10

Cybersecurity Policies and Legal Issues

Learning Objectives

1. Discuss the purpose of national cybersecurity laws.
2. Describe the purpose of national cybersecurity policies.
3. Discuss the tension between civil rights and national security.
4. Explain the difficulties in creating and enforcing international cybersecurity policies.

In the past decade, our world has become interconnected not only via computer networks but also via the IoT. It is expected that by 2020 there will be 20 billion IoT devices. Most of us carry at least one IoT device with us, but many of us carry several devices, including a smartwatch, a smartphone, a health tracker, an iPad, etc. Our smartphones can now open the front door, turn the house alarm on and off, monitor packages delivered to our door, monitor our children's whereabouts, locate family and friends, access our bank accounts, pay bills, and so on. We will soon be able to drive to school or work in driverless cars, trains, and buses. We will be able to divert energy sources from one town to another. These are incredible technological advances that will greatly improve our lives, but there are also costs attached to these advances—costs that can endanger our lives. Cybersecurity experts are working hard to keep up and develop security measures that will keep criminals from launching cyberattacks, including terrorist acts.[3] Just imagine you are riding in a self-driving bus and the bus is hijacked by a hacker who takes over control of the bus. The hacker could do that from anywhere in the world. He does not need to be near or inside the bus. He could make the bus go faster or change the destination, drive it into other cars or down a cliff. Researchers have shown that it is possible to hack into today's connected

THINK ABOUT IT 10.1

Mirai: A Shot Across the Bow—Distributed Denial-of-Service Attack

IMAGE 10.1 ● Mirai Botnet

Mirai Botnet Linked to Massive DDOS Attacks by Joey Devilla, https://upload.wikimedia.org/wikipedia/commons/3/36/Mirai-botnet-linked-to-massive-ddos-attacks-on-dyn-dns-gif.gif. Licensed under CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0/legalcode

On October 21, 2016, a massive distributed denial-of-service (DDoS) attack brought down much of the Internet in Europe and the United States. Some of the most popular websites, such as Amazon, Twitter, Reddit, CNN, PayPal, Fox News, the *New York Times*, the *Guardian*, and the *Wall Street Journal*, were unavailable for several hours. This outage also included Amazon's cloud-based service, which has become essential data storage for many large businesses. If businesses can't access their data, they lose money. If health care providers can't access patient records, people could die. Thus, a DDoS attack can have detrimental consequences.[1]

The attack used a botnet named Mirai. Mirai was not the typical botnet made up of computers; rather, it used devices that are part of the Internet of things (IoT) to overwhelm the servers of big companies with service requests until the servers broke down. These devices were mainly home Wi-Fi routers, connected video cameras, and other private home devices. The Mirai botnet was the largest of its kind thus far, but given the enormous growth of IoT devices, it will soon be outmatched by a new botnet. The Mirai botnet of IoT devices bombarded the server of a company called Dyn until the server crashed under the incoming attack traffic. Dyn controls much of the Internet's Domain Name System infrastructure. Experts from Dyn estimated that the Mirai botnet used at least 100,000 endpoint devices (e.g., home video cameras, etc.) and generated more than 1.2 terabytes per second traffic. The Dyn server sustained the pressure for almost an entire day until it broke down. David Fiedler from the Council of Foreign Relations stated:

> We have a serious problem with the insecurity of IoT devices and no real strategy to combat it. The IoT insecurity problem was exploited on this significant scale by a non-state group. Imagine what a well resourced state actor could do with insecure IoT devices.[2]

What Would You Do?

1. Give some examples of what a well-resourced state actor could do with insecure IoT devices.
2. What would be the consequences if a botnet similar to Mirai were to bring down the Internet for more than one week? How would it affect your life if there were no Internet?
3. Think back to prior chapters. What can you do to prevent your IoT devices from becoming infected by malware and being abused in a DDoS attack?

cars and take away the control of the driver. Cybersecurity experts will have to work closely with companies that build self-driving and connected vehicles to make them as safe as possible.

The past decade has seen a rapid increase in cyberattacks by hackers, terrorist groups, nation-states, and other actors. As you have learned in the prior chapters, these attacks have become more sophisticated and dangerous, and are now part of everyone's life. One of the main questions widely discussed is how to make the Internet safer. Some argue that the Internet needs to be strictly regulated; others believe that we need a holistic approach to this issue. The holistic approach includes cooperation between the industry, lawmakers, and cybersecurity specialists. The holistic approach emphasizes that neither technology nor policies in themselves can effectively address the myriad of cyberthreats. Over the past decade, cyberthreats have grown in number and also in sophistication with a widening range of victims, the growth of social engineering, and the increased threat of insiders (as discussed in prior chapters).[4]

The holistic approach encompasses technological, human, and physical factors. All cyberattacks are planned and executed by human beings, and almost all cyberattacks target humans to get access to a computer, server, or network. The Internet has vastly expanded the opportunities for corporations and individuals for business ventures, innovations, and sharing of data, but it has also increased access to individuals and organizations. This access is guarded by humans, who may be the greatest vulnerability with regard to cybersecurity because they must use their good judgment to protect the corporation and the data it holds. The strongest technological security measures cannot prevent an attack if the humans who are operating the technology make bad decisions.[5]

CASE STUDY 10.1

A Holistic Approach to Cybersecurity

A holistic approach integrates technological, human, and physical factors.

