4.15 CYBER ATTACK

SECTION 4.15 CYBER ATTACK

4.15-1 HAZARD OVERVIEW

Cyber terrorism is the use of existing computers and information, particularly over the Internet, to cause physical or financial harm or a severe disruption of infrastructure service. Transportation, public safety, and utility services are all critical, and are highly dependent on information technology. The motive behind such disruptions can be driven by religious, political, or other objectives. Three kinds of attacks that can be conducted on computers include attacks of physical means, electronic means, and attacks using malicious code (Waldron, 2011). Specifically, these types of include:

- Directing conventional kinetic weapons against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.
- The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, an EA disrupts the reliability of equipment and the integrity of data.
- Malicious code can be used to create a cyber-attack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyber-attack can disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications (Wilson and Clay, 2007)

Cyberterrorists typically have two broad motivations to carry out an attack. These motivations are:

- Effects-based: Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism.
- Intent-based: Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage (Rollins and Clay, 2007).

Cyber terrorists can attack several types of computer systems in a variety of ways and are described in Table 4.15-1 below.

Table 4.15-1 Computer Systems that can be Attacked

Computer System	Description
All system and network devices BIND weaknesses	The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of Domain Name Service (DNS) by which systems on the Internet are located by name, without having to know specific Internet protocol (IP) addresses. In a typical example of a BIND attack, intruders erase system logs and install tools to gain administrative access. They then compile and install Internet Relay Chat (IRC) utilities and network scanning tools, which are used to scan more than a dozen class-B networks in search of additional systems running vulnerable versions of BIND. In a matter of minutes, they can use the compromised system to attack hundreds of remote systems.
Vulnerable Common Gateway Interface (CGI) programs and application extensions (such as ColdFusion) installed on Web servers (multiple UNIX and Linux systems)	Most Web servers support CGI for data collection and verification. Intruders are known to have exploited vulnerable CGI programs to vandalize Web pages and steal credit cards.
RPC weaknesses (all Web servers)	Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely used to access network services such as shared files in the Network File System (NFS). There is compelling evidence that the vast majority of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had RPC vulnerabilities. In 1998, the broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems.

Computer System	Description
RDS security hole in Microsoft IIS (multiple UNIX and Linux systems)	Programming flaws in Microsoft's Internet Information Server (IIS) used to host websites deployed on Microsoft Windows NT and Windows 2000 are employed by malicious users to run remote commands with administrator privileges. Experts who developed the "Top Ten" list of the most exploited internet security flaws believe that exploits of other IIS flaws, such as .HTR files, are at least as common as exploits of Remote Desktop Services (RDS).
Sadmind (Solaris machines only)	Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to hostile parties.
User IDs, especially root/administrator with no or weak passwords (UNIX, Windows, and Macintosh systems)	Some systems come with "demo" or "guest" accounts with no passwords or with widely- known default passwords. Service workers often leave maintenance accounts with no passwords, while some database management systems install administration accounts with default passwords. In addition, busy system administrators often select system passwords that are easily guessable ("love," "money," "wizard" are common) or use a blank password. Many attackers try default passwords and then try to guess passwords before resorting to more sophisticated methods.
IMAP and POP buffer overflow vulnerabilities or incorrect configuration (all systems)	Internet message access protocol (IMAP) and Post Office Protocol (POP) are popular remote access mail protocols, allowing users to access their e-mail accounts. The "open access" nature of these services makes them especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Attackers who exploit flaws in IMAP or POP often gain instant root- level control.
Default SNMP community strings set to "public" and "private" (multiple UNIX and Linux systems)	The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices, ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption creates one level of security vulnerability, but the default community string used by the vast majority of SNMP devices is "public," with a few clever network equipment vendors changing the string to "private," which presents a greater security risk. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely.

In addition to the motivations for cyber terrorism and the vulnerable systems, cyber-attacks can be further divided by the complexity of the attack. The categories of attacks include:

- Simple-Unstructured: Simple-unstructured attacks are the most common. These are amateurish attacks with relatively minimal consequences.
- Advanced-Structured: Advanced-structured attacks are more sophisticated and consequential and have a greater emphasis on targeting victims prior to an attack, resulting in a more debilitating effect.
- Complex-Coordinated: Complex-coordinated attacks are the most advanced and most troublesome type of attack where success could mean a network shutdown.

