Hiring Hackers

The federal government turns to the underworld of computer cowboys for help shoring up its cyber defenses.

When hackers convene at their annual conferences, they play a game called Spot the Fed. The rules are simple. If you think you see a federal employee walking the halls, point the person out to your colleagues around you. This might, or might not, trigger a storm of controversy or some nervous laughter. If your fed radar proves keen enough, you win a free shirt that reads, "I spotted the fed!" The person identified gets an "I am the fed!" shirt.

The tradition started in 1990s, when the purpose was to duck from snooping law enforcement officials and avoid being detained. Today, hackers play the game mostly as a gag, a parody of their cat-and-mouse relationship with the buttoned-down »

BY DAWN LIM ILLUSTRATION BY ANTHONY TREMMAGLIA

establishment that used to haunt them at get-togethers like Black Hat, a weeklong gathering of phone phreaks, ham operators and hackers before it became professionalized, and DEF CON, a computer underground confab that is the more radical and freewheeling cousin of Black Hat.

And how has it changed for the feds? They aren't crashing the parties to infiltrate the hacker population anymore, at least most aren't. They're at these meetings to do some, pardon the pun, networking and to ask for help.

When Michael Hayden, former CIA director and ex-chief of the National Security Agency, was invited to give the keynote speech at the 2010 Black Hat conference in Las Vegas on July 29, he spoke about the fragile state of cybersecurity. "We all get treated like Poland on the Web, invaded from the West on even-numbered centuries, invaded from the East on odd-numbered centuries," he said. His statements were an overture to the hacking community to help secure the Internet. "Rivers, hills and mountains become a military officer's friend," because they make it difficult for networks to be penetrated, he said. "You're going to build the rivers and hills into the Web. You're going to create geography that is going to help the defense."

At the same time, representatives from the Defense Department's newly founded Cyber Command were making their rounds at the conference and at DEF CON, held right after Black Hat at the nearby Riveria Hotel and Casino, to check out the latest tricks the hacking community has up its sleeve.

Army Col. Rivers Johnson, a spokesman for the Cyber Command, explained their presence this way: "As we are a new organization, Cyber Command considers these venues important because we are always interested in the technology that may be available at these conferences." He wouldn't state on the record that representatives from the command were there recruiting possible cyberwarriors, but he did say the organization was hoping to do some networking.

The federal government needs help. More than 100 foreign intelligence organizations are trying to break into the networks that undergird U.S. military operations, Deputy Secretary of Defense William J. Lynn III wrote in the August edition of *Foreign Affairs*. Size doesn't work to the federal government's advantage when it comes to cyber defense. The multitude of platforms increases the risk of cyberattacks. "These are really big networks that were built a long time ago, and it's really difficult to move the foundation of buildings that are in use," says Dino Dai Zovi, an independent security researcher and former security analyst at Sandia National Laboratories.

GOOD WORK **If hackers have shown the capacity to do evil but chose not to, then the government should sign them on, says James Gosler, a scientist and IT specialist.**

JAMES KEGLEY

To plug the holes in its networks, the federal government is pouring billions of dollars annually into protecting its systems. A report the Center for Strategic and International Studies released in July highlighted a "desperate shortage" of people who could create tools sophisticated enough to guard systems against threats. There are only about 1,000 people in the federal government and private industry who understand operating systems deep enough to carry out front-line cyber defense, according to James Gosler, a scientist who specializes in information operations. Although Gosler has worked at the CIA, National Security Agency and the Energy Department, he spoke to *Government Executive* as an independent agent, and not on behalf of any agency. The government needs 20,000 to 30,000 people with these skill sets to have adequate defense, he says.

Federal agencies face stiff competition for these highly skilled experts, so they come to hacker conferences to tap into a subculture that used to be their foe. These computer wizards have the deep tactical knowledge of where the holes are in networks and how to exploit them—an insight agencies could use to build much needed cyber defenses.

But the alliance is an uneasy one. "Hackers feel persecuted by the rest of the world and the government . . . because they're scaring the shit out of people who are dumb," says Darren Greco, a computer specialist who does security auditing for federal agency affiliates and who attended the ideologically charged, left-leaning Hackers on Planet Earth Conference in New York in July. If the two parties can work out an understanding, then their collaboration could bolster vulnerable federal networks.

But both sides would have to put aside their paranoia.

The Cyber Squeeze

"There's no real difference between the skills needed to be a good defender and a good attacker," says James Lewis, senior fellow and director of the technology and public policy program at CSIS. "Think of it this way: Even though they teach cops how to drive fast, these are law enforcement skills."

Dan Guido, a consultant at the boutique security firm, iSEC Partners, who also teaches penetration testing at the Polytechnic Institute of New York University, says knowing how real attacks are performed is critical to stopping them. "If you work in a defensive role at a government agency building software, knowing exactly how that software breaks will force you to make it stronger," he says.

