GlobalResearch
Center for Research on Globalization

The Secret War: Infiltration, Sabotage, Devastating Cyber Attacks

For Years Four Star General Keith Alexander has been Building A Secret Army Capable of Launching Devastating Cyberattacks

By James Bamford
Global Research, June 13, 2013
wired.com

Theme: Militarization and WMD, US NATO War Agenda
In-depth Report: IRAN: THE NEXT WAR?

Inside Fort Meade, Maryland, a top-secret city bustles. Tens of thousands of people move through more than 50 buildings—the city has its own post office, fire department, and police force. But as if designed by Kafka, it sits among a forest of trees, surrounded by electrified fences and heavily armed guards, protected by antitank barriers, monitored by sensitive motion detectors, and watched by rotating cameras. To block any telltale electromagnetic signals from escaping, the inner walls of the buildings are wrapped in protective copper shielding and the one-way windows are embedded with a fine copper mesh.

This is the undisputed domain of General Keith Alexander, a man few even in Washington would likely recognize. Never before has anyone in America's intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy. A four-star Army general, his authority extends across three domains: He is director of the world's largest intelligence service, the National Security Agency; chief of the Central Security Service; and commander of the US Cyber Command. As such, he has his own secret military, presiding over the Navy's 10th Fleet, the 24th Air Force, and the Second Army.

Alexander runs the nation's cyberwar efforts, an empire he has built over the past eight years by insisting that the US's inherent vulnerability to digital attacks requires him to amass more and more authority over the data zipping around the globe. In his telling, the threat is so mind-bogglingly huge that the nation has little option but to eventually put the entire civilian Internet under his protection, requiring tweets and emails to pass through his filters, and putting the kill switch under the government's forefinger. "What we see is an increasing level of activity on the networks," he said at a recent security conference in Canada. "I am concerned that this is going to break a threshold where the private sector can no longer handle it and the government is going to have to step in."

In its tightly controlled public relations, the NSA has focused attention on the threat of cyberattack against the US—the vulnerability of critical infrastructure like power plants and water systems, the susceptibility of the military's command and control structure, the dependence of the economy on the Internet's smooth functioning. Defense against these threats was the paramount mission trumpeted by NSA brass at congressional hearings and hashed over at security conferences.

But there is a flip side to this equation that is rarely mentioned: The military has for years

been developing offensive capabilities, giving it the power not just to defend the US but to assail its foes. Using so-called cyber-kinetic attacks, Alexander and his forces now have the capability to physically destroy an adversary's equipment and infrastructure, and potentially even to kill. Alexander—who declined to be interviewed for this article—has concluded that such cyberweapons are as crucial to 21st-century warfare as nuclear arms were in the 20th.

And he and his cyberwarriors have already launched their first attack. The cyberweapon that came to be known as Stuxnet was created and built by the NSA in partnership with the CIA and Israeli intelligence in the mid-2000s. The first known piece of malware designed to destroy physical equipment, Stuxnet was aimed at Iran's nuclear facility in Natanz. By surreptitiously taking control of an industrial control link known as a Scada (Supervisory Control and Data Acquisition) system, the sophisticated worm was able to damage about a thousand centrifuges used to enrich nuclear material.

The success of this sabotage came to light only in June 2010, when the malware spread to outside computers. It was spotted by independent security researchers, who identified telltale signs that the worm was the work of thousands of hours of professional development. Despite headlines around the globe, officials in Washington have never openly acknowledged that the US was behind the attack. It wasn't until 2012 that anonymous sources within the Obama administration took credit for it in interviews with The New York Times.

But Stuxnet is only the beginning. Alexander's agency has recruited thousands of computer experts, hackers, and engineering PhDs to expand US offensive capabilities in the digital realm. The Pentagon has requested $4.7 billion for "cyberspace operations," even as the budget of the CIA and other intelligence agencies could fall by $4.4 billion. It is pouring millions into cyberdefense contractors. And more attacks may be planned.

