The Washington Post

SATURDAY, AUGUST 31, 2013

‘Black budget’ details a war in cyberspace

U.S. intelligence services carried out 231 offensive operations in 2011

BY BARTON GELLMAN
AND ELLEN NAKASHIMA

U.S. intelligence services carried out 231 offensive cyber-operations in 2011, the leading edge of a clandestine campaign that embraces the Internet as a theater of spying, sabotage and war, according to top-secret documents obtained by The Washington Post.

That disclosure, in a classified intelligence budget provided by NSA leaker Edward Snowden, provides new evidence that the Obama administration’s growing ranks of cyberwarriors infiltrate and disrupt foreign computer networks.

Additionally, under an extensive effort code-named GENIE, U.S. computer specialists break into foreign networks so that they can be put under surreptitious U.S. control. Budget documents say the $652 million project has placed “covert implants,” sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions.

The documents provided by Snowden and interviews with former U.S. officials describe a campaign of computer intrusions that is far broader and more aggressive than previously understood. The Obama administration treats all such cyber-operations as clandestine and declines to acknowledge them.

The scope and scale of offensive operations represent an evolution in policy, which in the past sought to preserve an international norm against acts of aggression in cyberspace, in part because U.S. economic and military power depend so heavily on computers.

“The policy debate has moved so that offensive options are more prominent now,” said former deputy defense secretary William J. Lynn III, who has not seen the budget document and was speaking generally. “I think there’s more of a case made now that offensive cyberoptions can be an important element in deterring certain adversaries.”

Of the 231 offensive operations conducted in 2011, the budget said, nearly three-quarters were against top-priority targets, which former officials say includes adversaries such as Iran, Russia, China and North Korea and activities such as nuclear proliferation. The document provided few other details about the operations.

Stuxnet, a computer worm reportedly developed by the United States and Israel that destroyed Iranian nuclear centrifuges in attacks in 2009 and 2010, is often cited as the most dramatic use of a cyberweapon. Experts said no other known cyberattacks carried out by the United States match the physical damage inflicted in that case.

U.S. agencies define offensive cyber-operations as activities intended “to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves,” according to a presidential directive issued in October 2012.

Most offensive operations have immediate effects only on data or the proper functioning of an adversary’s machine: slowing its network connection, filling its screen with static or scrambling the results of basic calculations. Any of those could have powerful effects if they caused an adversary to botch the timing of an attack, lose control of a computer or miscalculate locations.

U.S. intelligence services are making routine use around the world of government-built malware that differs little in function from the "advanced persistent threats" that U.S. officials attribute to China. The principal difference, U.S. officials told The Post, is that China steals U.S. corporate secrets for financial gain.

"The Department of Defense does engage" in computer network exploitation, according to an e-mailed statement from an NSA spokesman, whose agency is part of the Defense Department. "The department does ***not*** engage in economic espionage in any domain, including cyber."

'Millions of implants'

The administration's cyber-operations sometimes involve what one budget document calls "field operations" abroad, commonly with the help of CIA operatives or clandestine military forces, "to physically place hardware implants or software modifications."

Much more often, an implant is coded entirely in software by an NSA group called Tailored Access Operations (TAO). As its name suggests, TAO builds attack tools that are custom-fitted to their targets.

The NSA unit's software engineers would rather tap into networks than individual computers because there are usually many devices on each network. Tailored Access Operations has software templates to break into common brands and models of "routers, switches and firewalls from multiple product vendor lines," according to one document describing its work.

The implants that TAO creates are intended to persist through software and equipment upgrades, to copy stored data, "harvest" communications and tunnel into other connected networks. This year TAO is working on implants that "can identify select voice conversations of interest within a target network and exfiltrate select cuts," or excerpts, according to one budget document. In some cases, a single compromised device opens the door to hundreds or thousands of others.

Sometimes an implant's purpose is to create a back door for future access. "You pry open the window somewhere and leave it so when you come back the owner doesn't know it's unlocked, but you can get back in when you want to," said one intelligence official, who was speaking generally about the topic and was not privy to the budget. The official spoke on the condition of anonymity to discuss sensitive technology.

Under U.S. cyberdoctrine, these operations are known as "exploitation," not "attack," but they are essential precursors both to attack and defense.

By the end of this year, GENIE is projected to control at least 85,000 implants in strategically chosen machines around the world. That is quadruple the number — 21,252 — available in 2008, according to the U.S. intelligence budget.

The NSA appears to be planning a rapid expansion of those numbers, which were limited until recently by the need for human operators to take remote control of compromised machines. Even with a staff of 1,870 people, GENIE made full use of only 8,448 of the 68,975 machines with active implants in 2011.

For GENIE's next phase, according to an authoritative reference document, the NSA has brought online an automated system, code-named TURBINE, that is capable of managing "potentially millions of implants" for intelligence gathering "and active attack."

