**After Stuxnet: The new rules of cyberwar**

**Critical infrastructure providers face a rising tide of increasingly sophisticated and potentially destructive attacks.**

*

 

By **[Robert L. Mitchell](http://www.itworld.com/robert-l-mitchell)**, Computerworld

**November 05, 2012, 1:34 PM** — Three years ago, when electric grid operators were starting to talk about the need to protect critical infrastructure from cyberattacks, few utilities had even hired a chief information security officer.

Then came Stuxnet.

In 2010, that malware, widely [reported to have been created by the U.S. and Israel](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html%22%20%5Ct%20%22new), reportedly destroyed 1,000 centrifuges that Iran was using to enrich uranium after taking over the computerized systems that operated the centrifuges.

Gen. Michael Hayden, principal at security consultancy The Chertoff Group, was director of the National Security Agency, and then the CIA, during the years leading up to the event. "I have to be careful about this," he says, "but in a time of peace, someone deployed a cyberweapon to destroy what another nation would describe as its critical infrastructure." In taking this step, the perpetrator not only demonstrated that control systems are vulnerable, but also legitimized this kind of activity by a nation-state, he says.

The attack rattled the industry. "Stuxnet was a game-changer because it opened people's eyes to the fact that a cyber event can actually result in physical damage," says Mark Weatherford, deputy undersecretary for cybersecurity in the National Protection Programs Directorate at the U.S. Department of Homeland Security.

In another development that raised awareness of the threat of cyberwar, the U.S. government in October accused Iran of launching distributed denial-of-service (DDoS) [attacks against U.S. financial institutions](http://www.computerworld.com/s/article/9231515/U.S._banks_on_high_alert_against_cyberattacks%22%20%5Ct%20%22new). In a speech intended to build support for stalled legislation known as the [Cybersecurity Act](http://www.computerworld.com/s/article/9230099/White_House_exploring_executive_order_to_secure_critical_networks%22%20%5Ct%20%22new) that would enable greater information sharing and improved cybersecurity standards, [Defense Secretary Leon Panetta](http://www.computerworld.com/s/article/9232317/Future_cyber_attacks_could_rival_9_11_cripple_US_warns_Panetta%22%20%5Ct%20%22new) warned that the nation faced the possibility of a "cyber Pearl Harbor" unless action was taken to better protect critical infrastructure.

"Awareness of the problem has been the biggest change" since the release of Stuxnet, says Tim Roxey, chief cybersecurity officer for the North American Electric Reliability Corp. (NERC), a trade group serving electrical grid operators. He noted that job titles such as CISO and cybersecurity officer are much more common than they once were, [new cybersecurity standards are now under development](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html%22%20%5Ct%20%22new), and there's a greater emphasis on information sharing, both within the industry and with the DHS through [sector-specific Information Sharing and Analysis Centers](http://www.isaccouncil.org/%22%20%5Ct%20%22new). (Read our [timeline of critical infrastructure attacks](http://www.computerworld.com/s/article/9233173/Timeline_Critical_infrastructure_attacks_increase_steadily_in_past_decade%22%20%5Ct%20%22new) over the years.)

On the other hand, cybersecurity is still not among the top five reliability concerns for most utilities, according to John Pescatore, an analyst at Gartner. Says Roxey: "It's clearly in the top 10." But then, so is vegetation management.

Compounding the challenge is the fact that regulated utilities tend to have tight budgets. That's a big problem, says Paul Kurtz, managing director of international practice at security engineering company CyberPoint International and former senior director for critical infrastructure protection at the White House's Homeland Security Council. "We're not offering cost-effective, measurable solutions," he says. "How do you do this without hemorrhaging cash?"

**Falling Behind**

Most experts agree that critical infrastructure providers have a long way to go. Melissa Hathaway, president of Hathaway Global Strategies, was the Obama administration's acting senior director for cyberspace in 2009. That year, she issued a [Cyberspace Policy Review](http://www.whitehouse.gov/assets/documents/Cyperspace_Policy_Review_final.pdf%22%20%5Ct%20%22new) report that included recommendations for better protecting critical infrastructure, but there hasn't been much movement toward implementing those recommendations, she says. A draft National Cyber Incident Response plan has been published, but a national-level exercise, conducted in June, showed that the plan was insufficient to protect critical infrastructure.