"Lots of people can see to it that agencies are following procedures and updating their passwords. Few have an exacting and detailed understanding of how systems work at their most fundamental level," adds Sandia's Gosler. "A reasonable percentage of people with such skills probably have participated in various hacking activities." He admits when he first started dabbling in information security he spent his free time after work "reverse-engineering software and tearing apart zeros and ones."

Within the community, a hacker is seen simply as someone who turns the original design of a system on its head. "Hackers have insatiable curiosity about how things work under the hood," says Gosler. "They appreciate the beauty of microcontrollers and computer codes. They just want to take things apart to see how they work. If they've shown the capacity to do evil but chose not to, I want to hire as many of these people as I can find."

A hacking conference like Black Hat and DEF CON is such a gold mine of talent that "the government would be crazy not to do recruiting there," he adds.

Breaking the Mold

At this year's DEF CON, hacker Chris Paget built a rogue cell phone base station that could intercept and record mobile phone calls. He did it using only $1,500 worth of hardware and open source software. Paget's device tricked cell phones in the vicinity into believing that it was a legitimate cell phone tower, causing calls to be routed through it.

Paget was trying to make the statement that GSM cell phone networks—which are the dominant mobile phone standard—are not secure. But his homemade tower also made a mockery of the commercially available version intelligence and law enforcement agencies use, the IMSI catcher, which costs hundreds of thousands of dollars.

It was a slap in the face to federal authorities. The day before Paget was scheduled to speak on July 31, a Federal Communications Commission officer contacted him and warned he would be violating federal law if did a live demo of how the homemade device worked. Paget shrugged off the phone call as a "scare tactic," and went ahead anyway. There were no repercussions. Brilliance doesn't always fit the cookie-cutter. Sometimes it also breaks the law.

"There is a huge trend where people who explore cybersecurity weaknesses on the Internet—and this is completely illegal—later use the skills they develop to become penetration testers for the government," says Alan Paller, research director at the cybersecurity training school, the SANS Institute. "Because they have no way to get prepared, there are no real places for young people to do that."

There were even fewer outlets for security enthusiasts in the early 1990s when the pentesting industry hadn't ballooned yet, Paller says.

"Back in the '90s, hacking NASA was always a rite of passage in the community," says Dai Zovi, a hacker-turned-security-professional who is known for his hijacks of MacBooks. "People would say, 'It's just NASA. What are they going to do? It's just a bunch of servers set up for scientists to share data.' "

Gosler, currently a Sandia National Laboratory fellow and NSA visiting scientist, has been called on to advise senior federal leaders on how to deal

1,000

People in government and industry with the skills needed for sophisticated cyberdefense tasks

20,000 to 30,000

Skilled specialists are needed to meet federal and industry computer security needs

SOURCE: CSIS COMMISSION ON CYBERSECURITY, "A HUMAN CAPITAL CRISIS IN CYBERSECURITY" with potential hires whose specialty comes with a criminal record.

"The impact of compromise of U.S. government computers can be very high," he says. "Think in terms of systems used to control the security of physical facility or nuclear control."

Job candidates are required to disclose whether they've had close contact with foreign nationals or international intelligence sources or engaged in criminal activity. For low-level IT security jobs, background checks for prospective recruits reach back five years. For higher-level jobs, agencies dig deeper and further into their history. Typically, most information security defense contractors undergo background checks dating back seven years.

At the same time, government gatekeepers are slowly relaxing their hold, making tenuous overtures to the hacking community.

Lewis says Pentagon sources have confided they're realizing they need to be more tolerant of those who break the traditional mold. And Gosler notes there is less stigma surrounding these law-breakers who now are seen as "gray cases." Self-professed "hackers gone legitimate" form a robust, growing network of Beltway security consultants. One such case is DEF CON and Black Hat founder and director Jeff Moss, who goes by the handle The Dark Tangent. Moss was sworn in last June as a member of the Homeland Security Advisory Council.

"Since these skills are in such high demand, greater latitude is given on a case-by-case basis," Gosler says. "You give people the benefit of the doubt because of the critical shortage. Maybe they broke into systems when they were 16, but now they're 21. You have to take that into account."

The government, however, still errs on the side of caution as a function of security when it recruits from the hacker community. "Of course, there's a threshold, and if you go beyond that threshold no one will make an exception," Gosler adds.

UNEASY ALLIANCE Hackers-turned-contractors like Andrew Strutt, a.k.a. Rod3nt, have to work hard to gain the trust of their colleagues.

DAWN LIM

But that threshold isn't always clear. It's an open secret that at conference after-parties, FBI agents hang out and extend their feelers into the community over drinks and loud music. In a close-knit community and in the post-WikiLeaks landscape, it's not clear who's an informant and who's not. Hackers are finding themselves in a difficult position, villainized for the very skills that paradoxically give them that coveted edge in information security.

Not What It Seems

Andrew Strutt, a hacker and a defense contractor, wears many hats. He's volunteered to conduct digital forensics to tackle botnets and child pornography for law enforcement, and has contracted with the military to guard the IT networks that support satellite imaging. Now he is waiting for the green light on a security clearance that would allow him to deploy oversees to support military operations.

