INVESTIGATING CYBER TERRORISM AJU 447 / AJU 6647

Mississippi College
A CHRISTIAN UNIVERSITY

WEEK THREE

CRITICAL INFRASTRUCTURE & CYBERCRIMES

CRITICAL INFRASTRUCTURE

Defined

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience (February 12, 2013) Advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors.

16 Critical Infrastructure Sectors

1. Chemical - The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely.

2. Commercial Facilities - The Commercial Facilities Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within the sector operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities.

3. Communications - The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government using interconnected; satellite, wireless, and wireline providers which depend on each other to carry and terminate their traffic.

4. Critical Manufacturing - The Critical Manufacturing Sector has identified several industries to serve as the core of the sector including; primary metals manufacturing; machinery manufacturing; engine and turbine manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing.

16 Critical Infrastructure Sectors (Continued)

5. Dams - The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

6. Defense Industrial Base - The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

7. Emergency Services - The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

8. Energy - The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

9. Financial Services - The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.

16 Critical Infrastructure Sectors (Continued)

10. Food and Agriculture - The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity.

11. Government Facilities - The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment.

12. Healthcare and Public Health - The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters.

13. Information Technology – This sector provides virtual and distributed functions which produce and provide hardware, software, and information technology systems and services.

16 Critical Infrastructure Sectors (Continued)

14. Nuclear Reactors, Materials, and Waste - The Nuclear Reactors, Materials, and Waste Sector covers most aspects of America's civilian nuclear infrastructure, from the power reactors that provide electricity to millions of Americans, to the medical isotopes used to treat cancer patients.

15. Transportation Systems - The Transportation Systems Sector consists of seven key subsectors, or modes: aviation; highway and motor carrier; maritime transportation system; mass transit and passenger rail; pipeline systems; freight rail; and postal and shipping.

16. Water and Wastewater Systems – This sector ensures that the supply of drinking water and wastewater treatment and service is maintained to sustain the Nation's economy.

CYBERCRIMES

CYBER INTRUSION (Hacking)
The unlawful or unauthorized access of a computer network or system for any reason (read, write, delete, alter, etc.). This act is commonly known as "hacking."

CYBER ESPIONAGE
Knowingly benefit a foreign government by stealing trade secrets with the use of high-technology. Cyber Espionage may be conducted by a corporation, individual(s), or state actors.

MALWARE
Software designed to gain access, damage, and/or alter a computer or system without the knowledge of the owner. Examples of this software includes computer viruses, worms, Trojan horses, ransomware, spyware, and adware.

IDENTITY THEFT
Accessing personal identifiable information without the person's consent.

CYBER FRAUD
Using a person's personal identifiable information for illicit financial game.

CYBER BULLYING
Aggressive behavior involving a real or perceived power imbalance that is repeated, or has the potential to be repeated, over time using high-technology, such as cell phones, computers, social media, texting, chat programs, blogs, and Web sites.

CYBER THREATS
Threatening communications that are conveyed via high-technology to harm a person or property, to kidnap a person, or to damage a person's reputation (18 U.S.C. § 875).

CYBER STALKING
The use of high-technology to commit a pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear for themselves or their immediate family.

SWATTING

Deceives emergency responders into dispatching a Special Weapons and Tactics (SWAT) team to the location of the victim. Swatting is extremely dangerous for the victim and law enforcement personnel.

CYBER EXTORTION

An attack or threat of attack against computer services or networks using DDoS or malware that
encrypts data on an organization's computer system or network (Ransomware).

SEXTORTION

A form of cyber extortion that occurs when individuals demand that the victims provide them with sexual images, sexual favors, or other things of value. These demands are accompanied by threats to harm or embarrass the victims if they fail to comply (e.g., intimate photos). Victims of sextortion are often minors but can also be adults.

REVENGE PORN

The distribution of nude/sexually explicit images/videos taken consensually during an intimate relationship. The images/videos are posted online, often with personal identifiable information, motivated by revenge.

Other Definitions

DOXING

Broadcasting personally identifiable information about an individual on the Internet. It can expose the victim to an anonymous harassers, phone calls, email, and appearing at the victim's home ("GamerGate").

PERSONAL IDENTIFIABLE INFORMATION (PII)

Information which can be used to distinguish or trace an individual's identity.

Assignments

1. Read Chapter 3 and Chapter 5 in “Cybercrime”
2. Answer Essay Question (Assignment #2). Due 1/29/18
3. Complete FEMA Independent Study 200.b Due 2/1/18
4. Study for online Quiz (1/25/18)