1. Assessing vulnerabilities, cyber resiliency, and developing a security baseline

The corporation is not an association of computers and other devices on a network, but rather an association of people who work within a physical domain and who control the technical domain. Part of this assessment is to analyze the security culture of a company, its leadership, HR policies and practices, IT governance, physical defenses, and cyberthreat awareness. This information will provide the security baseline to measure against.

2. Identifying sensitive information

The company must first assess its critical assets that need to be protected. Sensitive information includes trade secrets, customer data, patents, and other aggregate data. A company may not be able to protect all data, so it must determine what receives the highest priority.

3. Determining who has access

After the company has prioritized their sensitive information, they must decide who is

(Continued)

(Continued)

allowed access to the information. Many organizations don't realize how many employees have access to their sensitive information, often without any need for access. Restricting virtual and physical access is imperative because the destruction of computers, devices, or a network would accomplish the same as a DDoS attack—the denial of access to the data.

4. Developing and disseminating ground rules and accountability

The ground rules must lay out precisely what people should and should not do. The accountability rules must clearly state the consequences for negligent and intentional violations. If people are not held accountable, there is also no incentive to follow the rules.

5. Cybersecurity awareness of employees

Employees are the greatest security threat. Most security breaches occur due to negligence. Cybersecurity training mitigates the risk by creating awareness of attack strategies.

6. Addressing the insider threat

Even though most cyberattacks occur due to negligent behaviors, the ones that are malicious cause more significant damage, often by giving away trade secrets and the most sensitive information. The most effective countermeasures are a positive cybersecurity culture and broad monitoring of access to information and employee behavior with regard to downloaded files and badge records. Closely monitoring employee online behaviors clashes with privacy concerns, and many companies do not engage in close monitoring to avoid conflict and attrition of employees. This lack of supervision, however, makes it relatively easier to steal sensitive information or manipulate data.

7. Cyberattack response

Companies must be aware that cyberattacks can happen at any time despite good cybersecurity measures and must prepare for such attacks by implementing a response protocol that everyone in the company follows. One of the first steps of the response protocol should be the assessment of the damage, followed by informing shareholders and partners, and following the response protocol to mitigate damages and restore the normal functioning of the network.[6]

National Cybersecurity Policies

Several laws have been passed in the last few years to more effectively address cybercrime and cybersecurity issues. The main purpose of these was to develop a comprehensive strategy to prevent and mitigate cyberattacks. Further, several new laws require regular assessment of the cybersecurity workforce and recruitment strategies. Another focus has been on streamlining regulations for critical infrastructures.

Comprehensive National Cybersecurity Initiative, 2008

The Comprehensive National Cybersecurity Initiative (CNCI) provided the basis for a comprehensive cybersecurity strategy. The CNCI developed three mutually reinforcing initiatives:

1. To establish a front line of defense against today's immediate threats.

"Creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions."

2. To defend against the full spectrum of threats.

   "Enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies."

3. To strengthen the future cybersecurity environment.

   "Expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace."[7]

On December 18, 2015, President Obama signed the Cybersecurity Information Sharing Act of 2015 (CISA), which creates a cybersecurity information-sharing system for public and private entities. Reporting is voluntary, and the Act guarantees the confidentiality of sensitive information, including the sources and methods of reporting. Four government agencies are working together: the director of National Intelligence, the secretary of Homeland Security, the secretary of defense, and the attorney general. The main task of this workgroup is to develop procedures for the sharing of classified and unclassified cyberthreat indicators and defense mechanisms. They are also responsible for sharing best practices for mitigating cyberthreats.[8] Critics of CISA have argued that Internet users have privacy rights and that their Internet traffic, such as searches and communications, ought to be private, similar to a phone call made from a public phone. The Fourth Amendment guarantees that people are secure from unreasonable search and seizure of their private communications. The question is whether communications sent through a third party are considered private. The government says no because it has been voluntarily disclosed to the third party. This argument, of course, ignores the fact that it is virtually impossible to e-mail another person without using a third-party Internet service provider (ISP).[9]

In addition, the FBI has formed the cyber task force, working to build alliances between governmental agencies and private companies across the United States. The "whole-government approach" is imperative to countering cyberthreats and keeping people safe. Cybercriminals are versatile, using real-world events such as the terrorist attacks in Paris, France, to solicit fraudulent donations, creating fake government websites to get individuals' private information (e.g., tax reporting websites during tax time), or payroll scams where individuals are notified that they need to confirm a change in their employment status. Once the individual logs into his or her account, the criminal has the login information and the ability to steal paychecks and personal information.[10]

Cybersecurity Workforce Act of 2014

The Cybersecurity Workforce Act was signed into effect on December 18, 2014. The Act requires the secretary of Homeland Security to assess the work of the cybersecurity workforce of the Department of Homeland Security (DHS) and

CASE STUDY 10.2

Ransomware—California Hospital Pays $17,000

Ransomware has become one of the most feared threats to cybersecurity. In the context of ransomware, cybercriminals take a computer or device hostage until the owner pays a ransom. The cybercriminals are very effective because if the ransom is not paid, the criminals can steal or delete the content of the computer or device. On February 5, 2016, Hollywood Presbyterian Hospital in Los Angeles noticed that their computer systems had been hacked and that the hackers were interfering with the operation of their computer systems. The hackers had encrypted the data, and even the FBI's attempts to decrypt the data were unsuccessful. Doctors had no access to e-mail and patient records for more than 1 week. The hospital eventually paid 40 bitcoins, which is $17,000, in exchange for the decryption key.[11]

develop a comprehensive strategy to improve the readiness and quality of the cybersecurity workforce. The secretary must conduct such assessment within 180 days of the signing of the law and annually for the following 3 years. The Act focuses on the following issues:

1. "The readiness and capacity of the cyber security workforce to meet its cyber security mission;
2. Where cyber security workforce positions are located within DHS;
3. Which such positions are performed by permanent full-time equivalent DHS employees, by independent contractors, and by individuals employed by other federal agencies;
4. Which such positions are vacant;
5. The percentage of individuals within each Cyber Security Category and Specialty Area who received essential training to perform their jobs; and
6. In cases in which such training was not received, what challenges were encountered regarding the provision of such training."[12]

National Cybersecurity and Critical Infrastructure Protection Act of 2014

The National Cybersecurity and Critical Infrastructure Protection Act of 2014 was also signed into effect on December 18, 2014. The Act enables the secretary of Homeland Security to conduct cybersecurity activities that will defend, mitigate, respond to, or recover from cyber incidents to critical infrastructures such as chemical plants; dams; the Defense Industrial Base Sector; nuclear reactors, materials, and waste; and transportation systems. A cyber incident is defined as

> an incident, or an attempt to cause an incident, that if successful, would: (1) jeopardize the security, integrity, confidentiality, or availability of an

THINK ABOUT IT 10.2

Ransomware

You are the owner of a small business selling home improvement goods. You receive a notice on your computer that your data has been encrypted. That data includes your customer data, payment information, orders, and supplies. It also means that you cannot access the data of your employees. The hacker asks for a ransom of $500.

What Would You Do?

1. Make a list of the benefits and risks of paying the ransom.
2. Make a decision on whether to pay the ransom. Justify your decision.
3. Discuss the implications of these decisions made by small business owners for cybercriminals and cybersecurity.

IMAGE 10.2 ● Ransomware

© iStockphoto.com/Chesky_W

information system or network or any information stored on, processed on, or transiting such a system; (2) violate laws or procedures relating to system security, acceptable use policies, or acts of terrorism against such a system or network; or (3) deny access to or degrade, disrupt, or destruct such a system or network or defeat an operations or technical control of such a system or network.[13]

The secretary of state has the responsibility to coordinate federal, state, and local governments, laboratories, critical infrastructure owners and operators, and other entities to accomplish the following goals:

1. "Facilitate a national effort to strengthen and maintain critical infrastructure from cyber threats;
2. Ensure that Department of Homeland Security (DHS) policies and procedures enable critical infrastructure owners and operators to receive appropriate and timely cyber threat information;
3. Seek industry sector-specific expertise to develop voluntary security and resiliency strategies and to ensure that the allocation of federal resources

is cost effective and reduces burdens on critical infrastructure owners and operators;

4. Upon request, provide risk management assistance to entities and education to critical infrastructure owners and operators; and
5. Coordinate a research and development strategy for cyber security technologies."[14]

Even though the past 2 years have seen a surge in cybersecurity laws, overall the law has been slow to catch up with cybercrime and its constant and fast-paced changes. By the time the U.S. government signs a new law, the cybercriminals and nation-state actors have long moved on to new techniques. In addition, corporations are unwilling to invest the money it takes to develop cybersecurity measures and protect the data on their servers. It is typically not until a company has to admit a major attack and the theft of private data that can be used for identity theft that the company begins to implement sophisticated cyberdefense mechanisms.

Some suggest that the government must force corporations to implement a certain cybersecurity standard. Without such policies, corporations will not invest in cybersecurity, and vulnerabilities will remain. Great Britain was the first country to show 20 national banks just how vulnerable they are and force them to implement cybersecurity measures. It announced to the banks that they would be attacked—not by hacktivists or someone else but by hired white-hat hackers. The Bank of England rehearsed a major hacking attack called Walking Shark II by employing 220 hackers to attack the 20 banks.[15]

International Cybersecurity Policies

Cyberspace and cybersecurity defy traditional governance because they are not confined within national borders; rather, they reach across geopolitical boundaries. This raises three main issues:

1. Who can make the law applicable to cyberspace and cybersecurity?
2. What law applies?
3. Who can enforce the applicable law?

In addition, there is a codependence of the government and private sector in which many private assets are detrimental to the public, and their security is of great importance to the government. For instance, many critical infrastructures are privately owned, but the government helps protect them. Proprietary information, such as company research, trade secrets, hardware, and software, is mostly owned by private companies, but the government has an interest in protecting this information. When cybercriminals steal or manipulate data or interfere with company operations, the main challenges that investigators face are anonymity and attribution. The anonymity of cyberspace makes it often impossible to determine who the criminal is and prove it.[16]

