Daten von Internet-Nutzern gesammelt. Die Aktion machte auch europäische Datenschützer hellhörig, wodurch am Freitag ein Treffen zwischen US-amerikanischen und europäischen Gesetzesvertretern vereinbart wurde.

Die EU-Kommissarin für Justiz, Viviane Reding, betonte im Anschluss, dass die Datensammlung über das Mobilfunknetz von Verizon überwiegend eine „amerikanische Frage“ sei. Über Prism wurden jedoch nicht nur Mobilfunkdaten, sondern auch Details aus

sozialen Netzwerken und Internet-Diensten in Europa gesammelt, wodurch die NSA die Datenschutzrichtlinien der EU gebrochen verletzt habe.

Laut Reding wurde inzwischen eine Arbeitsgruppe aus US- und EU-Vertretern der Sicherheitsbranche einberufen, die Prism näher beleuchten soll. Der amerikanische Geheimdienst habe im Rahmen des Projekts Daten von Europäern gesammelt, jedoch nur von Personen, bei denen ein dringender Verdacht auf terroristische Aktivitäten und Cyber-Crime-Machenschaften bestanden habe. Im Gegensatz zum Vorgehen in den USA würden in Europa also keine riesigen Datenmengen von allen Internet-Nutzern gesammelt, erklärt Reding.

Spähprogramm des britischen Geheimdienstes aufgedeckt

Nicht nur die NSA späht Internet-Nutzer mit ihrem Prism-Programm aus, auch der britische Geheimdienst hört weltweit Telefon- und Internet-Kommunikation mit seinem Tempora-Programm ab.

Nach der Enthüllung des US-Spähprogramms Prism deckte die Zeitung Guardian am Wochenende das europäische Pendant des britischen Geheimdienstes Government Communications Headquarters (GCHQ) auf. Unter dem Codenamen Tempora werden dabei die Glasfaserkabel für den transatlantischen Datenverkehr angezapft. Tempora geht jedoch noch sehr viel weiter als Prism. Laut dem Ex-NSA-Mitarbeiter Edward Snowden, der den Prism-Skandal aufdeckte und den Medien nun Material zu Tempora zuspielt, sei das britische Projekt "das grösste verdachtslose Überwachungsprogramm in der Geschichte der Menschheit".

Das britische Spähprogramm zapft über die wichtigen Glasfaserverbindungen die Telefon- und Internet-Kommunikation von Hunderten Millionen Nutzern an – darunter auch Deutsche. Bislang seien durchschnittlich 21 Petabyte an Daten täglich abgelegt worden. Während Inhalte von der GCHQ nur rund drei Tage aufbewahrt werden, speichert der Geheimdienst Telefonnummern, Verbindungsdaten und IP-Adressen rund einen Monat.

Während Unternehmen an Prism Daten nur auf gezielte Anfragen herausgeben, speichert das britische Programm prophylaktisch alle Daten. Tempora sei laut dem Guardian ausserdem bereits seit fünf Jahren im Einsatz. Gezielt ausgewertet werden die gesammelten Daten seit 18 Monaten. Laut einer anonymen Quelle suche der Geheimdienst dabei nach vier Themenbereichen: „Sicherheit, Terror, Organisiertes Verbrechen. Und wirtschaftliches Wohlergehen.“ Durch die Nutzung von juristischen Schlupflöchern gilt Tempora in Grossbritannien sogar als legal. Britische Datenschützer fordern nun eine Überarbeitung der entsprechenden Paragrafen.

Echtzeitüberwachung auch in Deutschland

Auch in Deutschland ist unter bestimmten Bedingungen die Überwachung der Bürger möglich. Welche Gesetze hierbei greifen, erörtern die beiden Rechtsanwälte Michael Rath und Christian Kuss in einem Gastbeitrag.

Die Enthüllung des Überwachungsprogramms PRISM der National Security Agency (NSA) durch Edward Snowden hat die Diskussion über die Tätigkeit der Sicherheitsbehörden sowie

den Schutz von Bürgerrechten im Internet erneut entfacht. Über PRISM soll die NSA im beträchtlichen Umfang auf Benutzerdaten grosser Internetkonzerne wie Google, Microsoft und Facebook zugreifen können. Zudem soll die US-Sicherheitsbehörde in Echtzeit auf Daten von E-Mails, Messenger oder Internettelefonie Einblick erhalten haben.

Der tatsächliche Einsatz ist unklar und wird es aufgrund der sicherheitspolitischen Bedeutung der Geheimdienste wohl auch bleiben. Die grossen Internetkonzerne dementierten jedenfalls, dass die NSA direkt auf ihre Server zugreifen und die gespeicherten Nutzerinformationen einsehen kann. Zudem beteuern sie, Nutzerinformationen nur im gesetzlichen Rahmen an die Sicherheitsbehörden weiterzugeben.

Geltendes Recht in Deutschland

Der Vorfall gibt jedoch Anlass, die Tätigkeiten der deutschen Sicherheitsbehörden zu hinterfragen. Nachdem die Einführung technischer Überwachungsmassnahmen, wie etwa dem "Bundestrojaner" oder der Vorratsdatenspeicherung, vom Bundesverfassungsgericht gestoppt wurden, lassen sich die Ermittlungsbefugnisse aus den bestehenden Gesetzen ableiten. Danach erhalten deutsche Geheimdienste und Sicherheitsbehörden unter bestimmten Voraussetzungen Zugriff auf Benutzerinformationen und die Kommunikation im Internet.