Regulations In Place To Manage The Hazard

The United States Department of Homeland Security (U.S. DHS) strengthens cybersecurity resilience across the country by investigating malicious cyber activity. An agency under U.S. DHS, the Cybersecurity and Infrastructure Security Agency (CISA), works to understand, manage, and reduce risk to cyber and physical infrastructure in the United States. CISA has two primary operational functions: (1) lead federal cybersecurity across the federal civilian executive branch and (2) coordinate critical infrastructure security and resilience by working with partners across government and industry to protect and defend the nation's critical infrastructure (U.S. DHS, 2023).

In New Jersey, a similar approach is taken. The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) was established in 2015 in order to address New Jersey's vulnerability to potential occurrences of a cyber-attack. NJCCIC focuses on information sharing, threat analysis and incident reporting with the intent of promoting awareness of the potential threat New Jersey faces to cyber-attack (NJCCIC, n.d.).

4.15-2 LOCATION, EXTENT, AND MAGNITUDE

Location

Cyber threats to critical infrastructures can be posed by anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, State-sponsored or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile. The fact that most of the nation's vital services are

delivered by private companies creates a significant challenge in assigning the responsibility for protecting our critical infrastructures from cyber-attacks. Across New Jersey, countless systems rely on computers for day-to-day operations including but not limited to traffic signals, power plants, HVAC systems, as well as systems responsible for ensuing New Jersey's State government can operate. While these are just a few examples of critical systems vulnerable to cyber-attacks, it should be noted that an attack could cripple not only the operations of New Jersey's systems but also the economy.

New Jersey remains a valuable target as it possesses a wealth of critical information infrastructure, much of which is inherently interdependent. New Jersey is strategically located along a heavy transit corridor for people and goods, and is a major node along the fiber path through the northeastern United States, connecting New Jersey to Philadelphia and Washington, D.C. Furthermore, New Jersey is one of the wealthiest states in the country and is home to many Fortune 500 companies. Any disruption to the State's economy could have a drastic impact on the national economy and thus the nation's economic stability (New Jersey Office of Homeland Security and Preparedness [NJ OHSP], 2008).

Extent and Magnitude

The magnitude of extent of an incident will vary greatly based on the extent and duration of the impact. Additionally, the extent will vary based upon which specific system is affected by an attack, the warning time, and ability to preempt an attack.

NJCCIC profiles different threats to various systems that can be impacted by an attack, providing some context of the extent an attack could have. Table 4.15-2 describes the malware that can impact different systems.

Table 4.15-2 Threat of Malware to Different Systems

Threat	Description of Malware
Android	Malicious software designed to exploit the Android operating systems (OS) running on smartphones, tablets, and other devices. Some variants of Android malware have the capability of disabling the device, allowing a malicious actor to remotely control the device, track the user's activity, lock the device, or encrypt or steal personal information transmitted from or stored on the device. As users are increasingly turning to mobile devices for both business and personal use, cyber threat actors are devoting their efforts to developing malware designed to compromise the device software.
Botnets	A group of internet-connected computers and devices that have been infected by malware that allows a malicious actor to control them remotely. The malicious actor then uses the botnet for nefarious purposes such as sending spam email, stealing data, spreading additional malware infections to other devices, generating illicit advertising revenue through click-fraud, mining cryptocurrencies, or conducting distributed denial-of-service (DDoS) attacks. In the cases where botnets are used to conduct DDoS attacks, these infected devices are used to generate an excessive amount of network traffic designed to overwhelm a website, server, or online service to the point that legitimate users cannot access it.
Exploit Kits	Toolkits that automate the exploitation of vulnerabilities in popular software applications to maximize successful infections and serve as a platform to deliver malicious payloads such as Trojans, spyware, ransomware, and other malicious software. Most users will encounter EKs from visiting seemingly legitimate, high-traffic websites that either contain links to EKs embedded within malicious advertising (malvertising) or have malicious code hidden directly within the website itself. Malicious URLs linking to EKs are commonly distributed through spam email and spear-phishing campaigns.
ICS	A collective term for several types of control systems and other equipment used to operate and/or automate industrial processes and includes supervisory control and data acquisition (SCADA) systems – often incorrectly used interchangeably with ICS – and distributed control systems (DCS).
IOS	Malicious software designed to exploit Apple's iOS operating system running on smartphones, tablets, and other devices. Some variants of iOS malware have the capability of disabling the device, allowing a malicious actor to remotely control the device, track the user's activity, lock the device, or encrypt or steal personal information transmitted from or stored on the device. As users are increasingly turning to mobile devices for both business and personal use, cyber threat actors are increasingly devoting their efforts to developing malware designed to compromise mobile devices, including operating systems, like iOS, and applications, like those available in the App Store. Android devices have historically seen more malware threats than iOS largely due to the open-source operating system; however, malware specifically targeting iOS has increased in the last two years.
MAC OS	Though the majority of known malware targeting operating systems are made to exploit Microsoft Windows, devices running macOS are vulnerable as well. Furthermore, as macOS has become increasingly popular, more malware has been created to target macOS. More macOS malware was discovered in the second quarter of 2017 than in all of 2016.
Point of Sale (PoS)	Malicious software designed to steal credit and debit card data from payment processing systems, known as point-of-sale (PoS) terminals.