'The ROC'

When it comes time to fight the cyberwar against the best of the NSA's global competitors, the TAO calls in its elite operators, who work at the agency's Fort Meade headquarters and in regional operations centers in Georgia, Texas, Colorado and Hawaii. The NSA's organizational chart has the main office as S321. Nearly everyone calls it "the ROC," pronounced "rock": the Remote Operations Center.

"To the NSA as a whole, the ROC is where the hackers live," said a former operator from another section who has worked closely with the exploitation teams. "It's basically the one-stop shop for any kind of active operation that's not defensive."

Once the hackers find a hole in an adversary's defense, "[t]argeted systems are compromised electronically, typically providing access to system functions as well as data. System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals," according to a 570-page budget blueprint for what the government calls its Consolidated Cryptologic Program, which includes the NSA.

Teams from the FBI, the CIA and U.S. Cyber Command work alongside the ROC, with overlapping missions and legal authorities. So do the operators from the NSA's National Threat Operations Center, whose mission is focused primarily on cyberdefense. That was Snowden's job as a Booz Allen Hamilton contractor, and it required him to learn the NSA's best hacking techniques.

According to one key document, the ROC teams give Cyber Command "specific target related technical and operational material (identification/recognition), tools and techniques that allow the employment of U.S. national and tactical specific computer network attack mechanisms."

The intelligence community's cybermissions include defense of military and other classified computer networks against foreign attack, a task that absorbs roughly one-third of a total cyber operations budget of $1.02 billion in fiscal 2013, according to the Cryptologic Program budget. The ROC's breaking-and-entering mission, supported by the GENIE infrastructure, spends nearly twice as much: $651.7 million.

Most GENIE operations aim for "exploitation" of foreign systems, a term defined in the intelligence budget summary as "surreptitious virtual or physical access to create and sustain a presence inside targeted systems or facilities." The document adds: "System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals."

The NSA designs most of its own implants, but it devoted $25.1 million this year to "additional covert purchases of software vulnerabilities" from private malware vendors, a growing gray-market industry based largely in Europe.

'Most challenging targets'

The budget documents cast U.S. attacks as integral to cyberdefense — describing them in some cases as "active defense."

"If you're neutralizing someone's nuclear command and control, that's a huge attack," said one former defense official. The greater the physical effect, officials said, the less likely it is that an intrusion can remain hidden.

"The United States is moving toward the use of tools short of traditional weapons that are unattributable — that cannot be easily tied to the attacker — to convince an adversary to change their behavior at a strategic level," said another former senior U.S. official, who also spoke on the condition of anonymity to discuss sensitive operations.

China and Russia are regarded as the most formidable cyberthreats, and it is not

> ***"The United States is moving toward the use of tools short of traditional weapons that are unattributable – that cannot be easily tied to the attacker – to convince an adversary to change their behavior at a strategic level."***
>
> **A former senior U.S. official**, speaking on the condition of anonymity to discuss sensitive operations

always easy to tell who works for whom. China's offensive operations are centered in the Technical Reconnaissance Bureau of the People's Liberation Army, but U.S. intelligence has come to believe that those state-employed hackers by day return to work at night for personal profit, stealing valuable U.S. defense industry secrets and selling them.

Iran is a distant third in capability but is thought to be more strongly motivated to retaliate for Stuxnet with an operation that would not only steal information but erase it and attempt to damage U.S. hardware.

The "most challenging targets" to penetrate are the same in cyber-operations as for all other forms of data collection described in the intelligence budget: Iran, North Korea, China and Russia. GENIE and ROC operators place special focus on locating suspected terrorists "in Afghanistan, Pakistan, Yemen, Iraq, Somalia, and other extremist safe havens," according to one list of priorities.

The growth of Tailored Access Operations at the NSA has been accompanied by a major expansion of the CIA's Information Operations Center, or IOC.

The CIA unit employs hundreds of people at facilities in Northern Virginia and has become one of the CIA's largest divisions. Its primary focus has shifted in recent years from counterterrorism to cybersecurity, according to the budget document.

The military's cyber-operations, including U.S. Cyber Command, have drawn much of the public's attention, but the IOC undertakes some of the most notable offensive operations, including the recruitment of several new intelligence sources, the document said.

Military cyber-operations personnel grouse that the actions they can take are constrained by the legal authorities that govern them. The presidential policy directive on cyber-operations issued in October made clear that military cyber-operations that result in the disruption or destruction or even manipulation of computers must be approved by the president. But the directive, the existence of which was first reported last fall by The Post and leaked in June by Snowden, largely does not apply to the intelligence community.

Given the "vast volumes of data" pulled in by the NSA, storage has become a pressing question. The NSA is nearing completion of a massive new data center in Utah. A second one will be built at Fort Meade "to keep pace with cyber processing demands," the budget document said.

According to the document, a high-performance computing center in Utah will manage "storage, analysis, and intelligence production." This will allow intelligence agencies "to evaluate similarities among intrusions that could indicate the presence of a coordinated cyber attack, whether from an organized criminal enterprise or a nation-state."

bart.gellman@washpost.com
ellen.nakashima@washpost.com