Der Bundesnachrichtendienst darf auf Grundlage des "Artikel-10-Gesetzes" internationale Handy- und Internetverbindungen anzapfen. Foto: BND Alexander Obst/Marion Schmieding

Dem Bundesnachrichtendienst (BND) steht zur Telekommunikationsüberwachung die sogenannte "strategische Fernaufklärung" zur Verfügung. Rechtsgrundlage ist das "Artikel-10-Gesetz", welches das Brief-, Post- und Fernmeldegeheimnis unter Umständen einschränkt und durch Artikel 10 Grundgesetz gewährleistet wird. Der BND ist berechtigt, internationale Telekommunikationsbeziehungen zu überwachen und aufzuzeichnen. Dies setzt aber eine

Gefahr für die Bundesrepublik Deutschland voraus. Hierunter fallen zum Beispiel Terrorabwehr, organisierte Kriminalität und Waffenhandel.

Zusätzlich muss die Überwachung auf internationale Kommunikationsbeziehungen Zweck der Auslandsaufklärung sein, so dass innerdeutsche Sachverhalte von der Rechtsgrundlage nicht erfasst werden. Der BND darf somit Telekommunikationsdienstleister auffordern, Zugriff auf die entsprechenden Informationen zu gewähren. Die Datenbestände werden auf bestimmte Schlagworte durchsucht und die Treffer werden hinterher ausgewertet.

Umfang der Überwachung unbekannt

Der Umfang der Kommunikationsüberwachung durch die deutschen Geheimdienste ist allerdings weitgehend unbekannt. Denn Informationen hierzu werden zum Schutz der Sicherheitsinteressen der Bundesrepublik Deutschland nur selten veröffentlicht. Die Geheimdienste werden aber durch das Parlamentarische Kontrollgremium kontrolliert, indem einzelne Bundestagsabgeordnete Einblick in die Tätigkeiten erhalten.

Informationen über diese Tätigkeiten sind zum Teil durch eine kleine Anfrage der Fraktion "Die Linke" im Mai 2012 bekannt geworden: Die Telekommunikationsdienstleister stellen an einem Übergabepunkt eine Kopie der Telekommunikation zur Verfügung, auf die der BND zugreifen kann. Die "Treffer" des jeweiligen Suchlaufs werten Mitarbeiter des BND aus. Stellen sie keine Relevanz fest, werden die Daten gelöscht. Dabei stellt die Verschlüsselung der Inhalte kein ernsthaftes Hindernis dar, denn die eingesetzte Technik soll auch auf verschlüsselte Inhalte zugreifen können. Der Erfolg dieser Massnahmen ist jedoch zweifelhaft. So sollen aus 37 Millionen überwachten E-Mail- und Datenverbindungen lediglich 213 Fälle verwertbarer Informationen für den Geheimdienst entstanden sein.

Standortermittlung des Mobiltelefons

Doch nicht nur die Geheimdienste, sondern auch andere Behörden der Bundesrepublik Deutschland können offen oder verdeckt auf Benutzerinformationen zugreifen. Beispielsweise erfolgt häufig eine Ermittlung von IP-Adressen aufgrund staatsanwaltschaftlicher Ermittlungen zur Aufklärung von Straftaten im Internet. Auf Anfrage der Staatsanwaltschaft und nach richterlicher Anordnung nennen die Telekommunikationsdienstleister den jeweiligen Anschlussinhaber. Über das Handy lässt sich zudem der Standort ermittelt, um Personen aufzuspüren. Auch wenn steuerrelevante Daten elektronisch aufbewahrt werden, müssen die Finanzbehörden elektronischen Zugriff auf diese Systeme erhalten. Hierfür wird (abhängig von den Zugriffsarten Z 1 - Z 3) eine Schnittstelle zu den Datenverarbeitungssystemen der Unternehmen eingerichtet, über die Finanzbehörden auf die Informationen zugreifen können.

Diese Beispiele zeigen, dass die Überwachung von Kommunikations- und Benutzerinformationen im Internet nicht ein rein amerikanisches Phänomen ist. Auch deutsche Behörden setzen ähnliche Methoden ein. Solange die Behörden im Rahmen der geltenden Gesetze handeln, lässt sich daran aber nichts beanstanden. (tw)

(Michael Rath ist Fachanwalt für IT-Recht und Partner der Luther Rechtsanwaltsgesellschaft mbH mit Sitz in Köln. Christian Kuss hat sich als Rechtsanwalt auf IT- und Datenschutzrecht spezialisiert.)

OECD nimmt FinFisher-Hersteller Gamma unter die Lupe

Das hat die nationale Kontaktstelle der OECD in Grossbritannien mitgeteilt. Nun wird untersucht, ob der Anbieter beim Export seiner Software nach Bahrein gegen OECD-Richtlinien verstossen hat. Über eine gleichlautende Beschwerde mehrerer Menschenrechtsorganisationen gegen die Münchner Firma Trovicor ist von der deutschen Kontaktstelle noch nicht entschieden worden.

Die nationale Kontaktstelle der OECD in Grossbritannien hat die Beschwerde mehrerer Menschenrechtsorganisationen gegen die britisch-deutsche Gamma Group angenommen. Reporter ohne Grenzen, das European Center for Constitutional and Human Rights, Privacy International, das Bahrain Center for Human Rights und Bahrain Watch hatten das OECD-Verfahren im Februar eingeleitet. Sie beschuldigen das Unternehmen, nicht ausreichend überprüft zu haben, ob seine Produkte zu Menschenrechtsverletzungen beitragen.

Derselbe Vorwurf derselben Organisationen trifft übrigens die Münchener Trovicor GmbH. Über die Beschwerde in Deutschland hat die hiesige OECD-Kontaktstelle noch nicht entscheiden. Wann das der Fall sein wird, ist offen.

Trovicor hatte im April auf Anfrage von ITespresso Vorwürfe von Reporter ohne Grenzen zurückgewiesen: Man sei überrascht, auf der Liste der “Feinde des Internets” aufzutauchen. Man stelle keinerlei Software her, die mit Staatstrojanern oder anderen Schnüffelprogrammen vergleichbare wäre, sondern relationale Datenbanksysteme. Ausserdem arbeite man mit der OECD zusammen und beachte allfällige Import und Export-Bestimmungen.

