The Digital Arms Race. By Jacob Appelbaum et al, Spiegel Online International, 18 January 2015.

Normally, internship applicants need to have polished resumes, with volunteer work on social projects considered a plus. But at Politerain, the job posting calls for candidates with significantly different skill sets. We are, the ad says, "looking for interns who want to break things."

Politerain is not a project associated with a conventional company. It is run by a US government intelligence organization, the National Security Agency (NSA). More precisely, it's operated by the NSA's digital snipers with Tailored Access Operations (TAO), the department responsible for breaking into computers.

Potential interns are also told that research into third party computers might include plans to "remotely degrade or destroy opponent computers, routers, servers and network enabled devices by attacking the hardware." Using a program called Passionatepolka, for example, they may be asked to "remotely brick network cards." With programs like Berserkr they would implant "persistent backdoors" and "parasitic drivers". Using another piece of software called Barnfire, they would "erase the BIOS on a brand of servers that act as a backbone to many rival governments."

An intern's tasks might also include remotely destroying the functionality of hard drives. Ultimately, the goal of the internship program was "developing an attacker's mindset."

The internship listing is eight years old, but the attacker's mindset has since become a kind of doctrine for the NSA's data spies. And the intelligence service isn't just trying to achieve mass surveillance of Internet communication, either. The digital spies of the Five Eyes alliance -- comprised of the United States, Britain, Canada, Australia and New Zealand -- want more.

The Birth of D Weapons

According to top secret documents from the archive of NSA whistleblower Edward Snowden seen exclusively by SPIEGEL, they are planning for wars of the future in which the Internet will play a critical role, with the aim of being able to use the net to paralyze computer networks and, by doing so, potentially all the infrastructure they control, including power and water supplies, factories, airports or the flow of money.

During the 20th century, scientists developed so-called ABC weapons -- atomic, biological and chemical. It took decades before their deployment could be regulated and, at least partly, outlawed. New digital weapons have now been developed for the war on the Internet. But there are almost no international conventions or supervisory authorities for these D weapons, and the only law that applies is the survival of the fittest.

Canadian media theorist Marshall McLuhan foresaw these developments decades ago. In 1970, he wrote, "World War III is a guerrilla information war with no division between military and civilian participation." That's precisely the reality that spies are preparing for today.

The US Army, Navy, Marines and Air Force have already established their own cyber forces, but it is the NSA, also officially a military agency, that is taking the lead. It's no coincidence that the director of the NSA also serves as the head of the US Cyber Command. The country's leading data spy, Admiral Michael Rogers, is also its chief cyber warrior and his close to 40,000 employees are responsible for both digital spying and destructive network attacks.

Surveillance only 'Phase 0'

From a military perspective, surveillance of the Internet is merely "Phase 0" in the US digital war strategy. Internal NSA documents indicate that it is the prerequisite for everything that follows. They show that the aim of the surveillance is to detect vulnerabilities in enemy systems. Once "stealthy implants" have been placed to infiltrate enemy systems, thus allowing "permanent accesses," then Phase Three has been achieved -- a phase headed by the word "dominate" in the documents. This enables them to "control/destroy critical systems & networks at will through pre-positioned accesses (laid in Phase 0)." Critical infrastructure is considered by the agency to be anything that is important in keeping a society running: energy, communications and transportation. The internal documents state that the ultimate goal is "real time controlled escalation".

One NSA presentation proclaims that "the next major conflict will start in cyberspace." To that end, the US government is currently undertaking a massive effort to digitally arm itself for network warfare. For the 2013 secret intelligence budget, the NSA projected it would need around $1 billion in order to increase the strength of its computer network attack operations. The budget included an increase of some $32 million for "unconventional solutions" alone.

