INTERACTIVE SESSION: MANAGEMENT

STUXNET AND THE CHANGING FACE OF CYBERWARFARE

In July 2010, reports surfaced about a Stuxnet worm that had been targeting Iran's nuclear facilities. In November of that year, Iran's President Mahmoud Ahmadinejad publicly acknowledged that malicious software had infected the Iranian nuclear facilities and disrupted the nuclear program by disabling the facilities' centrifuges. Stuxnet had earned its place in history as the first visible example of industrial cyberwarfare.

To date, Stuxnet is the most sophisticated cyberweapon ever deployed. Stuxnet's mission was to activate only computers that ran Supervisory Control and Data Acquisition (SCADA) software used in Siemens centrifuges to enrich uranium. The Windows-based worm had a "dual warhead." One part was designed to lay dormant for long periods, then speed up Iran's nuclear centrifuges so that they spun wildly out of control. Another secretly recorded what normal operations at the nuclear plant looked like and then played those recordings back to plant operators so it would appear that the centrifuges were operating normally when they were actually tearing themselves apart.

The worm's sophistication indicated the work of highly skilled professionals. Michael Assante, president and CEO at the National Board of Information Security Examiners, views Stuxnet as a weapons delivery system like the B-2 Bomber. The software program code was highly modular, so that it could be easily changed to attack different systems. Stuxnet only became active when it encountered a specific configuration of controllers, running a set of processes limited to centrifuge plants.

Over 60 percent of Stuxet-infected computers are in Iran, and digital security company Kaspersky Labs speculates that the worm was launched with nation-state support (probably from Israel and the United States) with the intention of disabling some or all of Iran's uranium enrichment program. Stuxnet wiped out about one-fifth of Iran's nuclear centrifuges by causing them to spin at too high a velocity. The damage was irreparable and is believed to have delayed Iran's ability to make nuclear arms by as much as five years. And no one is certain that the Stuxnet attacks are over. Some experts who examined the Stuxnet software code believe it contains the seeds for more versions and attacks.

According to a Tofino Security report, Stuxnet is capable of infecting even well-secured computer systems that follow industry best practices. Companies' need for interonnectivity between control systems make it nearly impossible to defend against a well-constructed, multi-pronged attack such as Stuxnet.

And Stuxnet is not the only cyberweapon currently at work. The Flame virus, released about five years ago, has been infecting computers in Iran, Lebanon, Sudan, Saudi Arabia, Egypt, Syria, and Israel. While researchers are still analyzing the program, the attack's main goal is stealing information and espionage. Flame is able to grab images of users' computer screens, record their instant messaging chats, collect passwords, remotely turn on their microphones to record audio conversations, scan disks for specific files, and monitor their keystrokes and network traffic. The software also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. These data, along with locally stored documents, can be sent to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.

The Duqu worm, discovered in September 2011, also aims to steal information by scanning systems. Duqu infects a very small number of very specific systems around the world, but may use completely different modules for infiltrating those separate systems. One of Duqu's actions is to steal digital certificates used for authentication from attacked computers to help future viruses appear as secure software. It is going largely undetected. Security researchers believe Duqu was created by the same group of programmers behind Stuxnet.

The real worry for security experts and government officials is an act of cyberwarfare against a critical resource, such as the electric grid, financial systems, or communications systems. (In April 2009, cyberspies infiltrated the U.S. electrical grid, using weak points where computers on the grid are connected to the Internet, and left behind software programs whose purpose is unclear, but which presumably could be used to disrupt the system.)

The U.S. has no clear strategy about how the country would respond to that level of cyberattack, and the

effects of such an attack would likely be devastating. Mike McConnell, the former director of national intelligence, stated that if even a single large American bank were successfully attacked, it would have an order-of-magnitude greater impact on the global economy than the World Trade Center attacks, and that the ability to threaten the U.S. money supply is the financial equivalent of a nuclear weapon.

Many security experts believe that U.S. cybersecurity is not well-organized. Several different agencies, including the Pentagon and the National Security Agency (NSA), have their sights on being the leading agency in the ongoing efforts to combat cyberwarfare. The first headquarters designed to coordinate government cybersecurity efforts, called Cybercom, was activated in May 2010 in the hope of resolving this organizational tangle. In May 2011 President Barack Obama signed executive orders weaving cyber capabilities into U.S. military strategy, but these capabilities are still evolving.

In 2014, a virus similar to Stuxnet called Energetic Bear was found to have attacked energy companies in the U.S. and Europe, lending credence to fears the the energy grid is vulnerable to these kinds of attacks. It's one thing to develop a next-generation computer virus, but another one to develop methods of defending established computer systems from them. Will the United States and other nations be ready when the next Stuxnet appears?

Sources: Michael B. Kelley, "A Stuxnet-Like Virus Has Infected Hundreds of US and European Energy Companies," Businessinsider.com, July 1, 2014; Brian Royer, "Stuxnet, the Nation's Power Grid, and the Law of Unintended Consequences," *Dark Reading, March* 12, 2012; Thomas Erdbrink, "Iran Confirms Attack by Virus That Collects Information," *New York Times*, May 29, 2012; Nicole Perlroth, "Virus Infects Computers across Middle East," *New York Times*, May 28, 2012; Thom Shanker and Elisabeth Bumiller, "After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action," *New York Times*, July 15, 2011; Robert Leos, "Secure Best Practices No Proof Against Stuxnet," CSO, March 3, 2011; Lolita C. Baldor, "Pentagon Gets Cyberwar Guidelines," Associated Press, June 22, 2011; William J. Broad, John Markoff, and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011; George V. Hulme, "SCADA Insecurity" and Michael S. Mimoso, "Cyberspace Has Gone Offensive," *Information Security's Essential Guide to Threat Management* (June 14, 2011); and Sibhan Gorman and Julian A. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 31, 2011.

CASE STUDY QUESTIONS

1. Is cyberwarfare a serious problem? Why or why not?
2. Assess the management, organization, and technology factors that have created this problem.
3. What makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
4. What solutions have been proposed for this problem? Do you think they will be effective? Why or why not?

Click Fraud

When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its products. **Click fraud** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising.

Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking, and botnets are often used for this purpose. Search engines such as Google attempt to monitor click fraud but have been reluctant to publicize their efforts to deal with the problem.