Reporter ohne Grenzen wirft beiden Firmen vor Überwachungstechnologie herzustellen, die von autoritären Staaten für Menschenrechtsverletzungen eingesetzt werden kann. Beispielsweise seien Informationen aus abgefangenen Telefon- und Internetverbindungen in Bahrain insbesondere seit dem Beginn von öffentlichen Proteste im Februar 2011 verwendet worden, um Dissidenten festzunehmen und ihnen unter Misshandlungen Geständnisse abzupressen.

Der Menschenrechtsorganisation liegen eigenen Angaben zufolge deutliche Hinweise darauf vor, dass Trovicor und Gamma entsprechende Technologie an den Golfstaat geliefert haben. Das Land steht auf Platz 165 von 179 der von Reporter ohne Grenzen geführten Rangliste der Pressefreiheit und ist auch einer der von der Organisation gerügten “Feinde des Internets“.

“Gamma muss sich seiner Verantwortung stellen und sich mit den Auswirkungen seiner Produkte in Bahrain sowie möglicherweise in weiteren Ländern auseinandersetzen. Wir hoffen, dass das OECD-Verfahren Unternehmen wie Gamma nun veranlasst, ihre Grundsätze und ihre Kunden genau zu überprüfen”, erklärt Eric King, Forschungsdirektor von Privacy International, in einer Pressemitteilung.

“Dieser Fall ist der erste seiner Art und basiert auf soliden Indizien, die die Beschwerdeführer geliefert haben”, so Ala’a Shehabi von Bahrain Watch in derselben Pressemitteilung. “Er wird den Blick auf wichtige grundsätzliche Fragen lenken: Wer Geschäfte macht, die sich direkt gegen Demokratie-Aktivisten im Kampf um gleiche Rechte richten, kann auf diese Weise zum Mittäter werden.“

Auf Anfrage präsentiert sich Trovicor als Anbieter relationaler Datenbanksysteme, auf der Website wirbt man dagegen mit den Schlagworten Intelligence,Solutions, Monitoring Center, Lawful Interception und Social Network Investigations deutlich mit den Einsatzzwecken der Datenbanktechnologie (Screenshot: ITespresso)

Gamma und Trovicor waren in den vergangenen Monaten schon mehrfach in die Kritik geraten. So hatte sich im Mai Mozilla dagegen verwahrt, dass sich deren Software FinFisher als Firefox tarnt. Ebenfalls in die Schlagzeilen geriet die Firma, weil das BKA für die Quellen-Telekommunikationsüberwachung für 147.000 Euro eine Lizenz der Software FinFisher http://www.itespresso.de/2013/05/03/bundesinnenministerium-zahlt-fur-schnuffelsoftware-finspy-147-000-euro/ erworben hatte. Die Piratenpartei Deutschland hat das BKA wegen des Kaufs von FinFisher allerdings angezeigt. Sie hält es für wahrscheinlich, dass der Trojaner ebenso verfassungswidrig ist wie der zuvor von DigiTask entwickelte Bundestrojaner.

Wie dieser besteht sie nämlich aus einem Basismodul, das Funktionsmodule – etwa für eine Überwachung von Skype – nachladen kann. Gerade die Fähigkeit, einen einmal installierten Trojaner zu aktualisieren und weitere Funktionen nachzuladen, verletzt jedoch die Vorgaben des Bundesverfassungsgerichts zum Einsatz eines Staatstrojaners.

Eine Überprüfung durch die OECD mündet in ein Vermittlungsverfahren. Im – aus Sicht der Firmen schlimmsten Fall – erhalten sie, wenn Verstösse gegen Richtlinien festgestellt werden, Belehrungen, wie sie diese in Zukunft vermeiden. Strafzahlungen oder andere Bussen kann die Handelsorganisation nicht verhängen.

Bundestrojaner versus Rechtsstaatlichkeit in der Schweiz

(von Rechtsanwalt Martin Steiger; E-Mail steiger@steigerlegal.ch)

In der Schweiz wird voraussichtlich bis spätestens Ende März 2013 ein Gesetzesentwurf vorliegen, der den Einsatz von Schadsoftware zu Überwachungszwecken legalisieren soll – so der Bundesrat im Einklang mit seiner bisherigen Haltung in seiner gestrigen Antwort auf eine Interpellation von Ständerat Claude Janiak. Die Strafprozessordnung soll dazu im Rahmen der laufenden Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) mit einer entsprechenden Rechtsgrundlage ergänzt werden. Dabei soll insbesondere auch geprüft werden, wie verschlüsselte Kommunikation überwacht werden kann:

«[…] So soll beim Einsatz von Government Software die Möglichkeit geprüft werden, dass die Strafverfolgungsbehörden auch verschlüsselt übermittelte Daten (z.B. verschlüsselte E-Mails oder Skype) überwachen können. Mit den traditionellen Mitteln der Fernmeldeüberwachung ist dies nicht möglich. […]»

Der Bundesrat greift wie schon bei früheren Stellungnahmen in diesem Zusammenhang auf Neusprech zurück und verwendet den verharmlosenden Begriff «Government Ware» anstatt von Bundestrojanern oder Staatstrojanern zu schreiben. Rechtsstaatlich bedenklich bliebe die staatlich sanktionierte Überwachung mit Schadsoftware in jedem Fall, auch wenn der heutige Mangel der fehlenden Rechtsgrundlage geheilt würde, denn Bundestrojaner taugen ***prinzipbedingt*** nicht zur beweissicheren und verhältnismässigen Überwachung. Der deutsche Chaos Computer Club (CCC) hatte diese nicht lösbare Problematik beim Einsatz von Bundestrojanern schon Anfang Oktober 2011 offengelegt:

«Die von den Behörden so gern suggerierte strikte Trennung von genehmigt abhörbarer Telekommunikation und der zu schützenden digitalen Intimsphäre existiert in der Praxis nicht. Der Richtervorbehalt kann schon insofern nicht vor einem Eingriff in den privaten Kernbereich schützen, als die Daten unmittelbar aus diesem Bereich der digitalen Intimsphäre erhoben werden.»

