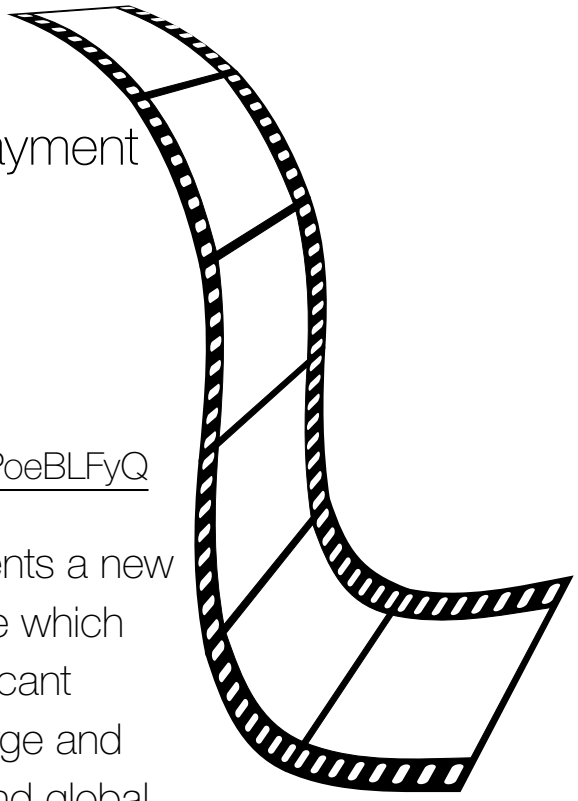
video case



chapter 5 E-commerce Security and Payment Systems

case 5.1 The Rise of Cyberwarfare

watch the video at https://www.youtube.com/watch?v=JSWPoeBLFyQ

summary The Stuxnet family of viruses represents a new type of weapon and style of war, one which threatens to become the most significant threat we face from enemies both large and small. Cyberattacks on major U.S. and global companies have become more commonplace, but as the Internet of Things grows in size and scope, the capacity for cybercriminals to wreak havoc on infrastructural targets will grow along with it. L: 16:53.

case In recent years, cyberwar has left the realm of science fiction and has become the cold, hard reality of the modern age. Every statistic having to do with the increase in frequency and size of cyberattacks is on the rise. In 2015, hackers targeted eBay, Home Depot, JPMorgan Chase, Anthem Health, and even the White House, exposing personal information

continued

belonging to thousands of customers of these companies. But unlike past examples of warfare, the online battlefield doesn't just belong to the strongest nations, although the U.S., China, and Russia are all actively engaged in both offensive and defensive cyberwar efforts.

The battlefield of the Internet has reduced differences between the strongest and weakest nations to a significant degree, and even one of the poorest countries on earth, North Korea, was alleged to have executed a successful attack on Sony's U.S. division, stealing, releasing, and destroying terabytes of private data. The reason behind the attack was the pending release of the movie *The Interview*, a comedy starring James Franco and Seth Rogen which depicts the assassination of Korean leader Kim Jong-un. An anonymous group calling themselves the "Guardians of Peace" orchestrated the attack, wreaking havoc on Sony's entire organization and insisting that *The Interview* be canceled. Sony eventually canceled the New York City premiere of the film and other major theater chains balked at screening the film. Although the film was eventually released across a very low number of theaters and featured major revisions to the plot, the attackers were largely successful in their goals.

Between bot networks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity theft, credit card fraud, and spyware, there's no shortage of ways for cybercriminals to make an impact online. However, as cybersecurity expert Amy Zertag explains in this video, the difference between these types of attacks, which can be extremely annoying to the victims and have major implications for e-commerce, and the next wave of cyberattacks, which have the potential to damage or destroy important components of national infrastructure, is significant. Restoring a stolen identity is annoying, as anybody who's had to do it understands. Canceling or interfering with a movie release has dire implications for creative expression. But attacks to systems such as self-driving car guidance systems, airplanes, or municipal power and water supplies, all of which are increasingly becoming computerized and automated, could have much more serious consequences.

The Stuxnet worm, which destroyed thousands of Iranian nuclear centrifuges in an effort by the U.S. and Israel to cripple Iran's nuclear program, was an example of this type of attack in action. While it was successful in this regard, it was also a proof of concept of this type of attack, and similar attacks have been made against industrial control modules, computer systems, and networks. The world is moving towards the Internet of Things, where everyday objects such as TVs, thermostats, appliances, cars, and other equipment gain the ability to connect to the Internet and share information. The potential applications of these technologies to improve our lives are limitless, but the Internet of Things also creates a whole new area of attack for potential cybercriminals.

continued

video case questions

1. What are the three classes of cyberattacks and their effects, according to Zertag?
2. What metaphor does Zertag use to describe the idea that online, there are "no safe neighborhoods?" What does she mean?
3. What does Zertag mean when she says that the Internet has a "huge attack surface"? How will the "Internet of Things" exacerbate this issue?
4. What are the five differences between cyberwarfare and traditional warfare, according to Zertag?