

Course Learning Outcomes for Unit I

Upon completion of this unit, students should be able to:

1. Explain how criminal justice theories and technologies impact the commission and solution of crime.
 - 1.1 Define the various cybercrimes and threats.
 - 1.2 Discuss the various classifications of computer crime.
 - 1.3 Evaluate the trends of computer crimes.
4. Examine causes, methods, and criminal justice agency counteractions to terrorism.
 - 4.1 Distinguish cyberterrorism, cybercrimes, and information warfare.
 - 4.2 Discuss the various and specific cyberterrorism risks, past, present, and future.

Reading Assignment

Chapter 1: Introduction and Overview of Digital Crime and Digital Terrorism

Chapter 2: Digital Terrorism and Information Warfare

Unit Lesson

Introduction to Cybercrimes and Terrorism

Cybercrimes and terrorism are evolving every day. In order to remain current on how to protect ourselves, we must stay on top of the threats, resources of the criminals, and our own vulnerabilities. In a world where people went from not locking their front doors to having panic rooms and state-of-the-art alarms, public awareness of cybercrimes remains quite low. Many in the online community have gone from having *password* as their password to unique identifiers. Despite this information, or lack thereof, the most commonly used password remains *password* with the second most popular password being 123456.

The Internet was created by two California Universities to share and conduct a free flow of information with no barriers. It operates on the simple foundation of a series of handshake agreements and trust between users. It should come as no surprise that the Internet was developed in a democratic nation. Though, as in every free society, there are those who seek to take advantage of the freedoms to commit crimes.

In the United States, what responsibility does the federal government have to protect its citizens from the many types of digital crimes? What role should the administration play in Internet governance, protection of the nation's critical infrastructure, and building a ring of defense? In this current day, Internet governance is of critical importance to national security and personal security of the public sector.

Cybercrimes and Threats

Click on the following link to hear a podcast detailing cybercrimes and threats, trends and classifications of computer crimes, the difference between cyberterrorism and cybercrime, and a history of the risks of cyberterrorism.

Please listen to the following podcast about cyberterrorism:
Cyberterrorism (Part I): <http://www.pearsoncustom.com/mct-enterprise/asset.php?isbn=1256689785&id=14645>

Classifications of Computer Crimes

There are many crimes under the large umbrella of the term *digital crimes*. When referring to digital crimes, cyber war, and cyberterrorism, the line tends to get blurred between these terms. A quick search of the Internet reveals that credible media and news outlets seem to use these terms interchangeably. It is easy to see why the layperson might be confused.

The textbook presents you with four classifications to organize these crimes: 1) computer as a target, 2) computer as an instrument of crime, 3) computer as incidental to the crime, and 4) crimes associated with prevalence of computers (Taylor, Fritsch, & Liederbach, 2015).

As you read through the various scenarios presented to you during the course, think about how you would classify each digital crime and where it should be placed under the larger umbrella.

No matter the definition, all digital crimes pose a very real threat to every level of society—from the average person walking down the street, to the top Fortune 500 companies. For example, on the lower level, New York City criminals have moved from pickpocketing to stealing information off of laptops at the corner Starbucks via wireless Internet. At the other extreme, cyberattacks have resulted in the loss of trillions of dollars by American businesses, including the loss of intellectual property and proprietary data.

Cyber war is also an emerging issue in this area. The term cyber war typically involves attacks by nation-states and includes various types of cyber espionage. As evidenced by the American military, the Pentagon receives, on average, one million cyberattacks per day on their systems. An example of one of the first known launches of a cyber-weapon that caused significant damage is the Stuxnet virus. Though not admitted, the United States and Israel were said to have collaborated on the development of Stuxnet and facilitated an attack on Iran's nuclear facilities. In this attack, the computer algorithm was the weapon used, not a drone or bomb. The technology behind the Stuxnet attack was on par with the efforts and intelligence behind the Manhattan Project and could not have been developed by teenagers in a basement.

Though, to blur the lines, nation-states have conducted attacks on American corporations using computers. For example, the Chinese military hacked into Coca-Cola's systems not to steal the famous secret formula, but to take information that they then used in their business negotiations with Coca-Cola during the purchase of the largest bottling plant in China. There are other reported instances of the Chinese government hacking into a number of American competitors to steal proprietary information, which it then handed over to Chinese corporations for them to use to push their competitors out of the market and take over.