Inside the government, the general is regarded with a mixture of respect and fear, not unlike J. Edgar Hoover, another security figure whose tenure spanned multiple presidencies. "We jokingly referred to him as Emperor Alexander—with good cause, because whatever Keith wants, Keith gets," says one former senior CIA official who agreed to speak on condition of anonymity. "We would sit back literally in awe of what he was able to get from Congress, from the White House, and at the expense of everybody else."

Now 61, Alexander has said he plans to retire in 2014; when he does step down he will leave behind an enduring legacy—a position of far-reaching authority and potentially Strangelovian powers at a time when the distinction between cyberwarfare and conventional warfare is beginning to blur. A recent Pentagon report made that point in dramatic terms. It recommended possible deterrents to a cyberattack on the US. Among the options: launching nuclear weapons.

He may be a four-star Army general, but Alexander more closely resembles a head librarian than George Patton. His face is anemic, his lips a neutral horizontal line. Bald halfway back, he has hair the color of strong tea that turns gray on the sides, where it is cut close to the skin, more schoolboy than boot camp. For a time he wore large rimless glasses that seemed to swallow his eyes. Some combat types had a derisive nickname for him: Alexander the Geek.

Born in 1951, the third of five children, Alexander was raised in the small upstate New York

hamlet of Onondaga Hill, a suburb of Syracuse. He tossed papers for the Syracuse Post-Standard and ran track at Westhill High School while his father, a former Marine private, was involved in local Republican politics. It was 1970, Richard Nixon was president, and most of the country had by then begun to see the war in Vietnam as a disaster. But Alexander had been accepted at West Point, joining a class that included two other future four-star generals, David Petraeus and Martin Dempsey. Alexander would never get the chance to serve in Vietnam. Just as he stepped off the bus at West Point, the ground war finally began winding down.

In April 1974, just before graduation, he married his high school classmate Deborah Lynn Douglas, who grew up two doors away in Onondaga Hill. The fighting in Vietnam was over, but the Cold War was still bubbling, and Alexander focused his career on the solitary, rarefied world of signals intelligence, bouncing from secret NSA base to secret NSA base, mostly in the US and Germany. He proved a competent administrator, carrying out assignments and adapting to the rapidly changing high tech environment. Along the way he picked up masters degrees in electronic warfare, physics, national security strategy, and business administration. As a result, he quickly rose up the military intelligence ranks, where expertise in advanced technology was at a premium.

In 2001, Alexander was a one-star general in charge of the Army Intelligence and Security Command, the military's worldwide network of 10,700 spies and eavesdroppers. In March of that year he told his hometown Syracuse newspaper that his job was to discover threats to the country. "We have to stay out in front of our adversary," Alexander said. "It's a chess game, and you don't want to lose this one." But just six months later, Alexander and the rest of the American intelligence community suffered a devastating defeat when they were surprised by the attacks on 9/11. Following the assault, he ordered his Army intercept operators to begin illegally monitoring the phone calls and email of American citizens who had nothing to do with terrorism, including intimate calls between journalists and their spouses. Congress later gave retroactive immunity to the telecoms that assisted the government.

In 2003 Alexander, a favorite of defense secretary Donald Rumsfeld, was named the Army's deputy chief of staff for intelligence, the service's most senior intelligence position. Among the units under his command were the military intelligence teams involved in the human rights abuses at Baghdad's Abu Ghraib prison. Two years later, Rumsfeld appointed Alexander—now a three-star general—director of the NSA, where he oversaw the illegal, warrantless wiretapping program while deceiving members of the House Intelligence Committee. In a publicly released letter to Alexander shortly after The New York Times exposed the program, US representative Rush Holt, a member of the committee, angrily took him to task for not being forthcoming about the wiretapping: "Your responses make a mockery of congressional oversight."