LEGAL ISSUE 10.1

THE CYBERWARS IN THE MIDDLE EAST

Most experts in the field seem to agree that the first real cyberwar attack occurred in January 2010 at the Natanz uranium enrichment plant in Iran. This was a new type of attack because it wasn't done by bombing the plant but rather by attacking the software. The attacker, even though it has not been officially admitted, is believed to have been the United States. The malware Stuxnet disrupted the centrifuges of the nuclear power plant while at the same time manipulating the computer control screens to show that everything was normal. But everything was not normal. One after another of the centrifuges spun out of control. By the end of the attack, more than 800 of the plant's centrifuges were destroyed by the malware, bringing to a halt the production of enriched plutonium, which is needed to produce energy but also to build an atomic bomb. It was the potential of building an atomic bomb that had sparked the cyberattack. The attackers were hoping that no one would ever be able to figure out what happened and that the software would stay within the plant. This did not happen, however. Instead, the most advanced cyberweapon at the time spread across the world and became widely available to anyone.[17]

The Counterattack

In a counterattack, Iran, in 2012, attacked the U.S. banking system and substantially slowed down major banking websites of the largest U.S. banks, including the Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank, and PNC Bank. Some banks' websites were completely inaccessible, making online banking impossible. It is believed that hackers working for the Iranian government used a DDoS attack to overwhelm the servers.[18]

In the aftermath, JPMorgan Chase announced that it spends $850 million per year and employs 1,000 security employees. Despite the large amount of money and security personnel, JPMorgan could not prevent the attack. During the attack, the banks turned to the U.S. government and asked for help, but the government told the banks that this was their problem. The banks turned to Internet service providers such as AT&T and asked them to help. They tried and failed. Eventually, the attack stopped, not because the banks or the U.S. government stopped it but because the Iranians ended it. They could have continued the attack, but they had made their point. The Iranian government had sent a message to the United States that they had the capability to attack and disrupt one of America's most important businesses: the banking industry. The U.S. government had created an offensive cyberunit as part of the military, but they had not built a cyberdefense system that would protect American citizens and corporations from potentially devastating cyberattacks by other nation-states or nonstate actors.[19]

Lessons Learned

When nation-states build a cyberunit, they put their money into creating offensive capabilities so they can attack their enemy. But the lack of cyberdefense systems leaves the corporations and government agencies vulnerable to the simplest attacks. Another lesson was learned by the banks and other corporations. Their takeaway was that if they come under attack, they should not count on the help of the government.[20] This lesson was also learned by Sony when it was attacked by North Korea over the release of the movie *The Interview*, which depicted the assassination of North Korean leader Kim Jong-un. The hackers stole data from the Sony servers, including executive e-mails and private data about actors such as salaries, addresses, etc. The data was then released online via social media, exposing very personal information. Stunned by the sophistication of the attack and threats by North Korea, Sony caved and cancelled the release of the movie.[21]

What Do You Think?

1. Would international agreements help prevent a cyberwar? How would these agreements be similar and different to other international agreements that cover wars, such as the Geneva Convention?
2. Should the U.S. government protect its citizens and corporations, and if so, how could they do that?

Legal Issues

Civil Rights

On November 14, 2015, the Islamic State (ISIS) killed 130 people in a terrorist attack in Paris, France. The terrorists attacked the citizens of Paris in six locations, with the first attacks at 9:20 p.m. outside of the Stade de France, a sports stadium where the French soccer team was playing against Germany. French President Hollande, who was in attendance, was safely evacuated and the stadium secured. The second explosion followed at 9:30 p.m. about 400 feet away from the stadium. Both suicide bombers and one person walking by died during the explosions. At 9:53 p.m., the third suicide bomber launched an explosion in the Rue de la Cokerie, injuring several people. The real attack, however, was yet to come and would last until 12:20 a.m. the following day. The first two targets, La Petit Cambodia and Le Carillon, were hit at 9:25 p.m. Men armed with automatic rifles killed 15 people. They then moved on to Café Bonne Biere, killing another five people. At 9:40 p.m., another single suicide bomber walked into a restaurant, Comptoir Voltair, and detonated his bomb. Several people were injured. Another group of three terrorists stormed the Bataclan concert hall where the U.S. band Eagles of Death Metal played before hundreds of people. The terrorists started shooting into the crowd, killing a total of 89 people. Eyewitnesses would later report that the terrorists shot people who were laying on the floor in execution style. The attack ended at 12:20 a.m. when French police stormed the concert hall. They killed one of the attackers immediately. The other two activated their suicide belts before the police could get to them.[22]

Reference Reading

The Real Story of Stuxnet

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Following the attack, FBI director James Comey warned that ISIS may also have cyberwar capabilities, which could be a threat to the United States. He stated, "Destructive malware is a bomb, and terrorists want bombs." There has been an increased presence of ISIS on social media trying to recruit persons, and there is a growing encryption of communication between ISIS and recruits. In an effort to gain intelligence about possible future terrorist and cyberattacks, the FBI has been critical of privacy rights because it leaves the FBI and other law enforcement agencies without information necessary to prevent an attack.[23]

