Society | DOI:10.1145/1859204.1859212

Samuel Greengard

The New Face of War

With the introduction of the sophisticated Stuxnet worm, the stakes of cyberwarfare have increased immeasurably.

Ever since European cybersecurity officials discovered the Stuxnet worm last June, it has been characterized as a "paradigm shift" in critical infrastructure threats. European Network and Information Security Agency Executive Director Udo Helmbrecht characterized Stuxnet, which is unprecedented in its capabilities and sophistication, as "a new class and dimension of malware."

Stuxnet, which contains four zero-day Windows vulnerabilities as well as two stolen digital certificates for authentication is the first discovered worm that secretly monitors and reprograms industrial control systems. Stuxnet exploits weaknesses in Windows operating systems and takes command of a Siemens component that controls critical industrial operations, such as those of oil pipelines, electrical power grids, and nuclear energy plants.

Whether Stuxnet is a new weapon of modern espionage or cyberwarfare is unclear. However, many security experts believe the sophisticated malware was developed by a well-funded private entity or a national government agency to attack Iran's industrial infrastructure, including the Bushehr nuclear power plant. Iranian officials report that Stuxnet has infected 30,000 machines involved in running its industrial control systems, and the Bushehr facility reportedly didn't work correctly for several months. "An electronic war has been launched against Iran," according to Mahmoud Liaii, director of Iran's Information and Technology Council of the Industries and Mines Ministry.

Cyberwarfare or industrial espionage? The Stuxnet worm has infected 30,000 machines in Iran, including an unknown number at the Bushehr nuclear power plant.

PHOTOGRAPH BY ISNA, MEHDI GHASEMI/AP PHOTO

To be certain, the digital age is ushering in entirely new ways to fight wars. "Cyber tools can be used as an instrument for government security as well as for military and intelligence purposes," states Herbert Lin, chief scientist for the Computer Science and Telecommunications Board at the U.S. National Research Council. Adds Rain Ottis, a staff scientist at the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, "Cyber warfare is almost certain to emerge the next time two technologically advanced states fight a major shooting war."

It's not an abstract concept. Although government Web sites and computer systems are likely targets (many government systems are 10 to 20 years old and can't support modern security standards), civilian targets like power grids, telecommunications networks, flight control systems, and financial networks are also at risk. "Cyberwarfare has the potential to cause significant strategic damage," observes Sami Saydjari, CEO of Cyber Defense Agency, a cybersecurity consulting firm headquartered in Wisconsin Rapids, WI.

The Changing Nature of War

The evolution of weaponry has always centered on gaining superiority over an enemy. However, in the digital age, the nature of war is changing radically. It's one thing to detect an invading army and its well-marked planes, tanks, and troops. It's not so simple to identify bits and bytes of data, ascertain exactly where they're coming from, and understand the sender's intentions.

In fact, hackers and others attack government and corporate systems for a broad array of reasons that have nothing to do with politics or ideology. As a result, defining cyberwarfare is a challenge and the hype often exceeds reality. "Some very visible and vocal people have seemingly equated any malicious activity on the Internet to cyberwarfare," Ottis observes. "Most, if not all, cyberattacks should be classified as criminal, espionage related, or hactivist, and not warfare."

Moreover, there is no clear international law covering cyberattacks although experts say the mere act of one nation or state invading another's computers could be construed as an act of war. Common attack methods include vandalism, spreading propaganda, gathering classified data, using distributed denial-of-service (DDoS) attacks to shut down systems, destroying equipment, attacking critical infrastructure, and planting malicious software.

Over the last few years, untold incidents may have fallen into these categories, but proving the legitimacy of attacks is next to impossible. That's because hackers hijack computers all over the world and use them as part of a botnet to launch attacks. Tracing back the Internet protocol address doesn't necessarily provide insight into who actually is launching the attack. In May 2007, for example, Estonia's government Web sites came under attack—presumably from Russia—after the government moved a Soviet war memorial. The wave after wave of DDoS attacks came from IP addresses all over the world, though many of them originated from Russian-hosted servers.