Alexander also proved to be militant about secrecy. In 2005 a senior agency employee named Thomas Drake allegedly gave information to The Baltimore Sun showing that a publicly discussed program known as Trailblazer was millions of dollars overbudget, behind schedule, possibly illegal, and a serious threat to privacy. In response, federal prosecutors charged Drake with 10 felony counts, including retaining classified documents and making false statements. He faced up to 35 years in prison—despite the fact that all of the information Drake was alleged to have leaked was not only unclassified and already in the public domain but in fact had been placed there by NSA and Pentagon officials themselves. (As a longtime chronicler of the NSA, I served as a consultant for Drake's defense team. The

investigation went on for four years, after which Drake received no jail time or fine. The judge, Richard D. Bennett, excoriated the prosecutor and NSA officials for dragging their feet. “I find that unconscionable. Unconscionable,” he said during a hearing in 2011. “That’s four years of hell that a citizen goes through. It was not proper. It doesn’t pass the smell test.”)

But while the powers that be were pressing for Drake’s imprisonment, a much more serious challenge was emerging. Stuxnet, the cyberweapon used to attack the Iranian facility in Natanz, was supposed to be untraceable, leaving no return address should the Iranians discover it. Citing anonymous Obama administration officials, The New York Times reported that the malware began replicating itself and migrating to computers in other countries. Cybersecurity detectives were thus able to detect and analyze it. By the summer of 2010 some were pointing fingers at the US.

Natanz is a small, dusty town in central Iran known for its plump pears and the burial vault of the 13th-century Sufi sheikh Abd al-Samad. The Natanz nuclear enrichment plant is a vault of a different kind. Tucked in the shadows of the Karkas Mountains, most of it lies deep underground and surrounded by concrete walls 8 feet thick, with another layer of concrete for added security. Its bulbous concrete roof rests beneath more than 70 feet of packed earth. Contained within the bombproof structure are halls the size of soccer pitches, designed to hold thousands of tall, narrow centrifuges. The machines are linked in long cascades that look like tacky decorations from a ’70s discotheque.

To work properly, the centrifuges need strong, lightweight, well-balanced rotors and high-speed bearings. Spin these rotors too slowly and the critical U-235 molecules inside fail to separate; spin them too quickly and the machines self-destruct and may even explode. The operation is so delicate that the computers controlling the rotors’ movement are isolated from the Internet by a so-called air gap that prevents exposure to viruses and other malware.

In 2006, the Department of Defense gave the go-ahead to the NSA to begin work on targeting these centrifuges, according to The New York Times. One of the first steps was to build a map of the Iranian nuclear facility’s computer networks. A group of hackers known as Tailored Access Operations—a highly secret organization within the NSA—took up the challenge.

They set about remotely penetrating communications systems and networks, stealing passwords and data by the terabyte. Teams of “vulnerability analysts” searched hundreds of computers and servers for security holes, according to a former senior CIA official involved in the Stuxnet program. Armed with that intelligence, so-called network exploitation specialists then developed software implants known as beacons, which worked like surveillance drones, mapping out a blueprint of the network and then secretly communicating the data back to the NSA. (Flame, the complex piece of surveillance malware discovered by Russian cybersecurity experts last year, was likely one such beacon.) The surveillance drones worked brilliantly. The NSA was able to extract data about the Iranian networks, listen to and record conversations through computer microphones, even reach into the mobile phones of anyone within Bluetooth range of a compromised machine.

The next step was to create a digital warhead, a task that fell to the CIA Clandestine Service’s Counter-Proliferation Division. According to the senior CIA official, much of this

work was outsourced to national labs, notably Sandia in Albuquerque, New Mexico. So by the mid-2000s, the government had developed all the fundamental technology it needed for an attack. But there was still a major problem: The secretive agencies had to find a way to access Iran's most sensitive and secure computers, the ones protected by the air gap. For that, Alexander and his fellow spies would need outside help.