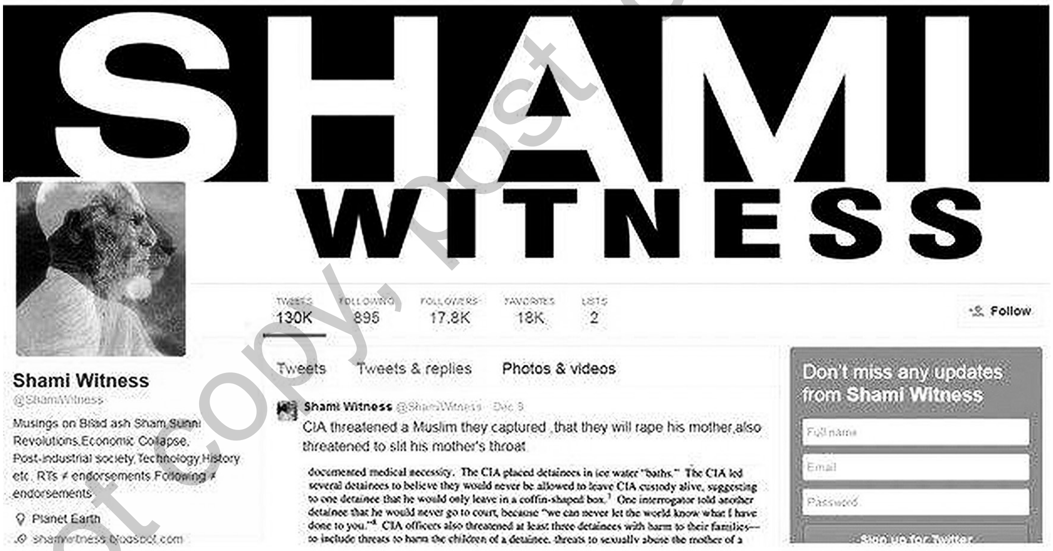
IMAGE 10.3 ● Privacy Versus Security

Pixaby.com

Security Versus Privacy

And herein lies the crux of the problem: What is the importance of civil rights and the importance of public safety? Which has priority if both can't be accomplished simultaneously? In 2014, the man behind ShamiWitness, the most influential pro-ISIS Twitter account, was arrested and the account shut down. He had more than 17,700 followers, many of whom were foreign fighters. He helped them before they joined ISIS and praised them as martyrs if they died. The man behind the account was Mehdi Biswas, an executive for an Indian conglomerate in Bangalore, India. Biswas also had Facebook accounts, one for his family and friends where he shared jokes and stories, and one where he promoted ISIS, terrorism, and rape. One of his tweets stated: "@ArjDnn I should thank PKK for recruiting female fighters, especially the ones caught alive by rebels, lol." The PKK is a Turkish separatist group who has been fighting against ISIS in Syria. The PKK has been coordinating their efforts with the American military.[24]

IMAGE 10.4 ● Shami Witness Screenshot



Shami Witness
@ShamiWitness
Musings on Bilad ash Sham,Sunni Revolutions,Economic Collapse, Post-industrial society,Technology,History etc. RTs ≠ endorsements Following ≠ endorsements
Planet Earth
shamiwitness.blogspot.com

Shami Witness @ShamiWitness · Dec 9
CIA threatened a Muslim they captured ,that they will rape his mother,also threatened to slit his mother's throat

documented medical necessity. The CIA placed detainees in ice water "baths." The CIA led several detainees to believe they would never be allowed to leave CIA custody alive, suggesting to one detainee that he would only leave in a coffin-shaped box.[7] One interrogator told another detainee that he would never go to court, because "we can never let the world know what I have done to you."[8] CIA officers also threatened at least three detainees with harm to their families—to include threats to harm the children of a detainee, threats to sexually abuse the mother of a

Shami Witness

Biswas also repeatedly tweeted videos of the execution of U.S. aid worker Peter Kassig, who was killed in Syria by ISIS fighters together with dozens of Syrian soldiers. Kassig had served in the Iraq War as an army ranger and later became an emergency medical technician. He founded the Special Emergency Response and Assistance Organization, which delivered medical supplies to northeastern Syria. Kassig was kidnapped by ISIS on October 1, 2013, and held hostage in Aleppo and later in Raqqa together with 23 other Western hostages. Kassig was forced to watch the beheadings of four other hostages in August 2014, and he seemed to know that he would also be killed. In a letter smuggled out in the summer of 2014, he wrote to his parents:

> I am obviously pretty scared to die but the hardest part is not knowing, wondering, hoping, and wondering if I should even hope at all. . . . Just know I'm with you. Every stream, every lake, every field and river. In the woods and in the hills, in all the places you showed me. I love you.

The video distributed by Mehdi shows the body of Kassig and the severed head, indicating that Kassig had been beheaded.[25] British investigators believe that Kassig was killed prior to the beheading because all the other videos showed the actual beheading and also forced the victims to make a statement prior to being killed. Kassig's video was very different, and investigators later saw what appeared to be a gunshot wound on his head.[26]

Mehdi Biswas was arrested by Indian authorities in December 2014. After his arrest, he stated, "No I haven't done anything wrong. I haven't harmed anybody. I haven't broken any laws of my country. I haven't raised any war or any violence against the public.[27]

Biswas's statement reflects a major problem: the right to free speech and privacy versus state interests. Biswas has been charged with cyberterrorism under Section 66F of India's Information Technologies Act. If convicted, he could be sentenced to life in prison. The prosecutor is arguing that Biswas was not simply stating his opinion but supported ISIS and terrorist acts by tweeting pictures and videos, encouraging others to join ISIS, and by becoming a meeting place for ISIS fighters and supporters.[28]

Even though most people in the United States support the right to free speech and the right to privacy, for some, this right, in their eyes, ends when public safety is at stake. The term *terrorism* invokes great anxieties and feelings of helplessness. People don't feel safe anymore in their everyday activities, such as shopping and going to a concert or a festival. There is the general sense that the police should keep the citizens safe, and if that can only happen if citizens give up some of their civil rights, then so be it. This reflects very similar fears and opinions to those after the 9/11 attacks, which had sparked the U.S. Congress to promptly pass the USA PATRIOT ACT.

