The New York Times | https://nyti.ms/2jlglTa

Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core

A serial leak of the agency's cyberweapons has damaged morale, slowed intelligence operations and resulted in hacking attacks on businesses and civilians worldwide.

By SCOTT SHANE, NICOLE PERLROTH and DAVID E. SANGER NOV. 12, 2017

WASHINGTON — Jake Williams awoke last April in an Orlando, Fla., hotel where he was leading a training session. Checking Twitter, Mr. Williams, a cybersecurity expert, was dismayed to discover that he had been thrust into the middle of one of the worst security debacles ever to befall American intelligence.

Mr. Williams had written on his company blog about the Shadow Brokers, a mysterious group that had somehow obtained many of the hacking tools the United States used to spy on other countries. Now the group had replied in an angry screed on Twitter. It identified him — correctly — as a former member of the National Security Agency's hacking group, Tailored Access Operations, or T.A.O., a job he had not publicly disclosed. Then the Shadow Brokers astonished him by dropping technical details that made clear they knew about highly classified hacking operations that he had conducted.

America's largest and most secretive intelligence agency had been deeply infiltrated.

"They had operational insight that even most of my fellow operators at T.A.O. did not have," said Mr. Williams, now with Rendition Infosec, a cybersecurity firm he founded. "I felt like I'd been kicked in the gut. Whoever wrote this either was a well-placed insider or had stolen a lot of operational data."

The jolt to Mr. Williams from the Shadow Brokers' riposte was part of a much broader earthquake that has shaken the N.S.A. to its core. Current and former agency officials say the Shadow Brokers disclosures, which began in August 2016, have been catastrophic for the N.S.A., calling into question its ability to protect potent cyberweapons and its very value to national security. The agency regarded as the world's leader in breaking into adversaries' computer networks failed to protect its own.

"These leaks have been incredibly damaging to our intelligence and cyber capabilities," said Leon E. Panetta, the former defense secretary and director of the Central Intelligence Agency. "The fundamental purpose of intelligence is to be able to effectively penetrate our adversaries in order to gather vital intelligence. By its very nature, that only works if secrecy is maintained and our codes are protected."

With a leak of intelligence methods like the N.S.A. tools, Mr. Panetta said, "Every time it happens, you essentially have to start over."

Fifteen months into a wide-ranging investigation by the agency's counterintelligence arm, known as Q Group, and the F.B.I., officials still do not know whether the N.S.A. is the victim of a brilliantly executed hack, with Russia as the most likely perpetrator, an insider's leak, or both. Three employees have been arrested since 2015 for taking classified files, but there is fear that one or more leakers may still be in place. And there is broad agreement that the damage from the Shadow Brokers already far exceeds the harm to American intelligence done by Edward J. Snowden, the former N.S.A. contractor who fled with four laptops of classified material in 2013.

Mr. Snowden's cascade of disclosures to journalists and his defiant public stance drew far more media coverage than this new breach. But Mr. Snowden released code words, while the Shadow Brokers have released the actual code; if he shared what might be described as battle plans, they have loosed the weapons themselves. Created at huge expense to American taxpayers, those cyberweapons have now been picked up by hackers from North Korea to Russia and shot back at the United States and its allies.

Millions of people saw their computers shut down by ransomware, with demands for payments in digital currency to have their access restored. Tens of

thousands of employees at Mondelez International, the maker of Oreo cookies, had their data completely wiped. FedEx reported that an attack on a European subsidiary had halted deliveries and cost $300 million. Hospitals in Pennsylvania, Britain and Indonesia had to turn away patients. The attacks disrupted production at a car plant in France, an oil company in Brazil and a chocolate factory in Tasmania, among thousands of enterprises affected worldwide.

American officials had to explain to close allies — and to business leaders in the United States — how cyberweapons developed at Fort Meade in Maryland came to be used against them. Experts believe more attacks using the stolen N.S.A. tools are all but certain.

Inside the agency's Maryland headquarters and its campuses around the country, N.S.A. employees have been subjected to polygraphs and suspended from their jobs in a hunt for turncoats allied with the Shadow Brokers. Much of the agency's arsenal is still being replaced, curtailing operations. Morale has plunged, and experienced specialists are leaving the agency for better-paying jobs — including with firms defending computer networks from intrusions that use the N.S.A.'s leaked tools.

"It's a disaster on multiple levels," Mr. Williams said. "It's embarrassing that the people responsible for this have not been brought to justice."

In response to detailed questions, an N.S.A. spokesman, Michael T. Halbig, said the agency "cannot comment on Shadow Brokers." He denied that the episode had hurt morale. "N.S.A. continues to be viewed as a great place to work; we receive more than 140,000 applications each year for our hiring program," he said.