This is where things get murky. One possible bread crumb trail leads to an Iranian electronics and computer wholesaler named Ali Ashtari, who later confessed that he was recruited as a spy by the Mossad, Israel's intelligence service. (Israel denied the claim.) Ashtari's principal customers were the procurement officers for some of Iran's most sensitive organizations, including the intelligence service and the nuclear enrichment plants. If new computers were needed or routers or switches had to be replaced, Ashtari was the man to see, according to reports from semi-official Iranian news agencies and an account of Ashtari's trial published by the nonprofit Iran Human Rights Voice.

General Alexander's Empire

The four-star general presides over a trifecta of intelligence agencies headquartered in Fort Meade, Maryland. Here's a guide to the alphabet soup of agency and subagency acronyms. — Cameron Bird

NSA

(National Security Agency)

The nation's largest employer of mathematicians. The Department of Defense created this agency in 1952 to intercept, collect, and decrypt foreign communications. In the past decade, the NSA poured hundreds of millions of dollars into offensive cyberwar R&D.

CSS

(Central Security Service)

Originally envisioned as a fourth branch of the armed services, this organization is now described as a "combat support agency." It coordinates with the Army, Navy, Coast Guard, Marines, and Air Force to eavesdrop on foreign signals—like tapping into undersea cable or wireless communications.

USCyberCom

(US Cyber Command)

Established by the Department of Defense in 2009 to deter cyberattacks—"proactively." In March, Alexander gave a hint of the command's mandate to the House Armed Services Committee: "I would like to be clear that this team, this defend-the-nation team, is not a defensive team."

CAE

(Centers for Academic Excellence)

Launched in 1998, this NSA initiative seeks to increase the number of college students competent in “information assurance.” Last year the agency accredited four universities to lead the way in training the next generation of cyber operators in “collection, exploitation, and response.”

SCS

(Special Collection Service)

A unit whose existence has never been officially acknowledged by the defense establishment. But according to the accounts of an anonymous CIA official, members of the ultra- top-secret group are involved in covert eavesdropping from US embassies around the world.

JFCC-NW

(Joint Functional Component Command for Network Warfare)

Created in 2005 as part of US Strategic Command, which controls the nation’s nuclear arsenal, it played a lead role in promoting the idea of thwarting Iran’s own nuclear ambitions with a cyberattack. Folded into Cybercom in 2010.

He not only had access to some of Iran’s most sensitive locations, his company had become an electronics purchasing agent for the intelligence, defense, and nuclear development departments. This would have given Mossad enormous opportunities to place worms, back doors, and other malware into the equipment in a wide variety of facilities. Although the Iranians have never explicitly acknowledged it, it stands to reason that this could have been one of the ways Stuxnet got across the air gap.

But by then, Iran had established a new counterintelligence agency dedicated to discovering nuclear spies. Ashtari was likely on their radar because of the increased frequency of his visits to various sensitive locations. He may have let down his guard. “The majority of people we lose as sources—who get wrapped up or executed or imprisoned—are usually those willing to accept more risk than they should,” says the senior CIA official involved with Stuxnet. In 2006, according to Iran Human Rights Voice, Ashtari was quietly arrested at a travel agency after returning from another trip out of the country.

The malware targeting Iran replicated and spread to computers in other countries

In June 2008 he was brought to trial in Branch 15 of the Revolutionary Court, where he confessed, pleaded guilty to the charges, expressed remorse for his actions, and was sentenced to death. On the morning of November 17, in the courtyard of Tehran’s Evin Prison, a noose was placed around Ashtari’s neck, and a crane hauled his struggling body high into the air.