NSA Docs on Network Attacks and Exploitation

In recent years, malware has emerged that experts have attributed to the NSA and its Five Eyes alliance based on a number of indicators. They include programs like Stuxnet, used to attack the Iranian nuclear program. Or Regin, a powerful spyware trojan that created a furor in Germany after it infected the USB stick of a high-ranking staffer to Chancellor Angela Merkel. Agents also used Regin in attacks against the European Commission, the EU's executive, and Belgian telecoms company Belgacom in 2011.

Given that spies can routinely break through just about any security software, virtually all Internet users are at risk of a data attack.

The new documents shed some new light on other revelations as well. Although an attack called Quantuminsert has been widely reported by SPIEGEL and others, documentation shows that in reality it has a low success rate and it has likely been replaced by more reliable attacks such as Quantumdirk, which injects malicious content into chat services provided by websites such as Facebook and Yahoo. And computers infected with Straitbizarre can be turned into disposable and non-attributable "shooter" nodes. These nodes can then receive messages from the NSA's Quantum network, which is used for "command and control for very large scale active exploitation and attack." The secret agents were also able to breach mobile phones by exploiting a vulnerability in the Safari browser in order to obtain sensitive data and remotely implant malicious code.

In this guerilla war over data, little differentiation is made between soldiers and civilians, the Snowden documents show. Any Internet user could suffer damage to his or her data or computer. It also has the potential to create perils in the offline world as well. If, for example, a D weapon like Barnfire were to destroy or "brick" the control center of a hospital as a result of a programming error, people who don't even own a mobile phone could be affected.

Intelligence agencies have adopted "plausible deniability" as their guiding principle for Internet operations. To ensure their ability to do so, they seek to make it impossible to trace the author of the attack.

It's a stunning approach with which the digital spies deliberately undermine the very foundations of the rule of law around the globe. This approach threatens to transform the Internet into a lawless zone in which superpowers and their secret services operate according to their own whims with very few ways to hold them accountable for their actions.

NSA Docs on Malware and Implants

Attribution is difficult and requires considerable forensic effort. But in the new documents there are at least a few pointers. Querty, for example, is a keylogger that was part of the Snowden archive. It's a piece of software designed to surreptitiously intercept all keyboard keys pressed by the victim and record them for later inspection. It is an ordinary, indeed rather dated, keylogger. Similar software can already be found in numerous applications, so it doesn't seem to pose any acute danger -- but the sourcecode contained in it does reveal some interesting details. They suggest that this keylogger might be part of the large arsenal of modules that that belong to the Warriorpride program, a kind of universal Esperanto software used by all the Five Eyes partner agencies that at times was even able to break into iPhones, among other capabilities. The documents published by SPIEGEL include sample code from the keylogger to foster further research and enable the creation of appropriate defenses.

'Just a Bunch of Hackers'

The men and women working for the Remote Operations Center (ROC), which uses the codename S321, at the agency's headquarters in Fort Meade, Maryland, work on one of the NSA's most crucial teams, the unit responsible for covert operations. S321 employees are located on the third floor of one of the main buildings on the NSA's campus. In one report from the Snowden archive, an NSA man reminisces about how, when they got started, the ROC people were "just a bunch of hackers." Initially, people worked "in a more ad hoc manner," the report states. Nowadays, however, procedures are "more systematic". Even before NSA management massively expanded the ROC group during the summer of 2005, the department's motto was, "Your data is our data, your equipment is our equipment."

The agents sit in front of their monitors, working in shifts around the clock. Just how close the NSA has already gotten to its aim of "global network dominance" is illustrated particularly well by the work of department S31177, codenamed Transgression.

The department's task is to trace foreign cyber attacks, observe and analyze them and, in the best case scenario, to siphon off the insights of competing intelligence agencies. This form of "Cyber Counter Intelligence" counts among the most delicate forms of modern spying.

In addition to providing a view of the US's own ability to conduct digital attacks, Snowden's archive also reveals the capabilities of other countries. The Transgression team has access to years of preliminary field work and experience at its disposal, including databases in which malware and network attacks from other countries are cataloged.