At present, there are laws in place to prevent an American corporation from retaliating or *hacking back*. This opens an ethical debate. If a bomb was detonated at Coca-Cola headquarters, would there be the expectation to retaliate on some level? How much should corporations be willing to lose to these attacks? What is the government's responsibility to protect its corporations? What would be the result if an American corporation entered into a cyber-battle with a nation-state without government approval?

Trends of Computer Crimes

Criminals continue to develop new types of skullduggery every day. Reports of ransom ware are on the rise in America. In this crime, hackers, essentially pirates here, break into a computer system via spam e-mails and encrypt the files making them unusable to the user. The hacker then demands a ransom to un-encrypt the files. This scheme has affected both individuals and corporations—basically anyone who uses e-mail.

Many hacker groups are now structured like the more traditional Mafia. Hacker sites have appeared offering commercial services to hack into a boyfriend's e-mail account or an ex-girlfriend's Facebook account, to larger crimes, such as breaking into a former employer's systems to wreak havoc. They also continue to operate on the Internet underground, the Dark Net, such as the Tor network, Silk Road, and the Invisible Internet Project (I2P). Though, there are still those who argue that hackers are beneficial to cyber security because through their hacking exploitations they expose vulnerabilities.

Does your car have a computerized control system? The future of technology will see coffee makers that can tweet their owners to remind them to set their timers. Now, if a hacker got into a coffee maker there might not be a morning caffeine fix, however, if a car's computer is hacked, there could be a disastrous result and even death.

With regards to cyberterrorism, social media (Twitter and Facebook) are the main methods terrorist groups use to recruit and spread their messages. Non-government organizations (NGOs) actively campaign to shut down the hundreds of Twitter accounts operated by terrorist organizations around the globe. Although, this situation is much like a multi-headed hydra; one head is cut off only to have another grow in its place.

Staying on top of the hackers, cybercriminals, and cyberterrorists is a full-time job that we appear to be failing at. Technological education is the future. There will be a need for millions to be educated in cyber security to be successful in fighting the growing nature and scope of this challenge on every level. For example, continuing education of law enforcement at the local level will remain key to the successful prosecution of crimes facilitated through the use of computers, such as child pornography, cyber stalking, and human trafficking. It is not a question of if bad things are going to happen operating on the Internet—they will. The key is resilience and the response plan for how to bounce back after a digital attack or crime is perpetrated.

Real World Implications

Could some of this be overkill? Maybe, but those whose security has been breached might disagree.

People generally go about their day with an imaginary layer of security. For example, one may have a Target Red Card or a Home Depot card. These are big companies, right? Surely they have safeguards in place to protect my information. Yes, presumably they do, but apparently not good enough. To be sure, your information may be safer at Target than from some obscure website, but sometimes the larger the company, the larger, and easier the target. No pun intended.

Despite the latest safeguards, for some reason, the hackers and terrorists often get the upper hand on techno security. Why is this? Because while people go about their daily lives, using the Internet for things that might make their lives easier on the surface (e.g., online bill pay and automatic withdrawal), the criminals are spending every waking moment trying to obtain this information.

One of the mistakes people make is assuming that they are safe because they change their password every month, or they never give out their information over the phone. To be sure, these are safeguards, and one should be commended for taking these measures. However, simply having certain everyday items makes people vulnerable, and the vast majority of them maintain only minimum security measures. For example, how many of you lock your smart phone? Do you use the ATM at the gas pump? The average citizen is worrying about getting through their work day with their family, not on how they can stay on top of every potential threat.

Conclusion

In this unit lesson you have read about the various threats, classifications, trends, risks, and different terms associated with cybercrimes and terrorism. For example, is all computer crime the same? No. Is cyberterrorism multifaceted? Yes. How do law enforcement personnel identify and protect people from these emerging threats? What can we do as a society to protect and strengthen our cyber infrastructure?

Reference

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). *Digital crime and digital terrorism* (3rd ed.). Upper Saddle River, NJ: Pearson.