In October of the same year, Israel mounted a sneak air attack against Syria and destroyed a fledgling nuclear research center deep inside the country. Some analysts believe that Israel avoided detection by hacking radar and other defense systems in Syria and perhaps additional countries. Afterward, *Aviation Week* magazine reported: "The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading message algorithms."

When Russian troops invaded the Republic of Georgia in August 2008 the news media diligently reported the event and analysts pondered the repercussions. But what wasn't apparent to many—at least immediately—was that the battle wasn't being fought only with troops and tanks. Several servers and Web sites operated by the Georgian government, including the nation's primary government site, were rendered useless through a steady barrage of DDoS attacks.

Almost immediately, the Georgian Ministry of Foreign Affairs issued a statement via a replacement site built on a blog-hosting service. It read: *A cyber warfare campaign by Russia is seriously disrupting many Georgian websites*. Meanwhile, Barack Obama, then a U.S. presidential candidate, issued a demand that Russia stop interfering with the Web sites. Analysts and security experts noted that the attacks—mostly originating in Russia and Turkey—were linked to the Russian Business Network, a group with close ties to Russian gangs and the government.

"Cyberwarfare is almost certain to emerge the next time two technologically advanced states fight a major shooting war," says Rain Ottis.

Meanwhile, the People's Republic of China and the U.S. have reportedly launched cyberattacks against each other dating back to the 1990s, though China has taken a lead in developing cyberwarfare systems, Saydjari says. For one thing, the government has adopted a more secure operating system named Kylin, which provides hardened protection that is not available with Windows, Unix, and Linux. China has also funneled capital and expertise into developing cyberwar capabilities, including enlisting patriotic hacker gangs. "They have acted slowly, patiently, and strategically," says Saydjari.

The New Battlefield

Although government-sponsored cyberattacks have so far occurred on a limited basis, the probability of a major cyberwar erupting over the next decade seems inevitable. In all likelihood, experts say, a cyberassault would accompany more traditional forms of warfare, but it could also serve as a way to wreak economic harm or destabilize a nation state without a conventional battle. As Ottis puts it, "In the end, the aim of war is usually not to kill your enemy but to impose your will on them."

Scott Borg, director and chief economist of the nonprofit U.S. Cyber Consequences Unit, located in Norwich, VT, has stated publicly that cyberattacks can cause "horrendous damage." Even a short-lived Internet failure could have severe repercussions. The cost of a flight control system crashing or an electrical power grid fading to black

Cybersecurity

Isolate Infected PCs?

Computers infected with malware should be disconnected from the Internet to prevent them from harming other members of the online community, Scott Charney, corporate vice president of Trustworthy Computing at Microsoft, said during his speech at ISSE 2010. The proposed measure would not only prevent the spread of malware, but also pose substantial difficulties for botnets, Charney noted.

Charney's speech, along with a simultaneously published paper, "Collective Defense: Applying Public Health Models to the Internet," urged the IT security community to rethink its approach to cybersecurity and adopt quarantine measures similar to those adopted by the public-health professionals.

"For a society to be healthy, its members must be aware of basic health risks and be educated on how to avoid them," Charney wrote in the paper. "In the physical world, there are also international, national, and local health systems that identify, track, and control the spread of disease including, where necessary, quarantining people to avoid the infection of others."

Meanwhile, the U.S. government is studying a number of voluntary ways to help the public and small businesses better protect themselves online. The possibilities include provisions in an Australian program that enable customers to receive alerts from their Internet service providers if their computer is hijacked via a botnet. U.S. officials are not advocating an option in the program that permits ISPs to block or limit Internet access by customers who fail to fix their infected computers. However, Harris Corporation's Dale Meyerrose, vice president of Cyber and Information Assurance, warns that voluntary programs will be insufficient. "We need to have things that have more teeth in them, like standards," Meyerrose says.

—Phil Scott

could extend into the hundreds of billions of dollars and lead to a cascade of economic problems.

Yet the ensuing fallout could cause an additional array of headaches. Because China manufactures many components, obtaining spare parts during a conflict could prove difficult, if not impossible. In addition, some analysts worry that electricity generators and other components imported from China and other countries could contain hidden software that allows hackers to access systems through a back door or execute a malicious software program on command.