The Snowden documents show that the NSA and its Five Eyes partners have put numerous network attacks waged by other countries to their own use in recent years. One 2009 document states that the department's remit is to "discover, understand (and) evaluate" foreign attacks. Another document reads: "Steal their tools, tradecraft, targets and take."

In 2009, an NSA unit took notice of a data breach affecting workers at the US Department of Defense. The department traced an IP address in Asia that functioned as the command center for the attack. By the end of their detective work, the Americans succeeded not only in tracing the attack's point of origin to China, but also in tapping intelligence information from other Chinese attacks -- including data that had been stolen from the United Nations. Afterwards, NSA workers in Fort Meade continued to read over their shoulders as the Chinese secretly collected further internal UN data. "NSA is able to tap into Chinese SIGINT collection," a report on the success in 2011 stated. SIGINT is short for signals intelligence.

The practice of letting other intelligence services do the dirty work and then tapping their results is so successful that the NSA even has a name for it: "Fourth Party Collection." And all countries that aren't part of the Five Eye alliance are considered potential targets for use of this "non-traditional" technique -- even Germany.

'Difficult To Track, Difficult To Target'

The Snowden documents show that, thanks to fourth party collection, the NSA succeeded in detecting numerous incidents of data spying over the past 10 years, with many attacks originating from China and Russia. It also enabled the Tailored Access Operations (TAO) to track down the IP address of the control server used by China and, from there, to detect the people responsible inside the Peoples' Liberation Army. It wasn't easy, the NSA spies noted. The Chinese had apparently used changing IP addresses, making them "difficult to track; difficult to target." In the end, though, the document states, they succeeded in exploiting a central router.

The document suggests that things got more challenging when the NSA sought to turn the tables and go after the attacker. Only after extensive "wading through uninteresting data" did they finally succeed in infiltrating the computer of a high-ranking Chinese military official and accessing information regarding targets in the US government and in other governments around the world. They also were able to access sourcecode for Chinese malware.

NSA Docs on Fourth Party Access

But there have also been successful Chinese operations. The Snowden documents include an internal NSA assessment from a few years ago of the damage caused. The report indicates that the US Defense Department alone registered more than 30,000 known incidents; more than 1,600 computers connected to its network had been hacked. Surprisingly high costs are listed for damage assessment and network repair: more than $100 million.

Among the data on "sensitive military technologies" hit in the attack were air refueling schedules, the military logistics planning system, missile navigation systems belonging to the Navy, information about nuclear submarines, missile defense and other top secret defense projects.

The desire to know everything isn't, of course, an affliction only suffered by the Chinese, Americans, Russians and British. Years ago, US agents discovered a hacking operation originating in Iran in a monitoring operation that was codenamed Voyeur. A different wave of attacks, known as Snowglobe, appears to have originated in France.

Transforming Defenses into Attacks

The search for foreign cyber attacks has long since been largely automated by the NSA and its Five Eyes partners. The Tutelage system can identify incursions and ensure that they do not reach their targets.

The examples given in the Snowden documents are not limited to attacks originating in China. The relatively primitive Low Orbit Ion Cannon (LOIC) is also mentioned. The name refers to malware used by the protest movement Anonymous to disable target websites. In that instance, one document notes, Tutelage was able to recognize and block the IP addresses being used to conduct the denial of service attack.

The NSA is also able to transform its defenses into an attack of its own. The method is described as "reverse engineer, repurpose software" and involves botnets, sometimes comprising millions of computers belonging to normal users onto which software has been covertly installed. They can thus be controlled remotely as part of a "zombie army" to paralyze companies or to extort them. If the infected hosts appear to be within the United States, the relevant information will be forwarded to the FBI Office of Victim Assistance. However, a host infected with an exploitable bot could be hijacked through a Quantumbot attack and redirected to the NSA. This program is identified in NSA documents as Defiantwarrior and it is said to provide advantages such as "pervasive network analysis vantage points" and "throw-away non-attributable CNA (*eds: computer network attack*) nodes". This system leaves people's computers vulnerable and covertly uses them for network operations that might be traced back to an innocent victim. Instead of providing protection to private Internet users, Quantumbot uses them as human shields in order to disguise its own attacks.