USA PATRIOT Act

The USA PATRIOT Act, under Section 215, gives the government the authority to collect content records related to telephone activities. The government, specifically the National Security Agency (NSA), defined telephone activities much broader than most people would have expected, however. Specifically, any digital information relevant to an investigation was included under Section 215. This interpretation allowed the government to collect vast amounts of metadata from millions of Americans and billions of people around the world, including European government officials such Angela Merkel, chancellor of Germany. Most data collection under Section 215 falls under the jurisdiction of the U.S. Foreign Intelligence Surveillance Court (FISC or FISA). The proceedings and outcomes of FISA court hearings and decisions are not published, meaning that people do not know what the court does or decides. It is in that sense, then, that FISA is a secret court.[29]

When Edward Snowden leaked the widespread snooping by the U.S. government and the secrecy of the FISA court in 2013, many people, and especially citizens of foreign countries who had been spied on, were outraged. As a consequence, the U.S. government passed the USA Freedom Act prohibiting the bulk collection of digital information. This does not preclude the NSA from collecting foreign Internet content from U.S. companies, however. Under the third-party doctrine, the NSA may collect all information that people voluntarily turn over to a third party. This includes sending e-mails by using a third-party Internet service provider, such as Verizon. It also includes messages on Twitter and Facebook, as they are third parties. The Freedom Act also has not changed much with regard to the FISA court proceedings and the ability of the NSA to thwart encryption. The NSA actively discourages corporations from marketing effective encryption tools to the public because encryption would significantly curtail the NSA's ability to read everything people send over the Internet.[30]

LEGAL ISSUE 10.2

UNITED STATES V. WARSHAK

In 2010, Steven Warshak sued the U.S. government for violating his Fourth Amendment rights. In 2006, Warshak had been charged with 112 counts of conspiracy to wire, mail, and bank fraud, making false statements to banks, conspiracy to commit money laundering, and a variety of other crimes. These crimes were related to the business practices of his company Berkley's, which was known for its product "Enzyte," a male enhancement supplement. The prosecution used thousands of e-mails to prove its case. The e-mails had been obtained from Warshak's Internet service provider. Warshak was convicted of the majority of charges, including fraud and money laundering, and sentenced to 25 years in prison. In addition, a forfeiture hearing was held and the jury found that most of Warshak's assets had been obtained through his criminal activities. The judge ordered that Warshak pay a fine of $93,000, surrender $495,540,000 in proceeds/money/judgment, and $44,876,781.68 in money-laundering proceeds.[31]

Warshak appealed his prison sentence and the forfeiture of his assets, and in 2010 his arguments were heard by the Sixth Circuit Court of Appeals. Warshak argued that using e-mails obtained from his Internet service provider violated his Fourth Amendment Rights against unreasonable search and seizure. In *Katz v. United States*, the Supreme Court established a two-pronged test of the right to privacy: (a) a person has "exhibited an actual (subjective) expectation of privacy" and (b) "that the expectation be one that society is prepared to recognize as reasonable" (p. 347).[32] The Katz decision had not been applied to digital communication, however, leaving much private information open to seizure by law enforcement. The Sixth Circuit for the first time extended the right to privacy to e-mails stored with third parties. Despite the Court's conclusion that the government had violated Warshak's Fourth Amendment rights, it did not overturn his conviction based on the grounds that the law enforcement officers had

(Continued)

(Continued)

acted in "good faith" because they believed that the e-mails were not protected by the Fourth Amendment.[33]

Following the Warshak decision, Congressman Kevin Yoder introduced the Email Privacy Act that would amend the Electronic Communications Privacy Act of 1986 to

> prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.[34]

What Do You Think?

1. Discuss the pros and cons of expanding the Fourth Amendment to digital communications.
2. Imagine if the government collected all of your e-mails, posts on Twitter, Facebook, and any other social media website, and charged you with the crime of violating copyright law by sharing music files or downloading pirated software. What would you argue to defend yourself?

Jurisdictional Issues

Universal Jurisdiction

In 2013, the reaction of the Turkish government to a series of protests, called the Gezi protests, across Turkey triggered a number of cyberattacks. The Turkish government had used brute force and tear gas against the protesters. The first cyberattacks came from Anonymous, ColdHaker, and other hacker groups that do not typically act together. The hackers took down the president's website and the website of Turkey's leading party.[35] In 2016, hackers attacked the website of the U.S. Democratic Party, stole e-mails and other confidential information, and released it during the presidential election. Some have argued that this security breach contributed to the loss of the election. This is an arguable position, but the main issue is that such attacks can cause great damage to the economy and democracy of a nation.[36]

There are a number of problems governments across the globe face when such attacks occur. One problem is the issue of attribution. As we have witnessed, it has been very difficult to attribute the cyberattacks to Russia in an attempt to help Trump win the election. Despite all the available resources, intelligence, and technologies, the U.S. government has not been able to present hard evidence, and Russian President Vladimir Putin has denied the attacks. If the cyberattack group does not publicly take responsibility, it is very difficult to determine who the attackers are. Second, a main question is how to react to such cyberattacks and what to do when the attacks originate in a foreign country, making the attackers legally untouchable even if they can be identified. There are no passport checks, border control, or other measures. Thus, traditional governance does not apply. So who makes the laws that apply to cyberspace globally? And how are these laws enforced? Cyberspace also faces the issue of enforcement. If there is a cyberattack, who is responsible for investigating and punishing criminals? Is it the country that was the victim of the attack or the country where the criminal resides? What if the laws with regard to punishment vary substantially between those two countries? This is only a glimpse of the problem of international cybersecurity laws. Not surprisingly, due to the complex nature of cyberspace and geopolitical relations, there is currently no international cybersecurity law. There are, however, some multilateral efforts to tackle cybercrime and cybersecurity.