Ashtari may well have been one of the human assets that allowed Stuxnet to cross the air gap. But he was not Israel's only alleged spy in Iran, and others may also have helped enable malware transfer. "Normally," says the anonymous CIA official, "what we do is look for multiple bridges, in case a guy gets wrapped up." Less then two weeks after Ashtari's execution, the Iranian government arrested three more men, charging them with spying for Israel. And on December 13, 2008, Ali-Akbar Siadat, another importer of electronic goods, was arrested as a spy for the Mossad, according to Iran's official Islamic Republic News Agency. Unlike Ashtari, who said he had operated alone, Siadat was accused of heading a nationwide spy network employing numerous Iranian agents. But despite their energetic counterintelligence work, the Iranians would not realize for another year and a half that a cyberweapon was targeting their nuclear centrifuges. Once they did, it was only a matter of time until they responded.

Sure enough, in August 2012 a devastating virus was unleashed on Saudi Aramco, the giant Saudi state-owned energy company. The malware infected 30,000 computers, erasing three-quarters of the company's stored data, destroying everything from documents to email to spreadsheets and leaving in their place an image of a burning American flag, according to The New York Times. Just days later, another large cyberattack hit RasGas, the giant Qatari natural gas company. Then a series of denial-of-service attacks took America's largest financial institutions offline. Experts blamed all of this activity on Iran, which had created its own cyber command in the wake of the US-led attacks. James Clapper, US director of national intelligence, for the first time declared cyberthreats the greatest danger facing the nation, bumping terrorism down to second place. In May, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team issued a vague warning that US energy and infrastructure companies should be on the alert for cyberattacks. It was widely reported that this warning came in response to Iranian cyberprobes of industrial control systems. An Iranian diplomat denied any involvement.

The cat-and-mouse game could escalate. "It's a trajectory," says James Lewis, a cyber-security expert at the Center for Strategic and International Studies. "The general consensus is that a cyber response alone is pretty worthless. And nobody wants a real war." Under international law, Iran may have the right to self-defense when hit with destructive cyberattacks. William Lynn, deputy secretary of defense, laid claim to the prerogative of self-defense when he outlined the Pentagon's cyber operations strategy. "The United States reserves the right," he said, "under the laws of armed conflict, to respond to serious cyberattacks with a proportional and justified military response at the time and place of our choosing." Leon Panetta, the former CIA chief who had helped launch the Stuxnet offensive, would later point to Iran's retaliation as a troubling harbinger. "The collective result of these kinds of attacks could be a cyber Pearl Harbor," he warned in October 2012, toward the end of his tenure as defense secretary, "an attack that would cause physical destruction and the loss of life." If Stuxnet was the proof of concept, it also proved that one successful cyberattack begets another. For Alexander, this offered the perfect justification for expanding his empire.

In May 2010, a little more than a year after President Obama took office and only weeks before Stuxnet became public, a new organization to exercise American rule over the increasingly militarized Internet became operational: the US Cyber Command. Keith Alexander, newly promoted to four-star general, was put in charge of it. The forces under his command were now truly formidable—his untold thousands of NSA spies, as well as 14,000 incoming Cyber Command personnel, including Navy, Army, and Air Force troops. Helping

Alexander organize and dominate this new arena would be his fellow plebes from West Point's class of 1974: David Petraeus, the CIA director; and Martin Dempsey, chair of the Joint Chiefs of Staff.

Indeed, dominance has long been their watchword. Alexander's Navy calls itself the Information Dominance Corps. In 2007, the then secretary of the Air Force pledged to "dominate cyberspace" just as "today, we dominate air and space." And Alexander's Army warned, "It is in cyberspace that we must use our strategic vision to dominate the information environment." The Army is reportedly treating digital weapons as another form of offensive capability, providing frontline troops with the option of requesting "cyber fire support" from Cyber Command in the same way they request air and artillery support.

All these capabilities require a giant expansion of secret facilities. Thousands of hard-hatted construction workers will soon begin erecting cranes, driving backhoes, and emptying cement trucks as they expand the boundaries of NSA's secret city eastward, increasing its already enormous size by a third. "You could tell that some of the seniors at NSA were truly concerned that cyber was going to engulf them," says a former senior Cyber Command official, "and I think rightfully so."