Ende Oktober 2011 bestätigte der CCC diese grundlegende Problematik erneut:

«Der CCC zeigt zusätzlich zu den bisherigen Erkenntnissen, dass eine sogenannte ‹revisionssichere Protokollierung› im Falle eines Staats- oder Bundestrojaners nicht effektiv umsetzbar ist. In der Realität der Trojaner-Software kann sogar von unautorisierten Dritten eine Ermittlungsmassnahme mit fingierten ‹Beweisen› irregeführt werden. […]

Dahinter steckt der simple Fakt, dass ein Trojaner auf einem unkontrollierbaren System läuft, nämlich dem Computer eines Verdächtigen. Hier ist er potentiell immer unter Kontrolle des Besitzers oder eines weiteren Angreifers. Es ist nicht möglich, einen Trojaner zu entwickeln, den unautorisierte Dritte nicht imitieren könnten. Alles dazu notwendige Wissen steckt schliesslich im Trojaner selbst, den man per Definition in dem Moment aus der Hand gibt, wenn man ihn auf dem Fremdsystem installiert. Hier kann er jederzeit entdeckt und untersucht werden. Mit Trojanern erlangte Erkenntnisse sind daher generell nicht gerichtsfest. […]

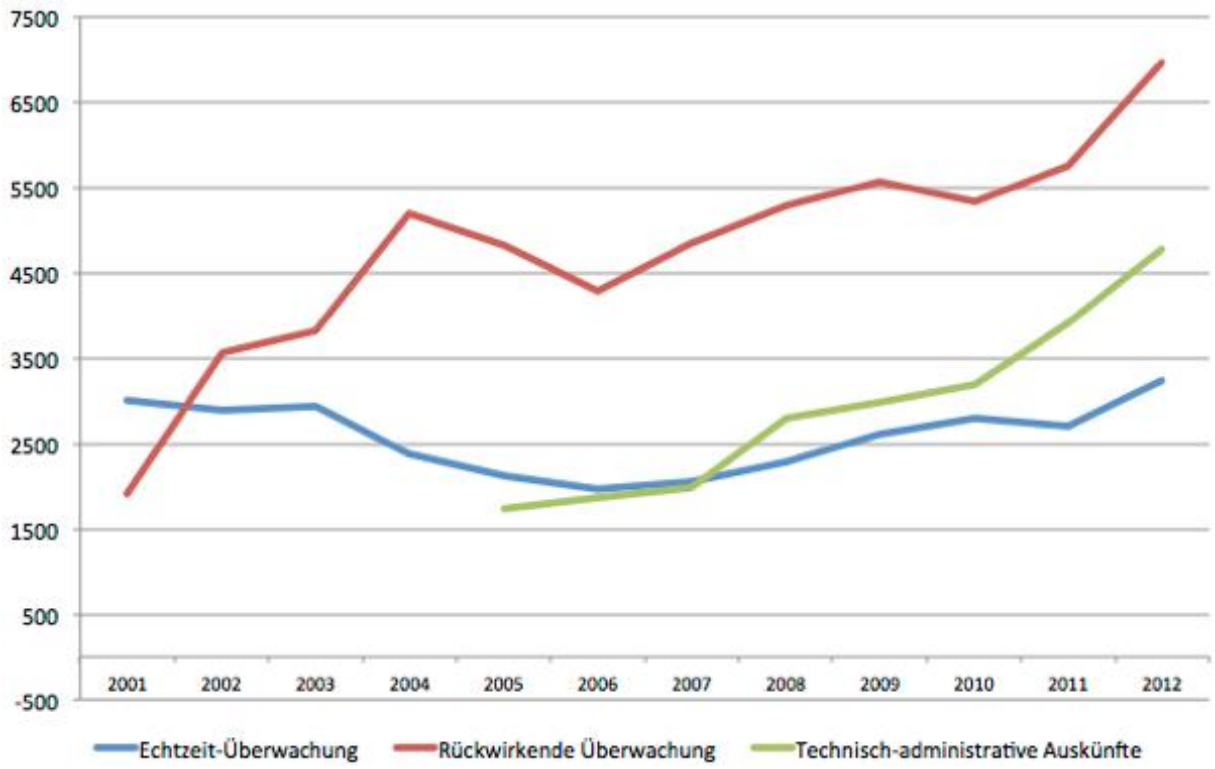
‹Per Trojaner erlangte Beweise dürfen generell nicht vor Gericht verwertet werden. Die Exekutive darf kein rechtsfreier Raum sein›, sagte ein CCC-Sprecher.»

Fazit: (Noch) Kein Bundestrojaner im Rechtsstaat

Angesichts dieser nicht lösbaren Problematik bei der Überwachung mit Bundestrojanern ist unverständlich, dass der Bundesrat dennoch an dieser zusätzlichen Art von Überwachung – ergänzend zu bereits zahlreichen Überwachungsmöglichkeiten einschliesslich Vorratsdatenspeicherung – festhält. Die rechtsstaatlichen Mängel beim Einsatz von Bundestrojanern lassen sich mit der Schaffung einer Rechtsgrundlage nicht lösen und sind auch andersweitig nicht lösbar – entsprechend sollte vollständig auf die Verwendung von Bundestrojanern verzichtet werden.