Compounding the pain for the N.S.A. is the attackers' regular online public taunts, written in ersatz broken English. Their posts are a peculiar mash-up of immaturity and sophistication, laced with profane jokes but also savvy cultural and political references. They suggest that their author — if not an American — knows the United States well.

"Is NSA chasing shadowses?" the Shadow Brokers asked in a post on Oct. 16, mocking the agency's inability to understand the leaks and announcing a price cut for subscriptions to its "monthly dump service" of stolen N.S.A. tools. It was a

typically wide-ranging screed, touching on George Orwell's "1984"; the end of the federal government's fiscal year on Sept. 30; Russia's creation of bogus accounts on Facebook and Twitter; and the phenomenon of American intelligence officers going to work for contractors who pay higher salaries.

One passage, possibly hinting at the Shadow Brokers' identity, underscored the close relationship of Russian intelligence to criminal hackers. "Russian security peoples," it said, "is becoming Russian hackeres at nights, but only full moons."

Russia is the prime suspect in a parallel hemorrhage of hacking tools and secret documents from the C.I.A.'s Center for Cyber Intelligence, posted week after week since March to the WikiLeaks website under the names Vault7 and Vault8. That breach, too, is unsolved. Together, the flood of digital secrets from agencies that invest huge resources in preventing such breaches is raising profound questions.

Have hackers and leakers made secrecy obsolete? Has Russian intelligence simply outplayed the United States, penetrating the most closely guarded corners of its government? Can a work force of thousands of young, tech-savvy spies ever be immune to leaks?

Some veteran intelligence officials believe a lopsided focus on offensive weapons and hacking tools has, for years, left American cyberdefense dangerously porous.

"We have had a train wreck coming," said Mike McConnell, the former N.S.A. director and national intelligence director. "We should have ratcheted up the defense parts significantly."

America's Cyber Special Forces

At the heart of the N.S.A. crisis is Tailored Access Operations, the group where Mr. Williams worked, which was absorbed last year into the agency's new Directorate of Operations.

T.A.O. — the outdated name is still used informally — began years ago as a side project at the agency's research and engineering building at Fort Meade. It was a cyber Skunk Works, akin to the special units that once built stealth aircraft

and drones. As Washington's need for hacking capabilities grew, T.A.O. expanded into a separate office park in Laurel, Md., with additional teams at facilities in Colorado, Georgia, Hawaii and Texas.

The hacking unit attracts many of the agency's young stars, who like the thrill of internet break-ins in the name of national security, according to a dozen former government officials who agreed to describe its work on the condition of anonymity. T.A.O. analysts start with a shopping list of desired information and likely sources — say, a Chinese official's home computer or a Russian oil company's network. Much of T.A.O.'s work is labeled E.C.I., for "exceptionally controlled information," material so sensitive it was initially stored only in safes. When the cumulative weight of the safes threatened the integrity of N.S.A.'s engineering building a few years ago, one agency veteran said, the rules were changed to allow locked file cabinets.

The more experienced T.A.O. operators devise ways to break into foreign networks; junior operators take over to extract information. Mr. Williams, 40, a former paramedic who served in military intelligence in the Army before joining the N.S.A., worked in T.A.O. from 2008 to 2013, which he described as an especially long tenure. He called the work "challenging and sometimes exciting."

T.A.O. operators must constantly renew their arsenal to stay abreast of changing software and hardware, examining every Windows update and new iPhone for vulnerabilities. "The nature of the business is to move with the technology," a former T.A.O. hacker said.

Long known mainly as an eavesdropping agency, the N.S.A. has embraced hacking as an especially productive way to spy on foreign targets. The intelligence collection is often automated, with malware implants — computer code designed to find material of interest — left sitting on the targeted system for months or even years, sending files back to the N.S.A.

The same implant can be used for many purposes: to steal documents, tap into email, subtly change data or become the launching pad for an attack. T.A.O.'s most public success was an operation against Iran called Olympic Games, in which implants in the network of the Natanz nuclear plant caused centrifuges enriching uranium to self-destruct. The T.A.O. was also critical to attacks on the Islamic State and North Korea.

It was this arsenal that the Shadow Brokers got hold of, and then began to release.

Like cops studying a burglar's operating style and stash of stolen goods, N.S.A. analysts have tried to figure out what the Shadow Brokers took. None of the leaked files date from later than 2013 — a relief to agency officials assessing the damage. But they include a large share of T.A.O.'s collection, including three so-called ops disks — T.A.O.'s term for tool kits — containing the software to bypass computer firewalls, penetrate Windows and break into the Linux systems most commonly used on Android phones.