Already, many nations have developed sophisticated hacking and intrusion capabilities, including planting Trojan horses, rootkits, and other nefarious tools on targeted systems. Many of these applications stealthily reside on computers until someone decides to flip a switch and activate them. In fact, much of the preparation goes on behind the scenes. "During 'peacetime' many nations actively prepare for offensive cyberoperations and some nations probably test their capabilities with nonattributable events," Ottis points out.

Of course, the idea of cyberwarfare hasn't been lost on terrorist organizations either. "While nation-states are likely to be quite choosey about how and when they use cyberwarfare tools, terrorists are likely to view things in a less methodical and calculating way," Saydjari explains. "Their goal can be as simple as destabilizing systems and creating chaos." Worse, it is nearly impossible to identify terrorists inflicting a cyberattack and strike back at a tangible target. Economic sanctions and diplomacy aren't viable either.

China has funneled capital and expertise into developing its cyberwar capabilities, including enlisting civilians and gangs of hackers.

What makes the situation all the more dangerous, Saydjari notes, is that a relatively large number of cybermercenaries exist and many openly advertise their skills. In some instances, they might be hired to handle a project that appears less harmful than it actually is or they might not be concerned about the repercussions. In addition, these individuals often act in a rogue manner and they can easily venture beyond a government's desired actions.

There is some pushback. For now, some businesses and governments are turning to ethical hackers to discover holes and vulnerabilities and report them to authorities. In addition, the U.S. government recently announced a $40-billion national cybersecurity plan to combat cyberattacks from foreign and domestic hackers. However, in May 2010, James Miller, principal deputy under secretary of defense for policy for the U.S. Department of Defense, noted the nation is losing enough data from cyberattacks to fill the Library of Congress many times over.

Make no mistake, the risk of cyberwarfare is growing and many, including Saydjari, warn that political leaders aren't entirely tuned into the severity of the threat. Murky definitions, old and insecure computer systems, difficult-to-detect actions, and vague rules of engagement aren't making things any easier. "Cyberwarfare must be taken seriously," Lin says. "The question isn't, Will it happen? It's *how* and *when* will it happen and what effect will it have on society."

Further Reading

Bruno, G.
***The Evolution of Cyber Warfare*, Council on Foreign Relations, Feb. 2008.**

Clarke, R.A. and Knake, R.
***Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, New York, NY, 2010.**

Drogin, B.
"In a doomsday cyber attack scenario, answers are unsettling," *Los Angeles Times*, February 17, 2010.

Mueller, R.S. III.
"The State of Cyberterrorism and Cyberattacks," speech, RSA Cyber Security Conference, San Francisco, CA, March 4, 2010.

National Research Council
***Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2009.**

Samuel Greengard is an author and journalist based in West Linn, OR.

Security

India Plans Its Own OS

India recently announced plans to develop its own operating system for government and high-level corporate computers to make them more secure.

Concerns about the vulnerabilities of Western-developed OSs and software and of cyberattacks from computers based in China raised the issue to one requiring a significant response from the Indian government as it moves forward technologically. Last year China developed its own OS, Kylin, for government computers.

India's Defense Research and Development Organization (DRDO) will partner with several other groups, including the Indian Institute of Science and the Indian Institute of Technology Madras, to build the new OS.

"With a homegrown system, the source code will be with us and it helps in securing our systems," according to Vijay Kumar Saraswat, scientific adviser to the defense minister and DRDO director-general. Development and maintenance of the OS source code is considered vital to protecting India's computer networks, Saraswat said.

However, some critics question the usefulness of an Indian OS and the government's motives. It appears Indian officials plan to keep the source code secure by not letting the OS be widely used beyond the nation's borders, but Bruce Schneier, chief security technology officer at BT, suspects this security measure will eventually fail, virtually making the OS irrelevant.

Indian officials have not made cost or time estimates for the project, leading some to suggest it is a public-relations ploy.

—*Graeme Stemp-Morlock*