Schweizer Schnüffelstaat 2012 mit Überwachungsrekord

Im letzten Jahr schnüffelte der Überwachungstaat in der Schweiz so viel wie noch nie, wie sich der heute veröffentlichten Statistik des Dienstes «Überwachung Post- und Fernmeldeverkehr» (Dienst «ÜPF») entnehmen lässt (Vorjahres-Statistik):



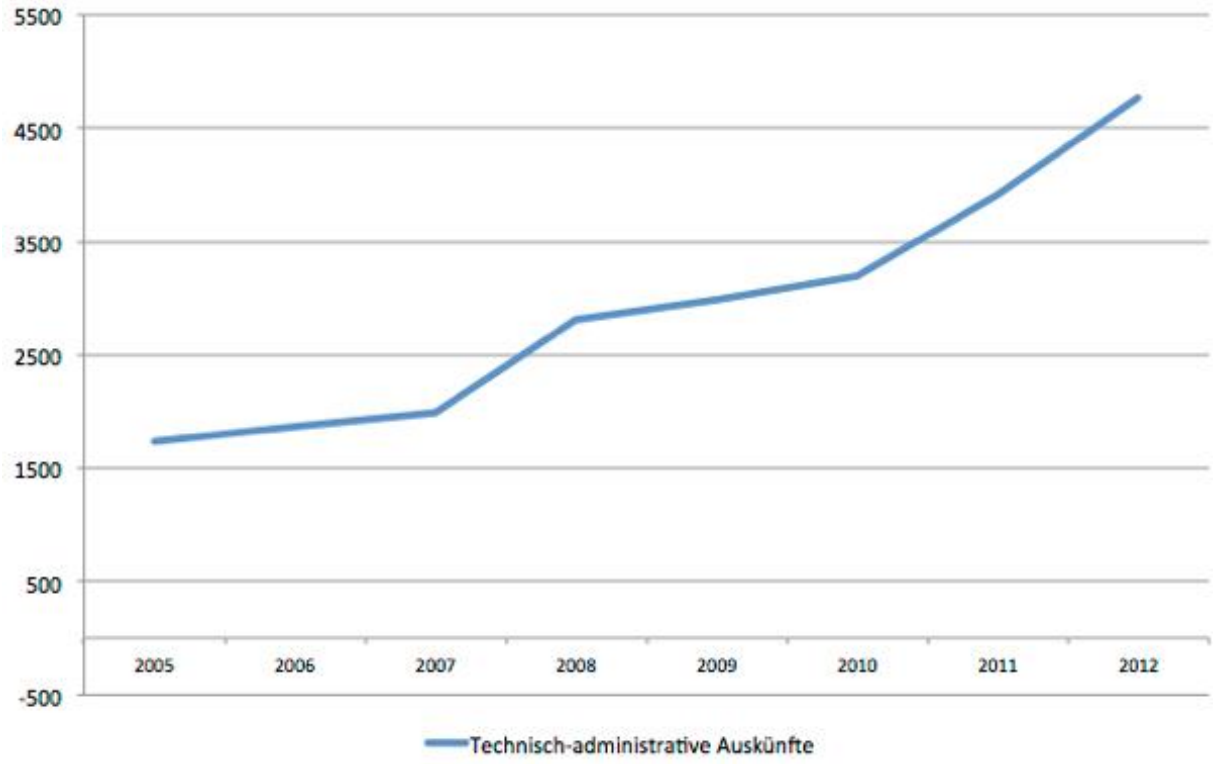
«[…] Die Statistik zeigt, dass die Fernmeldeüberwachungen in Echtzeit, also das Mithören von Telefonaten bzw. Mitlesen von E-Mails durch die jeweiligen Strafverfolgungsbehörden, im Jahr 2012 um 20 % auf 3‘233 zugenommen haben. Die Strafverfolgungsbehörden ordneten auch häufiger rückwirkende Fernmeldeüberwachungen an (+ 21% auf 6‘960) und ersuchten um mehr technisch-administrative Auskünfte (+ 22% auf 4’775). Die Zahl der einfachen Auskünfte nahm um 15% auf 202‘579 zu. […]»

Vorratsdatenspeicherung

Besonders stark stieg erneut die Zahl jener Überwachungsmassnahmen an, die Vorratsdatenspeicherung voraussetzen, nämlich die so genannt rückwirkenden Massnahmen basierend auf Verkehrsdaten-Erhebung (auch als Randdaten oder Vorratsdaten bezeichnet). Bemerkenswert ist die Verteilung der rückwirkenden Überwachungs-Massnahmen unter den schweizerischen Kantonen. So fiel fast ein Drittel davon im Kanton Genf an. Die Zahl rückwirkender Überwachungsmassnahmen hat sich schweizweit seit Anfang der 2000er-Jahre mehr als vervierfacht!

In der Dienst «ÜPF»-Statistik nicht direkt erwähnt werden die so genannten Antennensuchläufe. Dabei werden im Sinn einer Rasterfahdnung alle Mobilfunk-Teilnehmer, die zu einem spezifischen Zeitpunkt über eine definierte Mobilfunk-Antenne ihr Handy

benutzt haben, zu Verdächtigen. Gemäss der detaillierten Statistik (Microsoft Excel-Dokument) gab es im letzten Jahr 105 solcher Antennensuchläufe und zwar fast ausschliesslich bezüglich Raub (Art. 140 StGB).



Statistik mit beschränkter Aussagekraft

Der Dienst «ÜPF» betont, die Überwachungszahlen müssten in Relation zu den ***«begangenen Delikten»*** – an dieser Stelle fehlt «mutmasslich» – gesehen werden. Ausserdem seien pro Delikt häufig mehrere Massnahmen zur Überwachung notwendig, wobei weitere zahlenmässige Angaben zu den einzelnen Überwachungen allerdings fehlen. Beispiele für solche Angaben wären die Zahl der betroffenen Personen bei Antennensuchläufen oder die Zahl der mitgelesenen E-Mails. So bleibt die Statistik von beschränkter Aussagekraft.