"A lot of critical infrastructure is not even protected from basic hacking. I don't think the industry has done enough to address the risk, and they're looking for the government to somehow offset their costs," Hathaway says. There is, however, a broad recognition that critical infrastructure is vulnerable and that something needs to be done about it.

The Department of Defense has a direct stake in the security of the country's critical infrastructure because the military depends on it. "The Defense Science Board Task Force did a review of DOD reliance on critical infrastructure and found that an astute opponent could attack and harm the DOD's capabilities," says James Lewis, a senior fellow specializing in cybersecurity at the Center for Strategic and International Studies.

At a forum in July, NSA Director Gen. Keith Alexander was asked to rate the state of U.S. preparedness for an attack on critical infrastructure on a scale of 1 to 10. He responded, "I would say around a 3." The reasons include the inability to rapidly detect and respond to attacks, a lack of cybersecurity standards and a general unwillingness by both private companies and government agencies to share detailed information about threats and attacks. The DOD and intelligence agencies don't share information because they tend to overclassify it, says Hayden. And critical infrastructure providers prefer to keep things to themselves because they don't want to expose customer data and they're concerned about the liability issues that could arise and the damage their reputations could suffer if news of an attack were widely reported.

"The rules of the game are a little fuzzy on what you can and cannot share," says Edward Amoroso, chief security officer and a senior vice president at AT&T, noting that his biggest concern is the threat of a large-scale DDoS attack that could take down the Internet's backbone. "I need attorneys, and I need to exercise real care when interacting with the government," he says.

In some cases, critical infrastructure providers are damned if they do share information and damned if they don't. "If the government provides a signature to us, some policy observers would say that we're operating on behalf of that government agency," he says. All parties agree that, in a crisis, everyone should be able to share information in real time. "But talk to five different people and you'll get five different opinions about what is OK," says Amoroso. Unfortunately, government policy initiatives intended to resolve the issue, such as the Cybersecurity Act, have failed to move forward.

"It was disappointing for us that this nonpartisan issue became so contentious," says Weatherford. The lack of progress by policymakers is a problem for the DHS and the effectiveness of its National Cybersecurity and Communications Integration Center (NCCIC). The center, which is open around the clock, was designed to be the nexus for information sharing between private-sector critical infrastructure providers -- and the one place to call when there's a problem. "I want NCCIC to be the '911' of cybersecurity," he says. "We may not have all the answers or all the right people, but we know where they are."

Meanwhile, both the number of attacks and their level of sophistication have been on the rise. Richard Bejtlich, chief security officer at security consultancy Mandiant, says electric utilities and other businesses are under constant assault by foreign governments. "We estimate that 30% to 40% of the Fortune 500 have an active Chinese or Russian intrusion problem right now," he says. However, he adds, "I think the threat in that area is exaggerated," because the goal of such attacks is to steal intellectual property, not destroy infrastructure. (Read our [timeline of critical infrastructure attacks](http://www.computerworld.com/s/article/9233173/Timeline_Critical_infrastructure_attacks_increase_steadily_in_past_decade%22%20%5Ct%20%22new) over the years.)

Others disagree. "We've seen a new expertise developing around industrial control systems. We're seeing a ton of people and groups committed to the very technical aspects of these systems," says Howard Schmidt, who served as cybersecurity coordinator and special assistant to the president until last May and is now an independent consultant.

"People are too quick to dismiss the link between intellectual property loss through cyber intrusions and attacks against infrastructure," says Kurtz. "Spear phishing events can lead to the exfiltration of intellectual property, and that can have a spillover effect into critical infrastructure control system environments."

[Spear phishing](http://www.computerworld.com/s/article/9226960/CERT_warns_of_targeted_phishing_attacks_against_gas_pipeline_firms%22%20%5Ct%20%22new) attacks, sometimes called advanced targeted threats or advanced persistent threats, are efforts to break into an organization's systems by targeting specific people and trying, for example, to get them to open infected email messages that look like they were sent by friends. Such attacks have been particularly difficult to defend against.