In May, work began on a $3.2 billion facility housed at Fort Meade in Maryland. Known as Site M, the 227-acre complex includes its own 150-megawatt power substation, 14 administrative buildings, 10 parking garages, and chiller and boiler plants. The server building will have 90,000 square feet of raised floor—handy for supercomputers—yet hold only 50 people. Meanwhile, the 531,000-square-foot operations center will house more than 1,300 people. In all, the buildings will have a footprint of 1.8 million square feet. Even more ambitious plans, known as Phase II and III, are on the drawing board. Stretching over the next 16 years, they would quadruple the footprint to 5.8 million square feet, enough for nearly 60 buildings and 40 parking garages, costing $5.2 billion and accommodating 11,000 more cyberwarriors.

alexander's forces are formidable—thousands of NSA spies, plus 14,000 cyber troops.

In short, despite the sequestration, layoffs, and furloughs in the federal government, it's a boom time for Alexander. In April, as part of its 2014 budget request, the Pentagon asked Congress for $4.7 billion for increased "cyberspace operations," nearly $1 billion more than the 2013 allocation. At the same time, budgets for the CIA and other intelligence agencies were cut by almost the same amount, $4.4 billion. A portion of the money going to Alexander will be used to create 13 cyberattack teams.

What's good for Alexander is good for the fortunes of the cyber-industrial complex, a burgeoning sector made up of many of the same defense contractors who grew rich supplying the wars in Iraq and Afghanistan. With those conflicts now mostly in the rearview mirror, they are looking to Alexander as a kind of savior. After all, the US spends about $30 billion annually on cybersecurity goods and services.

In the past few years, the contractors have embarked on their own cyber building binge parallel to the construction boom at Fort Meade: General Dynamics opened a 28,000-square-foot facility near the NSA; SAIC cut the ribbon on its new seven-story Cyber Innovation Center; the giant CSC unveiled its Virtual Cyber Security Center. And at

consulting firm Booz Allen Hamilton, where former NSA director Mike McConnell was hired to lead the cyber effort, the company announced a “cyber-solutions network” that linked together nine cyber-focused facilities. Not to be outdone, Boeing built a new Cyber Engagement Center. Leaving nothing to chance, it also hired retired Army major general Barbara Fast, an old friend of Alexander’s, to run the operation. (She has since moved on.)

Defense contractors have been eager to prove that they understand Alexander’s worldview. “Our Raytheon cyberwarriors play offense and defense,” says one help-wanted site. Consulting and engineering firms such as Invertix and Parsons are among dozens posting online want ads for “computer network exploitation specialists.” And many other companies, some unidentified, are seeking computer and network attackers. “Firm is seeking computer network attack specialists for long-term government contract in King George County, VA,” one recent ad read. Another, from Sunera, a Tampa, Florida, company, said it was hunting for “attack and penetration consultants.”

One of the most secretive of these contractors is Endgame Systems, a startup backed by VCs including Kleiner Perkins Caufield & Byers, Bessemer Venture Partners, and Paladin Capital Group. Established in Atlanta in 2008, Endgame is transparently antitransparent. “We’ve been very careful not to have a public face on our company,” former vice president John M. Farrell wrote to a business associate in an email that appeared in a WikiLeaks dump. “We don’t ever want to see our name in a press release,” added founder Christopher Rouland. True to form, the company declined wired’s interview requests.

Perhaps for good reason: According to news reports, Endgame is developing ways to break into Internet-connected devices through chinks in their antivirus armor. Like safecrackers listening to the click of tumblers through a stethoscope, the “vulnerability researchers” use an extensive array of digital tools to search for hidden weaknesses in commonly used programs and systems, such as Windows and Internet Explorer. And since no one else has ever discovered these unseen cracks, the manufacturers have never developed patches for them.