Bei der Statistik ist im Übrigen zu beachten, dass der Dienst «ÜPF» ausschliesslich für die Überwachung des Post- und Fernmeldeverkehrs (Art. 269 ff. StPO) zuständig ist, so dass beispielsweise Angaben zu verdeckten Ermittlungen oder dem Einsatz technischer Überwachungsgeräte fehlen. Auch Angaben zur Bundestrojaner-Verwendung in der Schweiz kann der Dienst «ÜPF» nicht liefern.

Ein neues Nachrichtendienstgesetz erlaubt Lauschangriffe in- und ausserhalb der Landesgrenzen. Besonders im Ausland sind die Kompetenzen schier schrankenlos. Die Debatte um ein besseres Abwehrdispositiv erhält neuen Aufwind. (JNS und Agenturen)

Das Verteidigungsdepartement (VBS) bemängelt seit längerem „gewichtige Lücken im Abwehrdispositiv". Die Kontroversen um die mutmasslichen Verfehlungen von CIA-Agenten könnten der Diskussion nun neuen Schub verleihen. Das neue schweizerische Nachrichtendienstgesetz sieht jetzt natürlich auch die Erfassung der Leitungsnetze vor.

Bislang darf der Nachrichtendienst des Bundes (NDB) im Inland weder Telefonate mitschneiden noch private Gespräche in geschlossenen Räumen mithören und in fremde Computer eindringen. Aus diesem Grund endet die Abwehr ausländischer Spionageaktivitäten laut VBS heute an der Tür zum privaten Raum: „Spione nutzen diese Lücke bewusst aus; sie stehen vielfach unter diplomatischer Immunität und sind geschult, unter Tarnung Informationen zu beschaffen." Ein Problem seien auch internationale Ermittlungsbüros, die in getarntem staatlichen Auftrag handelten.

Carte Blanche im Ausland?

Im Jahr 2009 lehnte es das Parlament trotz eingeschränkter Spionageabwehr noch ab, die Kompetenzen des NDB auszuweiten. Im März hat der Bundesrat mit dem neuen Nachrichtendienstgesetz einen zweiten Anlauf gestartet. Pikant: Dieses erlaubt neu nicht nur Lauschangriffe im Inland, sondern regelt erstmals auf gesetzlicher Ebene verdeckte Beschaffungsaktivitäten im Ausland. Innerhalb der Landesgrenzen muss der NDB für jede gesetzte Wanze, jeden eingeschleusten Trojaner und jedes abgehörte Telefonat vorgängig eine Genehmigung vom Bundesverwaltungsgericht und dem VBS-Vorsteher einholen.

Ausserhalb der Landesgrenzen sind dem Dienst jedoch kaum Schranken gesetzt. Seine Mitarbeiter dürfen alle Beschaffungsmassnahmen in eigener Verantwortung umsetzen, ohne davor eine Bewilligung einholen zu müssen. Der Grund: Spionage ist eigentlich überall verboten. Darum ergibt es aus Sicht des Bundesrates wenig Sinn, wenn Schweizer Behörden illegale Aktionen auf fremdem Boden vorgängig genehmigen.

Attachés als legale Informanten

Ausserdem, so schreibt zumindest das VBS, benötigen jene NDB-Verantwortlichen, die für die Beschaffung von Auslandnachrichten zuständig sind, „eine grössere situative Handlungs- und Ermessensfreiheit in der Wahl der Mittel" als ihre Kollegen im Inland. Eine Bedingung gibt es jedoch: Der Nachrichtendienst muss all seine Aktivitäten im Ausland dokumentieren und dem VBS wie auch den parlamentarischen Aufsichtsgremien Rechenschaft ablegen.

Als legale Form der Informationsbeschaffung gilt es, wenn Verteidigungsattachés der Armee im Ausland ihr Kontaktnetz zu Partnerdiensten und diplomatischen Vertretungen nutzen, um den NDB auf dem Laufenden zu halten. Sie sind laut VBS „keine Spione in Uniform", sondern offiziell als Verdingungspersonen des NDB akkreditiert.

Wie E-Mails aus der Schweiz überwacht werden

Über ein Kabel laufen Übersee-Telefongespräche und Internetkommunikation aus der Schweiz. Dieses Kabel wird von Geheimdiensten genutzt, um Telefongespräche, E-Mail und Facebook-Aktivitäten der Schweizer Bürger zu überwachen.

So hat auch der britische Nachrichtendienst Government Communications Headquarters 200 Glasfaserkabel auf der ganzen Welt angezapft. Die abgefangenen Informationen sollen gemäss Snowden drei Tage lang gespeichert bleiben. Benutzerdaten gar während 30 Tagen.

Insgesamt gibt es rund ein Dutzend Tiefseekabel, die zwischen Europa und Amerika verlaufen. Wie die „Süddeutsche Zeitung“ herausgefunden hat, zapfen die Briten unter anderem das Kabel mit der Bezeichnung TAT-14 an, das im Dörfchen Bude an der britischen Küste anstösst.

Nun wird bekannt, dass über dieses Kabel auch Schweizer Telefongespräche in die USA, E-Mails, die über US-Server laufen, und Aktivitäten auf sozialen Netzwerken wie Facebook übermittelt werden. Das berichtete der Tages-Anzeiger in der Ausgabe vom 26.06.2013. Die gesammelten Informationen werden vom britischen Nachrichtendienst gefiltert und überwacht.

Indirekte Beteiligung der Swisscom

Wie der «Tages Anzeiger» weiter berichtet, ist die Swisscom am Kabel TAT-14 beteiligt. Sie gehörte zu einem Konsortium von rund 50 Telekommunikationsfirmen, das dieses Kabel im Jahr 2001 errichtet hat.

Seit 2005 ist die Swisscom jedoch nur noch indirekt über das belgische Telekommunikationsunternehmen Bics am Kabel beteiligt. Die Swisscom besitzt 22,4 Prozent der belgischen Firma. Wie hoch der Anteil der Bics am TAT-14 ist, ist nicht bekannt.