NSA Docs on Botnet Takeovers

NSA specialists at the Remote Operations Center (ROC) have an entire palette of digital skeleton keys and crowbars enabling access to even the best protected computer networks. They give their tools aggressive-sounding names, as though they were operating an app-store for cyber criminals: The implant tool "Hammerchant" allows the recording of Internet-based phone calls (VoIP). Foxacid allows agents to continually add functions to small malware programs even after they have been installed in target computers. The project's logo is a fox that screams as it is dissolved in acid. The NSA has declined to comment on operational details but insists that it has not violated the law.

But as well developed as the weapons of digital war may be, there is a paradox lurking when it comes to breaking into and spying on third party networks: How can intelligence services be sure that they won't become victims of their own methods and be infiltrated by private hackers, criminals or other intelligence services, for example?

To control their malware, the Remote Operation Center operatives remain connected to them via their own shadow network, through which highly sensitive telephone recordings, malware programs and passwords travel.

The incentive to break into this network is enormous. Any collection of VPN keys, passwords and backdoors is obviously of very high value. Those who possess such passwords and keys could theoretically pillage bank accounts, thwart military deployments, clone fighter jets and shut down power plants. It means nothing less than "global network dominance".

But the intelligence world is a schizophrenic one. The NSA's job is to defend the Internet while at the same time exploiting its security holes. It is both cop and robber, consistent with the motto adhered to by spies everywhere: "Reveal their secrets, protect our own."

As a result, some hacked servers are like a bus during rush hour, with people constantly coming and going. The difference, though, is that the server's owner has no idea anyone is there. And the presumed authorities stand aside and do nothing.

'Unwitting Data Mules'

It's absurd: As they are busy spying, the spies are spied on by other spies. In response, they routinely seek to cover their tracks or to lay fake ones instead. In technical terms, the ROC lays false tracks as follows: After third-party computers are infiltrated, the process of exfiltration can begin -- the act of exporting the data that has been gleaned. But the loot isn't delivered directly to ROC's IP address. Rather, it is routed to a so-called Scapegoat Target. That means that stolen information could end up on someone else's servers, making it look as though they were the perpetrators.

Before the data ends up at the Scapegoat Target, of course, the NSA intercepts and copies it using its mass surveillance infrastructure and sends it on to the ROC. But such cover-up tactics increase the risk of a controlled or uncontrolled escalation between the agencies involved.

It's not just computers, of course, that can be systematically broken into, spied on or misused as part of a botnet. Mobile phones can also be used to steal information from the owner's employer. The unwitting victim, whose phone has been infected with a spy program, smuggles the information out of the office. The information is then retrieved remotely as the victim heads home after work. Digital spies have even adopted drug-dealer slang in referring to these unsuspecting accomplices. They are called "unwitting data mules."

NSA agents aren't concerned about being caught. That's partly because they work for such a powerful agency, but also because they don't leave behind any evidence that would hold up in court. And if there is no evidence of wrongdoing, there can be no legal penalty, no parliamentary control of intelligence agencies and no international agreement. Thus far, very little is known about the risks and side-effects inherent in these new D weapons and there is almost no government regulation.

Edward Snowden has revealed how intelligence agencies around the world, led by the NSA, are doing their best to ensure a legal vacuum in the Internet. In a recent interview with the US public broadcaster PBS, the whistleblower voiced his concerns that "defense is becoming less of a priority than offense."

Snowden finds that concerning. "What we need to do," he said, "is we need to create new international standards of behavior."

By Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt and Michael Sontheimer.