Bloomberg Businessweek

Technology

How the U.S. Government Hacks the World

By Michael Riley on May 23, 2013
http://www.businessweek.com/articles/2013-05-23/how-the-u-dot-s-dot-government-hacks-the-world

Obscured by trees and grassy berms, the campus of the National Security Agency sits 15 miles north of Washington's traffic-clogged Beltway, its 6 million square feet of blast-resistant buildings punctuated by clusters of satellite dishes. Created in 1952 to intercept radio and other electronic transmissions—known as signals intelligence—the NSA now focuses much of its espionage resources on stealing what spies euphemistically call "electronic data at rest." These are the secrets that lay inside the computer networks and hard drives of terrorists, rogue nations, and even nominally friendly governments. When President Obama receives his daily intelligence briefing, most of the information comes from government cyberspies, says Mike McConnell, director of national intelligence under President George W. Bush. "It's at least 75 percent, and going up," he says.

The key role NSA hackers play in intelligence gathering makes it difficult for Washington to pressure other nations—China in particular—to stop hacking U.S. companies to mine their databanks for product details and trade secrets. In recent months the Obama administration has tried to shame China by publicly calling attention to its cyber-espionage program, which has targeted numerous companies, including Google (GOOG), Yahoo! (YHOO), and Intel (INTC), to steal source code and other secrets. This spring, U.S. Treasury Secretary Jacob Lew and General Martin Dempsey, chairman of the Joint Chiefs of Staff, traveled to Beijing to press Chinese officials about the hacking. National Security Advisor Thomas Donilon is scheduled to visit China on May 26.

Illustration by James Dawe; Getty Images

(18)

The Chinese response, essentially: Look who's talking. "You go in there, you sit across from your counterpart and say, 'You spy, we spy, but you just steal the wrong stuff.' That's a hard conversation," says Michael Hayden, who headed the NSA, and later the CIA, under Bush. "States spying on states, I got that," says Hayden, now a principal at the Chertoff Group, a Washington security consulting firm. "But this isn't that competition. This is a nation-state attempting espionage on private corporations. That is not an even playing field."

The tension between the two nations escalated in May, when a Pentagon report to Congress for the first time officially linked China's government directly to the hacking of U.S. defense contractors. It revealed that U.S. intelligence had been tracking a vast hacking bureaucracy adept at stealing technology from American companies. China's leaders have long denied being behind the hacks. An article about the Pentagon report in the official People's Daily newspaper called the U.S. the "real hacking empire."

The U.S. government doesn't deny that it engages in cyber espionage. "You're not waiting for someone to decide to turn information into electrons and photons and send it," says Hayden. "You're commuting to where the information is stored and extracting the information from the adversaries' network. We are the best at doing it. Period." The U.S. position is that some kinds of hacking are more acceptable than others—and the kind the NSA does is in keeping with unofficial, unspoken rules going back to the Cold War about what secrets are OK for one country to steal from another. "China is doing stuff you're not supposed to do," says Jacob Olcott, a principal at Good Harbor Security Risk Management, a Washington firm that advises hacked companies.

The men and women who hack for the NSA belong to a secretive unit known as Tailored Access Operations. It gathers vast amounts of intelligence on terrorist financial networks, international money-laundering and drug operations, the readiness of foreign militaries, even the internal political squabbles of potential adversaries, according to two former U.S. government security officials, who asked not to be named when discussing foreign intelligence gathering. For years, the NSA wouldn't acknowledge TAO's existence. A Pentagon official who also asked not to be named confirmed that TAO conducts cyber espionage, or what the Department of Defense calls "computer network exploitation," but emphasized that it doesn't target technology, trade, or financial secrets. The official says the number of people who work for TAO is classified. NSA spokeswoman Vaneé Vines would not answer questions about the unit.

The two former security officials agreed to describe the operation and its activities without divulging which governments or entities it targets. According to the former officials, U.S. cyberspies, most from military units who've received specialized training, sit at consoles running sophisticated hacking software, which funnels information stolen from computers around the world into a "fusion center," where intelligence analysts try to make sense of it all. The NSA is prohibited by law from spying on people or entities within the U.S., including noncitizens, or on U.S. citizens abroad. According to one of the former officials, the amount of data the unit harvests from overseas computer networks, or as it travels across the Internet, has grown to an astonishing 2 petabytes an hour—that's nearly 2.1 million gigabytes, the equivalent of hundreds of millions of pages of text.

The agency has managed to automate much of the process, one of the former officials says, requiring human hackers to intervene only in cases of the most well-protected computers. Just like spies in the physical world, the U.S. cyberspies take pains to obscure their tracks or disguise themselves as something else—hackers from China, say—in case their activities are detected.

Even as the rest of the Pentagon budget shrinks, the importance of the NSA's hacking operations has helped create a booming cyber-industrial complex. Specialized units of big defense contractors, and boutique firms that create hacking tools, look for security flaws in popular software programs that allow government hackers to take over computers. A company called KEYW does a robust business training hackers for U.S. intelligence, says Chief Executive Officer Leonard Moodispaw, who cautions that he can't reveal more. "Our federal partners don't like it if we're too explicit."

All this activity gives China leverage against Washington's complaints, says Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists. Beijing can turn U.S. protests about industrial espionage around and claim that Washington is doing something even worse. "It's OK to steal plans for a new automobile," Aftergood says the Chinese can argue, "but not our national secrets."

Intelligence officials say one way to exert pressure on China is to change the subject from spying to trade—threatening restrictions on imports of goods made using stolen technology, or withholding visas for employees of companies that make such products. "We don't have to get into a philosophical argument about what does and does not constitute accepted espionage," says Hayden. Instead, the U.S. should focus on reducing China's incentives for "committing the original crime—and that's economic."

In February the Obama administration said it may consider sanctions on countries that permit thefts of corporate information. Such punishments would be difficult to implement in practice, says Christopher Finan, a cybersecurity expert who served on Obama's National Security Council until last year. "It's just too hard to determine whether a product uses stolen technology, or is an enhancement," he says. "The current enforcement of intellectual-property protections is a mess without adding this."

Finan believes aggressive sanctions could result in little more than a trade war, hurting many of the same U.S. companies and products they were intended to protect. "China is already looking for ways to constrain U.S. companies in the domestic market," he says. "This would give it to them."

The bottom line: *Using automated hacking tools, NSA cyberspies pilfer 2 petabytes of data every hour from computers worldwide.*