Endgame hunts for hidden security weaknesses that are ripe for exploitation

Thus, in the parlance of the trade, these vulnerabilities are known as “zero-day exploits,” because it has been zero days since they have been uncovered and fixed. They are the Achilles’ heel of the security business, says a former senior intelligence official involved with cyberwarfare. Those seeking to break into networks and computers are willing to pay millions of dollars to obtain them.

According to Defense News’ C4ISR Journal and Bloomberg Businessweek, Endgame also offers its intelligence clients—agencies like Cyber Command, the NSA, the CIA, and British intelligence—a unique map showing them exactly where their targets are located. Dubbed Bonesaw, the map displays the geolocation and digital address of basically every device connected to the Internet around the world, providing what’s called network situational awareness. The client locates a region on the password-protected web-based map, then picks a country and city— say, Beijing, China. Next the client types in the name of the target organization, such as the Ministry of Public Security’s No. 3 Research Institute, which is responsible for computer security—or simply enters its address, 6 Zhengyi Road. The map will then display what software is running on the computers inside the facility, what types of

malware some may contain, and a menu of custom-designed exploits that can be used to secretly gain entry. It can also pinpoint those devices infected with malware, such as the Conficker worm, as well as networks turned into botnets and zombies— the equivalent of a back door left open.

Bonesaw also contains targeting data on US allies, and it is soon to be upgraded with a new version codenamed Velocity, according to C4ISR Journal. It will allow Endgame's clients to observe in real time as hardware and software connected to the Internet around the world is added, removed, or changed. But such access doesn't come cheap. One leaked report indicated that annual subscriptions could run as high as $2.5 million for 25 zero-day exploits.

The buying and using of such a subscription by nation-states could be seen as an act of war. "If you are engaged in reconnaissance on an adversary's systems, you are laying the electronic battlefield and preparing to use it," wrote Mike Jacobs, a former NSA director for information assurance, in a McAfee report on cyberwarfare. "In my opinion, these activities constitute acts of war, or at least a prelude to future acts of war." The question is, who else is on the secretive company's client list? Because there is as of yet no oversight or regulation of the cyberweapons trade, companies in the cyber-industrial complex are free to sell to whomever they wish. "It should be illegal," says the former senior intelligence official involved in cyberwarfare. "I knew about Endgame when I was in intelligence. The intelligence community didn't like it, but they're the largest consumer of that business."

Thus, in their willingness to pay top dollar for more and better zero-day exploits, the spy agencies are helping drive a lucrative, dangerous, and unregulated cyber arms race, one that has developed its own gray and black markets. The companies trading in this arena can sell their wares to the highest bidder—be they frontmen for criminal hacking groups or terrorist organizations or countries that bankroll terrorists, such as Iran. Ironically, having helped create the market in zero-day exploits and then having launched the world into the era of cyberwar, Alexander now says the possibility of zero-day exploits falling into the wrong hands is his "greatest worry."

He has reason to be concerned. In May, Alexander discovered that four months earlier someone, or some group or nation, had secretly hacked into a restricted US government database known as the National Inventory of Dams. Maintained by the Army Corps of Engineers, it lists the vulnerabilities for the nation's dams, including an estimate of the number of people who might be killed should one of them fail. Meanwhile, the 2013 "Report Card for America's Infrastructure" gave the US a D on its maintenance of dams. There are 13,991 dams in the US that are classified as high-hazard, the report said. A high-hazard dam is defined as one whose failure would cause loss of life. "That's our concern about what's coming in cyberspace—a destructive element. It is a question of time," Alexander said in a talk to a group involved in information operations and cyberwarfare, noting that estimates put the time frame of an attack within two to five years. He made his comments in September 2011.

*Contributor **James Bamford** (washwriter@gmail.com) wrote about the NSA's new Utah Data Center in issue 20.04.*

Illustrations by Mark Weaver

Articles by: **James Bamford**