Budapest Convention on Cybersecurity (2001)

The Council of Europe passed the Budapest Convention on Cybercrime in an effort to establish a uniform law that applies to all signatories. The 50 countries that ratified the convention promised to adopt domestic legislation that would expedite preservation, search and seizure, and interception of data. In addition, the signatories agreed to cooperate with regard to extradition of criminals and access and interception of computer data. Another important part of the convention is the agreement to prosecute cybercrimes committed in the states' territories.[37]

Unfortunately, the Budapest Convention has no teeth—that is, it lacks enforcement mechanisms that would punish violations. It's a symbolic legislation to assure the public that the international community is taking steps to combat cybercrime and the threat of a cyberwar. Unfortunately, adherence to the law is entirely up to the goodwill of the signatory countries, and many countries have taken no steps to implement the provisions of the convention.[38]

Network and Information Security Directive (2016)

In July 2016, the European Union (EU) passed a new Network and Information Security (NIS) Directive establishing the first actual cybersecurity rules. Specifically, the directive regulates network and information security and information sharing. The new NIS directive focuses on critical infrastructures (e.g., energy, transport, health, financial, and digital services) and establishes specific cybersecurity measures. Businesses supplying critical infrastructures are also regulated via the directive and must demonstrate that they have the capability to resist a cyberattack. In addition, the businesses that run or supply critical infrastructures must report all cyberincidents to a national agency. This also includes Amazon and Google and their cloud services. Finally, EU countries have agreed to cooperate on cybersecurity and also build cooperative relationships with service providers.[39]

The main strength of the NIS directive is the ability of the EU to enforce the standards laid out in the NIS directive. Member states have 21 months to implement the standards and an additional 6 months to identify all entities operating critical infrastructures.[40] A major weakness of the directive is its scope. It only applies to countries within the EU. That is a good start, but without a truly international agreement, the impact on cybercrime will be limited.

Issues With Enforcement/Jurisdiction

The response of law enforcement to a terrorist or cyberattack often determines how many people die and are victimized. Cybercriminals and terrorists have been quick to adapt and use available tools such as social media and location services to gain an advantage over law enforcement. The uncontrollable nature of social media poses great challenges to coordinating effective federal and state law enforcement responses to cyberattacks and terrorist acts. The darknet has become the underground Amazon for criminals and nation-states looking for weapons, including cyberweapons such as worms and Trojan horses.[41]

Effective law enforcement responses have been difficult to establish, often due to jurisdictional and geopolitical issues.[42] Every nation-state is a sovereign entity—that is, only law enforcement in that nation has the right to enforce the laws. Similarly, every court only has jurisdiction over crimes that occur in territory under its authority.[43]

If a crime is committed in the United States, only the U.S. government has the right to investigate the crime and arrest the suspect. Even if law enforcement in other countries have an interest in capturing the offender, they cannot simply cross over the border to the United States and arrest the suspect. For instance, Edward Snowden, who released classified information about the U.S. government, is one of the most wanted criminals. Snowden found asylum in Russia, which has declined to extradite Snowden. As much as U.S. law enforcement may want to go to Russia and arrest Snowden, they do not have the right to violate Russia's sovereignty as a nation.[44]

Another problem is that some countries are more developed than others and differ significantly with regard to cybercrime laws. The United States has many more laws against cybercrime than many other nations. If a certain behavior is not a crime in the country where it started, that causes great problems for law enforcement. In 2000, a person from the Philippines released the ILoveYou virus, which damaged files on millions of personal computers around the globe. At the time, there was no law against releasing a virus in the Philippines, and thus, the man had not committed a crime, at least not in the Philippines.[45]

These jurisdictional and geopolitical problems are exacerbated by differences in cultural values between nations. What some nations consider a crime is not considered a crime in others. This difference in political, moral, and constitutional convictions greatly hampers the development of universal enforcement rules. For instance, the U.S. Constitution guarantees the right to free speech and religion. These are not guaranteed rights in numerous other countries. A person in the United States may post a blog with comments that are critical of the Chinese government. In the United States, this is protected speech under the First Amendment. A person in China who reads the blog or even affirmatively responds to the blog may be committing a crime.