In hacking circles Strutt cuts a deviant figure under the handle Rod3nt and hosts the IRC network for 2600, a group known for its anti-institutional bent and support of the whistleblower website WikiLeaks.

Strutt, who stresses that his opinions are not representative of the organizations he is affiliated with, recalls sitting in on a meeting and discussing network vulnerabilities. "I told them, you could just bust that open with XYZ—I've done that. They responded with, 'Oh my God, we thought you were just a good network administrator,' " he says.

"I've had to work hard to build up trust," Strutt adds. He doesn't disclose his identity as a hacker to the people he refers to as his handlers. And he doesn't advertise to hackers that he works for the .mil or .gov community either. At a DEF CON party, one hacker gave him the cold shoulder. "When he found out about my contracting work and figured that I was sort of a fed without arresting powers, his tone changed," Strutt says. "He said, 'So you work for them, you're basically a fed.' "

Strutt's predicament reflects the ambivalence and growing pains of a community as it sorts through its allegiances against the backdrop of a ballooning, multimillion-dollar cybersecurity industry. As the more corporate Black Hat crowd spills into DEF CON, occasionally clashing with the traditionally unruly cousin, there's a sense that the community is being pulled in two directions.

"The hacker community is just starting to become the development community," says Greco. "It appears softer, but at the same time, there are still a lot of hard-core people out there." On that other end of the spectrum are the die-hard anarchists: They tend to be younger; they've drawn the line in the sand on any contact with the feds, and they might be sneered at as "script kiddies"—a derogatory term for those who use programs others develop to break into systems.

"I never thought some of them would join the government. They looked too deviant, and now they're sitting in agencies. It surprises me."
—Nasir Memon, NYU's Polytechnic Institute

Luring Young Gurus

One group is trying to carve out a controlled space where hacking skills are being legitimized and detached from the politics of this underworld. The U.S. Cyber Challenge, a series of national competitions sponsored by agencies and organizations such as the Defense Department's Cyber Crime Center, the Air Force Association and the SANS Institute, aims to give students and information technology professionals a laboratory where they can compete as hackers.

"What is considered today's hacking may be against the norms," says Karen Evans, director of the U.S. Cyber Challenge and former chief of the Office of Management and Budget's Office of Electronic Government and Information Technology. "But it might become tomorrow's best defense if you can draw in these skills in a positive, controlled environment."

Cyber Challenge's home page reads, "Be the next cybersecurity top gun," and dangles the chance for competitors to "earn respect among your peers," "get noticed by a nationwide cybersecurity community," and "help the U.S. beat the bad guys." The aim is to scout for 10,000 experts to help the nation gain the lead in cyberspace.

"The key to attracting people with the right skills is that these competitions must have realistic threats and involve real sites and real problems," Paller says.

In 2009, for instance, USCC's inaugural NetWars competition featured a cybersecurity simulation exercise that required participants to hack into a computer without a password to access and play an online game. The winner was Michael Coppola, a.k.a. SevenM7, a precocious 17-year-old who hacked into the computer that hosted the game and rigged his own score. In July, USCC organizers made sure scores for its Capture the Flag competition in New York were computed with pen and paper.

Lawmakers have caught on to the realization that talented tricksters like Coppola need to be cheered on, not reprimanded. In June, Sens. Joe Lieberman, I-Conn.; Susan Collins, R-Maine; and Tom Carper, D-Del., called for more cyber competitions to inspire students. Federal agencies were on hand to recruit during a cybersecurity camp that led up to the New York event.

Not all participants at that competition were convinced the federal government was the right fit for them, however.

"It's a little bit difficult for participants to think about the federal government. A lot of times they think of private industry and big bucks," Evans says. Gosler knows cybersecurity experts who came on board with the government after Sept. 11 in a burst of patriotism. They had to settle for $100,000 to $150,000 federal paychecks after years of earning higher six- and seven-figure salaries, he estimates.

The deeper problem is the perception that there are irreconcilable differences between hackers and feds.

Nasir Memon, director of the Information Systems and Internet Security lab at the Polytechnic Institute of NYU, where USCC's New York Capture the Flag competition was held, said about 100 of his students have been placed in federal agencies in the past decade. "I never thought some of them would join the government," he says. "They looked too deviant, and now they're sitting in agencies. It surprises me."

But being able to bend the rules doesn't always mean breaking them, hackers say. "If someone used the word 'legitimate hacker,' they clearly have no idea what this is about," says Greco.

"But I want a place to practice my craft," he adds, "At some point, you say, 'I have to buckle down and be something that's respected—even if I'm feared—and able to support myself in the environment I live in.' "

Lewis agrees: "There has always been this wild cowboy element at DEF CON and Black Hat, but hackers wear suits when they have to."

Dawn Lim, a journalist in New York, is a contributing writer for Government Executive's *sister publication* Nextgov.