Then there's the issue of [zero-day attacks](http://www.computerworld.com/s/article/9220099/Researcher_discloses_zero_day_flaws_in_SCADA_systems%22%20%5Ct%20%22new). While software and systems vendors have released thousands of vulnerability patches over the past 10 years, Amoroso says, "I wouldn't be surprised if there are thousands of zero-day vulnerabilities that go unreported." And while hacktivists may brag about uncovering vulnerabilities, criminal organizations and foreign governments prefer to keep that information to themselves. "The nation-state-sponsored attack includes not only the intellectual property piece but the ability to pre-position something when you want to be disruptive during a conflict," Schmidt says.

Usually in espionage it's much easier to steal intelligence than it is to do physical harm. That's not true in the cyber domain, says Hayden. "If you penetrate a network for espionage purposes, you've already got everything you'll want for destruction," he says.

On the other hand, while it's impossible for a private company to defend itself from physical warfare, that's not true when it comes to cyberattacks. Every attack exploits a weakness. "By closing that vulnerability, you stop the teenage kid, the criminal and the cyberwarrior," says Pescatore.

**Control Anxiety**

Computerized control systems are a potential problem area because the same systems are in use across many different types of critical infrastructure. "Where you used to turn dials or throw a switch, all of that is done electronically now," Schmidt says.

In addition, many industrial control systems that used to be "air-gapped" from the Internet are now connected to corporate networks for business reasons. "We've seen spreadsheets with thousands of control system components that are directly connected to the Internet. Some of those components contain known vulnerabilities that are readily exploitable without much sophistication," says Marty Edwards, director of control systems security at the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the DHS. The organization, with a staff that's grown tenfold to 400 in the past four years, offers [control system security standards](http://www.us-cert.gov/control_systems/csstandards.html%22%20%5Ct%20%22new), shares threat data with critical infrastructure providers and has a rapid response team of "cyberninjas," high-level control systems engineers and cybersecurity analysts who can be deployed at a moment's notice.

Last year, ICS-CERT issued 5,200 alerts and advisories to private industry and government. "[Edwards] had teams fly out seven times last year to help businesses respond to events that either took them offline or severely impacted operations," says Weatherford, who declined to provide details on the nature of those events.

Control systems also suffer from another major weakness: They're usually relatively old and can't easily be patched. "A lot of them were never designed to operate in a network environment, and they aren't designed to take upgrades," Schmidt says. "Its firmware is soldered onto the device, and the only way to fix it is to replace it." Since the systems were designed to last 10 to 20 years, organizations need to build protections around them until they can be replaced. In other cases, updates can be made, but operators have to wait for the service providers who maintain the equipment to do the patching.

So where should the industry go from here?

The place to start is with better standards and best practices, real-time detection and containment, and faster and more detailed information sharing both among critical infrastructure providers and with all branches of government.

Internet at Risk

While some progress has been made with standards at both the DHS and industry groups such as the NERC, some argue that government procurement policy could be used to drive higher security standards from manufacturers of hardware and software used to operate critical infrastructure. Today, no such policy exists across all government agencies.

"Government would be better off using its buying power to drive higher levels of security than trying to legislate higher levels of security," argues Pescatore. But the federal government doesn't require suppliers to meet a consistent set of security standards across all agencies.

Even basic changes in contract terms would help, says Schmidt. "There's a belief held by me and others in the West Wing that there's nothing to preclude one from writing a contract today that says if you are providing IT services to the government you must have state-of-the-art cybersecurity protections in place. You must have mechanisms in place to notify the government of any intrusions, and you must have the ability to disconnect networks," he says.

But government procurement policy's influence on standards can go only so far. "The government isn't buying turbines" and control systems for critical infrastructure, says Lewis.

When it comes to shutting down attacks, faster reaction times are key, says Bejtlich. "Attackers are always going to find a way in, so you need to have skilled people who can conduct rapid and accurate detection and containment," he says. For high-end threats, he adds, that's the only effective countermeasure. Analysts need high visibility into the host systems, Bejtlich says, and the network and containment should be achieved within one hour of intrusion.

**Opening the Kimono**

Perhaps the toughest challenge will be creating the policies and fostering the trust required to encourage government and private industry to share what they know more openly. The government not only needs to pass legislation that provides the incentives and protections that critical infrastructure businesses need to share information on cyberthreats, but it also needs to push the law enforcement, military and intelligence communities to open up. For example, if the DOD is planning a cyberattack abroad against a type of critical infrastructure that's also used in the U.S., should information on the weakness being exploited be shared with U.S. companies so they can defend against counterattacks?