Evidence shows that the Shadow Brokers obtained the entire tool kits intact, suggesting that an insider might have simply pocketed a thumb drive and walked out.

But other files obtained by the Shadow Brokers bore no relation to the ops disks and seem to have been grabbed at different times. Some were designed for a compromise by the N.S.A. of Swift, a global financial messaging system, allowing the agency to track bank transfers. There was a manual for an old system code-named UNITEDRAKE, used to attack Windows. There were PowerPoint presentations and other files not used in hacking, making it unlikely that the Shadow Brokers had simply grabbed tools left on the internet by sloppy N.S.A. hackers.

Some officials doubt that the Shadow Brokers got it all by hacking the most secure of American government agencies — hence the search for insiders. But some T.A.O. hackers think that skilled, persistent attackers might have been able to get through the N.S.A.'s defenses — because, as one put it, "I know we've done it to other countries."

The Shadow Brokers have verbally attacked certain experts, including Mr. Williams. When he concluded from their Twitter hints that they knew about some of his hacks while at the N.S.A., he canceled a business trip to Singapore. The United States had named and criminally charged hackers from the intelligence agencies of China, Iran and Russia. He feared he could be similarly charged by a country he had targeted and arrested on an international warrant.

He has since resumed traveling abroad. But he says no one from the N.S.A. has contacted him about being singled out publicly by the Shadow Brokers.

"That feels like a betrayal," he said. "I was targeted by the Shadow Brokers because of that work. I do not feel the government has my back."

The Hunt for an Insider

For decades after its creation in 1952, the N.S.A. — No Such Agency, in the old joke — was seen as all but leakproof. But since Mr. Snowden flew away with hundreds of thousands of documents in 2013, that notion has been shattered.

The Snowden trauma led to the investment of millions of dollars in new technology and tougher rules to counter what the government calls the insider threat. But N.S.A. employees say that with thousands of employees pouring in and out of the gates, and the ability to store a library's worth of data in a device that can fit on a key ring, it is impossible to prevent people from walking out with secrets.

The agency has active investigations into at least three former N.S.A. employees or contractors. Two had worked for T.A.O.: a still publicly unidentified software developer secretly arrested after taking hacking tools home in 2015, only to have Russian hackers lift them from his home computer; and Harold T. Martin III, a contractor arrested last year when F.B.I. agents found his home, garden shed and car stuffed with sensitive agency documents and storage devices he had taken over many years when a work-at-home habit got out of control, his lawyers say. The third is Reality Winner, a young N.S.A. linguist arrested in June, who is charged with leaking to the news site The Intercept a single classified report on a Russian breach of an American election systems vendor.

Mr. Martin's gargantuan collection of stolen files included much of what the Shadow Brokers have, and he has been scrutinized by investigators as a possible source for them. Officials say they do not believe he deliberately supplied the material, though they have examined whether he might have been targeted by thieves or hackers.

But according to former N.S.A. employees who are still in touch with active workers, investigators of the Shadow Brokers thefts are clearly worried that one or more leakers may still be inside the agency. Some T.A.O. employees have been asked to turn over their passports, take time off their jobs and submit to questioning. The small number of specialists who have worked both at T.A.O. and

at the C.I.A. have come in for particular attention, out of concern that a single leaker might be responsible for both the Shadow Brokers and the C.I.A.'s Vault7 breaches.

Then there are the Shadow Brokers' writings, which betray a seeming immersion in American culture. Last April, about the time Mr. Williams was discovering their inside knowledge of T.A.O. operations, the Shadow Brokers posted an appeal to President Trump: "Don't Forget Your Base." With the ease of a seasoned pundit, they tossed around details about Stephen K. Bannon, the president's now departed adviser; the Freedom Caucus in Congress; the "deep state"; the Alien and Sedition Acts; and white privilege.

"TheShadowBrokers is wanting to see you succeed," the post said, addressing Mr. Trump. "TheShadowBrokers is wanting America to be great again."

The mole hunt is inevitably creating an atmosphere of suspicion and anxiety, former employees say. While the attraction of the N.S.A. for skilled operators is unique — nowhere else can they hack without getting into legal trouble — the boom in cybersecurity hiring by private companies gives T.A.O. veterans lucrative exit options.

Young T.A.O. hackers are lucky to make $80,000 a year, while those who leave routinely find jobs paying well over $100,000, security specialists say. For many workers, the appeal of the N.S.A's mission has been more than enough to make up the difference. But over the past year, former T.A.O. employees say an increasing number of former colleagues have called them looking for private-sector work, including "graybeards" they thought would be N.S.A. lifers.

