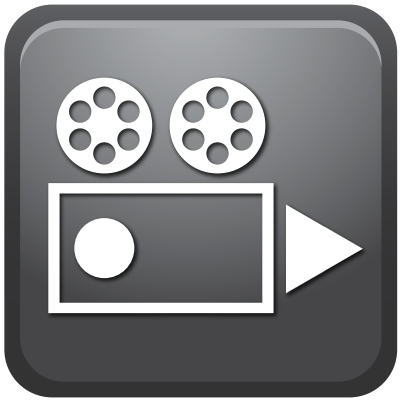
CHAPTER 8 SECURING INFORMATION SYSTEMS

CASE 1

Stuxnet and Cyberwarfare



SUMMARY Cyberattacks against major U.S. firms and government agencies have demonstrated the difficulty of keeping domestic systems secure. These same techniques can be used in cyberwar, where one nation attacks another by dealing decisive blows against its infrastructure. Stuxnet was one of a family of software viruses launched by the United States and Israel in 2010 against Iranian nuclear centrifuges and other industrial facilities that are used to concentrate nuclear fuel to nuclear bomb-grade quality. The Stuxnet event in 2010 was arguably the first documented instance of one nation attacking another using computer software. In 2011 and 2012, Stuxnet became a powerful symbol of a newly emerging weapon and style of war.

(a) Cyberwar | Amy Zegart | TEDxStanford

URL https://www.youtube.com/watch?v=JSWPoeBLFyQ; L=8:41

(b) "60 Minutes" investigates cyber-warfare

URL https://www.youtube.com/watch?v=kw--zLJT3ak; L=5:52

CASE The list of cyberattacks against business firms and government agencies keeps growing: DDoS attacks, Trojans, phishing, ransomware, data theft, identity theft, credit card fraud, and spyware. Less well known is that nations are planning to use these same techniques to bring down the infrastructure of their real and perceived enemies. All advanced societies rely on the Internet to operate water systems, electrical grids, train and airplane control systems, logistics systems, medical, and financial systems. The growth of the Internet of Things

continued

(IoT) greatly expands the reach of the Internet to automobiles, appliances, aircraft, and shipping. If these systems could be made inoperable, even for a short time, societies and economies would collapse in a matter of weeks. Civilian casualties would quickly mount, civilian government would be crippled, and military systems made ineffective or inoperable. Ironically, even relatively small countries can present these kinds of threats to much larger and more powerful countries.

The Stuxnet worm is a high-visibility example of the use of malware (viruses) to disrupt an industrial process in an advanced country. It is an example of cyberwarfare because it was launched by one nation against another nation with the intent of causing harm to the civilian and military capabilities of the target nation.

First discovered in June 2010, Stuxnet was designed to disable the computers that control the centrifuges in Iran's uranium enrichment process. Many commentators believe Stuxnet was created by a joint United States–Israel operation code-named Olympic Games. Iran has reported the virus caused Siemens' industrial centrifuges to spin out of control and eventually destroy themselves. The virus works by infecting industrial control devices called "programmable logic controllers," or PLCs, in this case also made by Siemens. PLCs are used through the industrial and developing world as a basic machine control unit that usually is attached to, or close by, a computer control machine tool, such as a lathe, cutting tool, robot, or centrifuge. The PLC contains software that connects it to the factory's network (or Internet), which in turn allows managers in offices to control and monitor machine operations.

In another strike against Iran in April 2012, malware wiped computers in the Iranian Oil Ministry and the National Iranian Oil Company clean. Initial reports identified the malware as a Trojan dubbed Flame. Flame was suspected of pursuing multiple Iranian objectives including key oil export hubs. Iran's National Computer Emergency Response Team released a tool to detect and destroy Flame in early May.

Although cyberattacks are reported as discrete incidents, they are in fact ongoing activities punctuated by major events. In the United States, the public Web, air-traffic control systems, healthcare, and telecommunications services have all been attacked. Both China and Russia have been caught trying to infiltrate the U.S. electric-power grid, leaving behind software code to be used to disrupt the system. In July 2010, after 10 years of debate, 15 nations including the United States and Russia agreed on a set of recommendations that, it was hoped, would lead to an international treaty banning computer warfare. Despite agreement on principles, the nations involved have not proposed nor approved a treaty.

Powerful states can launch cyberattacks but cannot easily defend against them. Offense has the advantage. First strike is an attractive option. Perhaps because this is so, the United States and China have conducted two cyberwar game events, with a third in the works. Designed as a preventative measure against a conventional arms confrontation should either side feel threatened in cyberspace, they gave the United States the opportunity to

continued

confront China about its cyberespionage, apparently to little effect. According to Jim Lewis, director of the Center for Strategic and International Studies think tank, which coordinated the games in conjunction with a Chinese think tank, China believes the United States is in decline, putting it in the one-up position. Organizing the games through think tanks rather than government channels enables government and intelligence agency officials to meet in an atmosphere that allows for candid discussion as opposed to more formal talks. Dubbed "Track 1.5" diplomacy, events such as these allow the Chinese to express that they too have been afflicted by cyberespionage and believe they have been unfairly scapegoated. Participants of the first event were tasked with developing a response to a cyberattack from a malware agent such as Stuxnet. In the second, they were specifically asked to outline their response if they knew that the attack had been perpetrated by the other party. This purportedly went poorly. Lewis' impression is that the present balance of power in China favors factions that support conflict over those that support cooperation.

With the United States refocusing its military attention on China as a dual cyber-weapon/conventional military threat, any attempt to reduce the distrust and ignorance that fuel arms races are welcome. Even if a complete ban on cyberweapons is unrealistic, measures such as prohibiting infrastructure and financial system attacks might be achievable. Better yet, persuading nations to agree that cyberweapons should be banned, just as poison gas and nuclear weapons have been either banned or controlled. An international treaty seems our best hope of avoiding MAD 2.0, the modern version of the Cold War era "mutually assured destruction," in which cyberoffensive actions are utilized to destroy other countries' Internet and other critical infrastructure. Because most nations cannot survive these attacks, it makes little sense to use them.

VIDEO CASE QUESTIONS

1. What are the three classes of cyberattacks and their effects, according to the Zertag video?
2. What are the five differences between cyberwarfare and traditional warefare?
3. Why is the Stuxnet event considered to be historic?
4. What is a danger that the creators of Stuxnet have created for other industrial counties, including the United States? What is the greatest fear created by Stuxnet?
5. Why are people (agents) needed "on the ground" in order for the Stuxnert virus to work?
6. Why did Iran, and American commentators, not consider Stuxnet an act of war?

continued