"There is a need for American industry to be plugged into some of the most secretive elements of the U.S. government -- people who can advise them in a realistic way of what it is that they need to be concerned about," says Hayden. Risks must be taken on both sides so everyone has a consistent view of the threats and what's going on out there.

One way to do that is to share some classified information with selected representatives from private industry. The House of Representatives recently passed an intelligence bill, the Cyber Intelligence Sharing and Protection Act, which would give security clearance to officials of critical industry operators. But the bill has been [widely criticized by privacy groups](http://www.aclu.org/blog/national-security-technology-and-liberty/cyber-protection-act-too-broad-infringes-our-privacy%22%20%5Ct%20%22new), which say it's too broad. Given the current political climate, Hayden says he expects the bill to die in the Senate.

Information sharing helps, and standards form a baseline for protection, but ultimately, every critical infrastructure provider must customize and differentiate its security strategy, Amoroso says. "Right now, every business has exactly the same cybersecurity defense, usually dictated by some auditor," he says. But as in football, you can't win using just the standard defense. A good offense will find a way around it. "You've got to mix it up," Amoroso says. "You don't tell the other guys what you're doing."

**Cyberdefense Strategies**

**Should the U.S. Strike Back?**

Most best practices on dealing with cyberattacks on critical infrastructure focus on defense: patching vulnerabilities and managing risk. But should the U.S. conduct preemptive strikes against suspected attackers -- or at least hit back?

Gen. Michael Hayden, principal at security consultancy The Chertoff Group, and former director of the NSA and the CIA, says the cybersecurity problem can be understood through the classic risk equation: Risk (R) = threat (T) x vulnerability (V) x consequences (C). "If I can drive any factor down to zero, the risk goes down to zero," he says. So far, most efforts have focused on reducing V, and there's been a shift toward C, with the goal of determining how to rapidly detect an attack, contain the damage and stay online. "But we are only now beginning to wonder, how do I push T down? How do I reduce the threat?" Hayden says. "Do I shoot back?"

The DOD is contemplating the merits of "cross-domain" responses, says James Lewis, senior fellow at the Center for Strategic and International Studies. "We might respond with a missile. That increases the uncertainty for opponents."

Ultimately, countries that launch such attacks will pay a price, says Howard Schmidt, former cybersecurity coordinator and special assistant to the president. The U.S. response could involve economic sanctions -- or it could involve the use of military power.

**-- Robert L. Mitchell**

**Global Threat**

**Hacking on the Rise**

Cyberattackers fall into three primary categories: criminal organizations interested in stealing for monetary gain, hacktivists bent on furthering their own agendas, and foreign governments, or their agents, aiming to steal information or lay the groundwork for later attacks.

The Chinese are the most persistent, with several tiers of groups participating, says Richard Bejtlich, chief security officer at security consultancy Mandiant. Below official state-sponsored attacks are breaches by state militias, quasi-military and quasi-government organizations, and what he calls "patriotic hackers."

"It's almost a career path," says Bejtlich.

There's disagreement on which groups are the most sophisticated or dangerous, but that's not what matters. What matters is that the universe of attackers is expanding and they have ready access to an ever-growing wealth of knowledge about hacking, along with black hat tools helpful in launching attacks. "Over the next five years, low-level actors will get more sophisticated and the Internet [will expand] into areas of the Third World where the rule of law is weaker," says Gen. Michael Hayden, principal at security consultancy The Chertoff Group. "The part of the world responsible for criminal groups such as the Somali pirates is going to get wired."

**-- Robert L. Mitchell**

**Telecoms Deal With Escalating DDoS Threat**

Electric grid operators worry about compromised computerized industrial control systems taking them offline. Telecommunications companies worry that a large-scale distributed denial-of-service (DDoS) attack will take out another type of critical infrastructure: the Internet.

Until 2009 or so, AT&T might have seen one major DDoS attack a year, says Edward Amoroso, chief security officer and a senior vice president at the telecommunications giant. Today, Tier 1 Internet service providers find themselves fending off a few dozen attacks at any given moment. "It used to be two guys bailing out the ship. Now we have 40, 50 or 60 people dumping the water out all the time," he says. In fact, attacks have been scaling up to the point where Amoroso says he worries they could potentially flood backbone networks, taking portions of the Internet offline.