"Snowden killed morale," another T.A.O. analyst said. "But at least we knew who he was. Now you have a situation where the agency is questioning people who have been 100 percent mission-oriented, telling them they're liars."

Because the N.S.A. hacking unit has grown so rapidly over the past decade, the pool of potential leakers has expanded into the hundreds. Trust has eroded as anyone who had access to the leaked code is regarded as the potential culprit.

Some agency veterans have seen projects they worked on for a decade shut down because implants they relied on were dumped online by the Shadow

Brokers. The number of new operations has declined because the malware tools must be rebuilt. And no end is in sight.

"How much longer are the releases going to come?" a former T.A.O. employee asked. "The agency doesn't know how to stop it — or even what 'it' is."

One N.S.A. official who almost saw his career ended by the Shadow Brokers is at the very top of the organization: Adm. Michael S. Rogers, director of the N.S.A. and commander of its sister military organization, United States Cyber Command. President Barack Obama's director of national intelligence, James R. Clapper Jr., and defense secretary, Ashton B. Carter, recommended removing Admiral Rogers from his post to create accountability for the breaches.

But Mr. Obama did not act on the advice, in part because Admiral Rogers's agency was at the center of the investigation into Russia's interference in the 2016 election. Mr. Trump, who again on Saturday disputed his intelligence agencies' findings on Russia and the election, extended the admiral's time in office. Some former intelligence officials say they are flabbergasted that he has been able to hold on to his job.

A Shadow War With Russia?

Lurking in the background of the Shadow Brokers investigation is American officials' strong belief that it is a Russian operation. The pattern of dribbling out stolen documents over many months, they say, echoes the slow release of Democratic emails purloined by Russian hackers last year.

But there is a more specific back story to the United States-Russia rivalry.

Starting in 2014, American security researchers who had been tracking Russia's state-sponsored hacking groups for years began to expose them in a series of research reports. American firms, including Symantec, CrowdStrike and FireEye, reported that Moscow was behind certain attacks and identified government-sponsored Russian hacking groups.

In the meantime, Russia's most prominent cybersecurity firm, Kaspersky Lab, had started work on a report that would turn the tables on the United States. Kaspersky hunted for the spying malware planted by N.S.A. hackers, guided in

part by the keywords and code names in the files taken by Mr. Snowden and published by journalists, officials said.

Kaspersky was, in a sense, simply doing to the N.S.A. what the American companies had just done to Russian intelligence: expose their operations. And American officials believe Russian intelligence was piggybacking on Kaspersky's efforts to find and retrieve the N.S.A.'s secrets wherever they could be found. The T.A.O. hackers knew that when Kaspersky updated its popular antivirus software to find and block the N.S.A. malware, it could thwart spying operations around the world.

So T.A.O. personnel rushed to replace implants in many countries with new malware they did not believe the Russian company could detect.

In February 2015, Kaspersky published its report on the Equation Group — the company's name for T.A.O. hackers — and updated its antivirus software to uproot the N.S.A. malware wherever it had not been replaced. The agency temporarily lost access to a considerable flow of intelligence. By some accounts, however, N.S.A. officials were relieved that the Kaspersky report did not include certain tools they feared the Russian company had found.

As it would turn out, any celebration was premature.

On Aug. 13 last year, a new Twitter account using the Shadow Brokers' name announced with fanfare an online auction of stolen N.S.A. hacking tools.

"We hack Equation Group," the Shadow Brokers wrote. "We find many many Equation Group cyber weapons."

Inside the N.S.A., the declaration was like a bomb exploding. A zip file posted online contained the first free sample of the agency's hacking tools. It was immediately evident that the Shadow Brokers were not hoaxsters, and that the agency was in trouble.

The leaks have renewed a debate over whether the N.S.A. should be permitted to stockpile vulnerabilities it discovers in commercial software to use for spying — rather than immediately alert software makers so the holes can be plugged. The agency claims it has shared with the industry more than 90 percent of flaws it has found, reserving only the most valuable for its own hackers. But if it

can't keep those from leaking, as the last year has demonstrated, the resulting damage to businesses and ordinary computer users around the world can be colossal. The Trump administration says it will soon announce revisions to the system, making it more transparent.

Mr. Williams said it may be years before the "full fallout" of the Shadow Brokers breach is understood. Even the arrest of whoever is responsible for the leaks may not end them, he said — because the sophisticated perpetrators may have built a "dead man's switch" to release all remaining files automatically upon their arrest.

"We're obviously dealing with people who have operational security knowledge," he said. "They have the whole law enforcement system and intelligence system after them. And they haven't been caught."

A version of this article appears in print on November 13, 2017, on Page A1 of the New York edition with the headline: Deep Security Breach Cripples N.S.A.