Another example relates to sexuality and sexually explicit pictures or pornography. There are many countries in which pornography in all forms is illegal. However, in Europe, the United States, and other countries, many forms of pornography are legal. Someone living in the United States may post pornographic images that are not violating any laws to be viewed by people in nations where such images can result in harsh punishment.[46]

A further problem is that it is very difficult to investigate, prosecute, and punish cybercriminals. Anonymity and identity are the main problems for law enforcement. Even for technologically advanced nations, it is difficult to collect evidence of cybercrimes. The evidence is typically made up of 0s and 1s, and can easily disappear or be changed. The investigator may inadvertently change the evidence simply by examining it, making it useless. For instance, the malicious software may be programmed to self-destruct if accessed by someone other than the criminal. In other cases, the fraudster may erase all logs that would show what happened.[47] Even if evidence of the crime can be collected, this does not necessarily reveal the identity of the criminal. In cases of child pornography, it may be fairly easy to get the evidence, but proving that the person downloaded the images knowingly is significantly more difficult. The suspect can claim that someone else hacked into the computer and stored the illegal images without the user's knowledge.[48] This is certainly possible and does happen. For nations with less-developed technologies, it becomes nearly impossible to determine the identity of the criminal and collect the evidence necessary to punish the fraudster.[49] Even within U.S. law enforcement, the main challenge that has plagued federal and state law enforcement agencies is the development of guidelines to secure the integrity of the agency, improve the training of officers with regard to cybercrime investigations, and develop effective response mechanisms to cyberattacks and terrorist attacks.[50] The investigation of cybercrime is very complex, requiring cybersecurity experts. Traditional law enforcement training does not include such specialized skills. These experts are also highly sought after, and there is an apparent shortage.

LEGAL ISSUE 10.3

LAW OF THE SEA

Some people have suggested applying the law of the sea to cybercrimes. Crimes at sea are similar to cybercrimes in that there is often no clear jurisdiction. In the historical perspective, only a certain part of the sea directly surrounding a nation (a 3-mile radius) was part of the nation's jurisdiction. The rest of the sea was free to all. Thus, there was no regulation of fishing, pollution, natural resources (e.g., oil and gas), and military presence above and under the sea. This began to change at the end of World War I. In 1945, U.S. President Harry S. Truman unilaterally extended the rights to the resources of the sea on the continental shelf. This expansion was in great part due to the pressure from the oil industry, which had realized the enormous potential of underwater oil resources. In 1946, Chile followed the United States in their expansion efforts, and over time, more and more countries expanded their control over the sea. The main industries were oil production and deep-sea fishing but also the search for diamonds and valuable metals. The sea was being exploited as it never had before, which led to conflicts between countries over sea territories, and between countries and environmental activists such as Greenpeace over the pollution of the sea.

On November 1, 1976, the United Nations held their first Conference on the Law of the Sea, but it took until 1982 to adopt the United Nations Convention on the Law of the Sea. The Convention regulates navigational rights, territorial sea limits, economic jurisdiction, legal status of resources beyond national jurisdiction, passing of ships, and preservation of wildlife and seabeds. The Convention also set enforcement rules and is widely regarded as a landmark in international law.

If negotiations between countries fail to resolve a problem, the countries can choose between four options.

1. International Tribunal for the Law of the Sea
2. International Court of Justice

(Continued)

(Continued)

3. Submission to an International Arbitration Procedure
4. Submission to a Special Arbitration Tribunal

In cases where national sovereignty is at issue, states can appeal to the conciliation commission, but they don't have to submit to the decision. However, there is much moral pressure to adhere to the commission's findings.[51]

What Do You Think?

1. Why is the Law of the Sea proposed as a possible solution to jurisdictional issues with regard to cybercrime? Explain.
2. Propose a Law of Cyberspace, including enforcement strategies.

Summary

The last 2 decades could be termed the *decades of the Internet*, as the Internet has developed with lightning speed. The rapid growth of computer technologies, communication infrastructure, and social media has outpaced the legal system and the ability of law enforcement to respond to the dangers posed by the Internet. The main problems for law enforcement and the legal system are attribution, apprehension, and punishment of offenders. Another main issue is the sharing of public assets by private companies and the government, such as critical infrastructures. Protecting companies, individuals, and critical infrastructures is complicated by the fact that cyberspace extends across geopolitical borders and that international coordination on cyber issues is lacking. Even though the EU has begun to cooperate in the fight against cybercrime, the existing conventions are without much force. Different countries have different cultural values, different definitions of crime, and are in different stages of cybercrime preparedness. This is even more complicated at the global level. The trend appears to go toward a regional and national incorporation of treaty-based cybersecurity legal regimes.

Key Term

Cyberincident 195

Discussion Questions

1. Discuss the holistic approach to cybersecurity. What is the focus, and how does it improve cybersecurity?
2. Read "The Real Story of Stuxnet" and discuss the likely consequences of similar attacks on the United States and your life.

3. Discuss the issues related to international jurisdiction, and especially the issue of enforcement of existing international laws. What solutions would you propose?
4. Read Michigan's Cyber Disruption Response Plan. What is the purpose of the plan, and what are the most important steps of the plan?

Internet Resources

United Nations Convention of the Law of the Sea
http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

The Real Story of Stuxnet
http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

State of Michigan Cyber Disruption Response Plan
https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

Further Reading

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). *Cutting the Gordian knot: A look under the hood of ransomware attacks*. Retrieved from https://seclab.ccs.neu.edu/static/publications/dimva2015ransomware.pdf

Nelson, B. (2016). *Children's connected toys: Data security and privacy concerns*. Office of Oversight and Investigations Report. Retrieved from https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf

Wei, J. (n.d.). *DDoS on Internet of Things—A big alarm for the future*. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2016/jwei.pdf

Digital Resources

Want a better grade?

Get the tools you need to sharpen your study skills. Access practice quizzes and eFlashcards, at **study.sagepub.com/kremling**.