Trotzdem sind nicht nur Telefongespräche und Internetdaten der Swisscom vom Lauschangriff der Briten betroffen, sondern alle Gespräche und Daten, die über die Knotenpunkte Zürich und Genf laufen und dann via Frankfurt oder Paris in die Nordsee oder den Atlantik gelangen.

Die Swisscom erklärte auf Anfrage des „Tages Anzeigers“, dass ihnen „keine“ Informationen vorlägen, dass es zu unerlaubten Zugriffen auf das TAT-14-Netzwerk bekommen sei. Es werden „grundsätzlich keine Informationen an ausländische Behörden geliefert.“

Zu den ganzen Themen von Spionage und illegalen Abhörmethoden ausländischer Nachrichtendienste gehörte die Schweiz von Anfang an mit zu den entscheidenden Playern in diesem globalem Gesamtsystem der Spionage. Ein wichtiger Teil ist hierbei das Schweizer Abhörsystem Onyx.

Rückblende: Am Mittwoch, dem 13. August 1997, tagte der Bundesrat in der Besetzung Jean-Pascal Delamuraz (FDP), Kaspar Villiger (FDP), Arnold Koller (CVP), Flavio Cotti (CVP), Ruth Dreifuss (SP), Moritz Leuenberger (SP) und Adolf Ogi (SVP).

Ogi, der damalige Wehrminister, brachte den hochgeheimen Antrag ein, es sei das «Projekt Satos 3» zu starten, die dritte Stufe eines seit Anfang der neunziger Jahre laufenden militärischen Geheimprogramms. «Satos 1» und «Satos 2» waren Systeme, mit denen die Kommunikation per Kurzwellen, Richtfunk und Faxsignale abgefangen werden konnte. Nun sollte Satos 3 die vollständige «elektronische Aufklärung von Satellitenverbindungen» ermöglichen, genau wie das grosse Vorbild, das «Echelon»-System der USA.

Ausgearbeitet hatte den Plan, von Zimmerwald aus weltweit die Telefon-, Fax- und Mailverbindungen zu überwachen, der militärische Geheimdienst unter dem Kommando von Divisionär Peter Regli. Die Kosten für den Aufbau der Infrastrukturen und für die Software wurden intern auf rund fünfzig Millionen Franken geschätzt, ohne die Löhne der über vierzig Sprachspezialisten und Informatiker, die rekrutiert werden mussten. Die Landesregierung stimmte erstens dem Vorhaben Satos 3 zu, segnete zweitens die versteckte, also illegale Finanzierung und drittens die totale Geheimhaltung ab. Der Entscheid vom 13. August 1997 fehlt sogar im hochvertraulichen Verzeichnis der Beschlüsse des Bundesrates. Ein Protokoll existiert offenbar auch nicht; an die Öffentlichkeit drang nichts.

In fast fahrlässiger Ahnungslosigkeit hatte darum das Parlament zuerst unter nicht näher deklarierten Rubriken, später unter dem verschleiernden Titel „Neubau eines Mehrzweckgebäudes in Zimmerwald“ blind ab 1997 regelmässig Kredittranchen bewilligt. Diese verdeckte, illegale Finanzierung des gigantischen Systems ist ein Skandal, wenn auch noch der kleinste. Das zweite Ärgernis ist der steile Anstieg der Kosten. Gemäss inoffiziellen Angaben bewilligte der Bundesrat im August 1997 einen Betrag von 50 Millionen für das Projekt. Diese Summe hat sich laut damaliger GPDel-Berichterstatterin, FDP-Ständerätin Helen Leumann (LU), bis Mitte 2003 bereits verdreifacht.

Genaue Beträge wollte auch die Eidgenössische Finanzkontrolle (EFK) in diesem delikaten Fall nie nennen. Nur in ihrem Jahresbericht 2003 monierte sie, „dass die geschätzten Kosten, die dem Entscheid des Bundesrates zugrunde gelegt wurden, zu wenig fundiert waren beziehungsweise ungenügende Hinweise auf Unsicherheiten und Risiken gemacht wurden“. Mit der Abwicklung des Projektes über drei verschiedene Budgetrubriken werde zudem die finanzielle Transparenz eingeschränkt. Mehr hat die zahlende Öffentlichkeit bisher nicht vernehmen dürfen. Das Projekt Satos-Onyx den internen Revisoren definitiv entglitten.

Was die Geheimdienstler allerdings genau abhören und wer welches Material zu welchem Zweck erhält und wie weiterverwendet, ist auch bis heute nicht ganz klar. Zwar stellen Parlamentarier ab und zu Fragen, doch der grösste und perfideste Lauschangriff der Geschichte der Schweiz wurde an allen Kontrollinstanzen vorbei eingerichtet und dem Volk verschwiegen. Auf den Onyx-Grossrechnern laufen Programme, welche alle abgesaugten Rohinformationen mit Hilfe von Künstlicher Intelligenz (KI), optischer Texterkennung (OCR), Sprach- und Stimmprüfung sowie von Schlüsselwort- und Themenanalysen filtern und sortieren. Werden vier bis fünf dieser «hitwords» oder «keywords» kombiniert, lässt sich die riesige Datenflut entscheidend kanalisieren und werden anschliessend an die beteiligten Dienste weitergeleitet.

Der Bund hat offiziell über die Swisscom das Areal in Leuk an den amerikanischen Telekommunikationskonzern „Verestar Teleport“ verkauft, der alle Arten von leitungsgebundenen oder satellitengestützten Verbindungen anbietet und auch das US-Verteidigungsministerium und NSA beliefert. Bereits im Jahre 2002 verweisen die Berichte der französischen und belgischen Sicherheits- und Verteidigungskommissionen, dass technische und organisatorische Verbindungen zwischen dem Schweizer Horchposten und der Verestar-Anlage bestehen. Und der Schweizer Bundesrat hält ungeachtet dessen an seiner Verlautbarung fest. „Es gebe keine Verbindung zwischen dem Onyx-System und der US-Firma; und operiere nicht mit sensiblem Material.“

Abhören von Schweizer Kommunikationsteilnehmern

Eigentlich sollten Informationen schweizerischer Kommunikationsteilnehmer per Gesetzes wegen ausgenommen sein. Die abgefangene Informationen dieses Personenkreises werde als "Nebenprodukte" bezeichnet, müssten laut Art. 5 Abs. 2 EKVF gelöscht werden. Der gleiche Artikel besagt aber auch, dass sie in "bearbeiteter" Form an die Auftraggeber weitergeleitet werden können, "soweit sie der Erfüllung des Auftrages dienen". Ergänzend erlaubt Art. 5 Abs. 3 VEKF in Verbindung mit dem erst im Januar 2004 eingefügten Art. 99 Abs. 2bis des Bundesgesetzes vom 3. Februar 1995 über die Armee und die Militärverwaltung (MG), dass diese Nebenprodukte trotzdem an den DAP weitergeleitet werden dürfen, wenn sie "für die innere Sicherheit oder die Strafverfolgung von Bedeutung sind". Aus einem Bericht der GPDel geht hervor, dass es zu Weitergaben von eben diesen Nebenprodukten an den SND kommt, was eigentlich verboten ist, denn der Bericht erwähnt zur geheimen "Beilage 4", dass "in einem derartigen Fall weitergeleitete Informationen Gegenstand eines vom SND und der EKF erstellten Protokolls sind.

Damit wird offiziell bestätig, dass die ONYX Stationen und die EKF über einen "Umweg" trotz des Verbots inländischer Aufklärung auch der Überwachung von Personenkreisen dienen, die als Schweizerische Kommunikationsteilnehmer zu verstehen sind und diese "Nebenprodukte" aus den Abhörmassnahmen der ONYX Stationen, die sich ja eigentlich nur auf Funkaufklärungsobjekte im Ausland und auf Themen aus dem Ausland beziehen dürften, die die äussere Sicherheit der Schweiz betreffen, auch dem SND und einem Geheimdienst wie dem DAP zufliessen, der laut Definition nur für Belange der inneren Sicherheit und Strafverfolgung innerhalb der Schweiz zuständig ist.

Nachrichtendienstlicher Austausch mit dem Ausland

Neben der Weitergabe der Informationen durch die EKF zuerst an den SND und den DAP und vorn dort an weiter Behörden erfolgt auch die Weitergabe an ausländische Geheimdienste. Mit wem DAP und SND regelmässige Kontakte hat, bestimmt der Bundesrat, die Namen der ausländischen "Partner" wird nicht öffentlich bekanntgegeben.

Im Vordergrund steht vor allem die Weitergabe von Informationen im Tausch von ausländischen Diensten und sich mit den ONYX Kapazitäten in der globalen Geheimdienstlandschaft als „neutrale“ Schweiz Geltung zu verschaffen. Zum Beispiel erlauben Art. 7 Abs. 3 der Verordnung über die Nachrichtendienste (VND) dem SND Informationen mit ausländischen Diensten auszutauschen, wenn dies im Interesse der Schweiz erforderlich ist, Art. 99 Abs. 2 MG besagt, dass die EKF Personendaten mit Einschluss von besonders schützenswerten Daten und Persönlichkeitsprofilen abweichend von datenschutzrechtlichen Bestimmungen ins Ausland weitergeben kann und Art. 17 Abs. 3 des Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) erlaubt den Nachrichtendiensten Personendaten an die Sicherheitsorgane anderer Staaten weitergeben, z. B. wenn dies "zur Wahrung erheblicher Sicherheitsinteressen der Schweiz oder des Empfängerstaates unerlässlich ist".

Laut einem GPDel-Bericht bilden die Onyx-Informationen „ein nützliches Tauschmittel“ an der internationalen Geheimdienstbörse. Der Aufwand von Hunderten von Millionen Franken wird demnach hauptsächlich betrieben, um „befreundete Dienste“ wie die Secret Services der USA zu beliefern: „Die mit Hilfe von Onyx eingeholten Informationen sind deshalb auch ein Instrument, mit dem die Türen zu anderen Nachrichtendiensten geöffnet werden können und mit dem sich die schweizerischen Nachrichtendienste im Ausland Glaubwürdigkeit verschaffen können.“

Bei derart engen Verflechtungen zwischen den Schweizer und den US- oder Nato-Diensten schrumpft die immer wieder gestellte Frage nach der direkten technischen Vernetzung von Onyx mit dem amerikanischen Echelon-System zur Bagatelle. Wenn die Geschäftsprüfer auch weiterhin versuchen zu vermelden, dass sie keine Hinweise „auf eine mögliche Integration des Systems Onyx in irgendein internationales Abhörnetz“ gefunden hätten, dass Onyx „autonom“ funktioniere und „über keine Schnittstellen mit einem anderen, ausländischen System“ verfüge, dann sind diese Erkenntnisse relativ unerheblich.

Die Zusammenarbeit zwischen der Schweiz, der NSA und den anderen westlichen Nachrichtendiensten funktioniert seit über einem Jahrzehnt bestens. Es werden Frequenzen, Übermittlungskanäle, Verkehrsanalysen und sogar auch Rufnummern ausgetauscht, um die Aufklärungsziele besser zu identifizieren oder um Doppelspurigkeit zu vermeiden. Die internationale Gruppenarbeit wird nach erfolgter Belauschung fortgesetzt: Die Resultate werden quasi automatisch weiter geleitet und gegenseitig abgeglichen.

Nur der Schweizer Bevölkerung gegenüber versucht man sich erstaunt zu geben, wenn über die Medien Berichte verteilt werden, dass in der Schweiz ausländische Dienste wie der NSA tätig sind.