Threat	Description of Malware
Ransomware	Malicious software (malware) that attempts to extort money from victims by restricting access to a computer system or files. The most prevalent form of this profit-motivated malware is crypto-ransomware, which encrypts files into encoded messages that can only be decrypted (decoded) with a key held by the malicious actor.
Trojans	A type of malware that, unlike viruses and worms, does not self-replicate. Named after the mythological wooden horse used to sneak Greek warriors through the gates of Troy, trojans are often disguised as legitimate software to avoid detection or trick users into installing the trojan onto their system. Users can be exposed to trojans through numerous vectors, such as clicking on links or opening attachments in phishing emails, other forms of social engineering, malicious advertising (malvertisting), or by visiting compromised websites, known as drive-by downloads. Once a trojan executes, it often downloads other malware onto the system or provides an attacker with a backdoor to gain access and conduct further malicious activity, such as stealing, deleting, or modifying data.

Source: NJCCIC, n.d.

4.15-3 PREVIOUS OCCURRENCES AND LOSSES

Cyber terrorism is an emerging hazard that can impact the county's computer infrastructure and the systems and services that are provided to the public. Across the United States, concerns over cyber terrorism are growing; former FBI director Louis Freeh warns that cyber-terrorism could have a crippling effect in the United States (ANI, 2013).

In 2016, New Jersey released the annual statistics on cyber breaches for the first time. The information released details breaches that involve the unauthorized access to personal information, such as a name, social security number, driver's license number, bank account, etc. The state police had 676 data breaches reported to them in 2016, affecting over 116,000 New Jersey account holders (Department of Law and Public Safety, Office of the Attorney General, 2016). In 2017, 958 data breaches were reported to the New Jersey State Police. This is a 41% increase in security breaches from 2016 (Department of Law and Public Safety, Office of the Attorney General, 2018).

FEMA Related Disasters

There have been no FEMA disaster declarations related to a cyber-attack to date.

4.15-4 PROBABILITY OF FUTURE OCCURRENCES

Security experts describe the threat of cyber terrorism as eminent and highly likely to occur in any given year in New Jersey. As illustrated by the Freeh comments, cyber terrorism is expected to have a significant impact on the United States and New Jersey. The level of success of an attack and the subsequent damage it can create will vary greatly. Intrusion detection systems log thousands of attempts in a single month.

Potential Effects of Climate Change

Due to the manmade nature of cyber-attack, this hazard is not related to climate change.

4.15-5 VULNERABILITY ASSESSMENT

The following sections discuss New Jersey's vulnerability, in a qualitative nature, to the cyber-attack hazard. A consequence analysis for this hazard was also conducted and presented in Section 10.0: EMAP. Impacts on the public, responders, continuity of operations, and delivery of services; property, facilities, and infrastructure; the environment, economic condition of the state, and the public confidence in the State's governance is discussed in Section 10.0: EMAP in accordance with EMAP standards. This section addresses assessing vulnerability and estimating potential losses by jurisdiction and to state facilities.

Built Environment

The capitol of New Jersey, the City of Trenton, is particularly vulnerable due to the concentration of State buildings there. The sensitive data housed on the computer networks in State buildings are highly vulnerable to this hazard.

All State-owned and leased buildings in New Jersey are exposed to cyber-terrorism attacks. State-owned and leased buildings are particularly vulnerable to cyber-terrorist attacks because of their importance in the daily operation of New Jersey. While

the physical structures of these buildings are not vulnerable, the information systems within them are. The vast computer networks present in State-owned and leased buildings contain sensitive data that are integral to the security of New Jersey. State-owned facilities are vulnerable to cyber-attacks given the importance of these buildings to the State.

Critical facilities are also vulnerable to cyber-terrorism attacks based on the significance of the facilities, and the potential to interrupt critical systems in the State. As previously mentioned, many critical facilities are reliant upon computer networks to monitor and control critical functions. An example is nuclear power plants, which rely on sophisticated networks to prevent catastrophic failure. A cyber-terrorist attack could result in catastrophic failure of one of these facilities. Likewise, the power grid is reliant upon computer systems to distribute power to the State. An attack could disrupt power to millions of New Jersey residents. These are just two examples of how critical facilities are vulnerable to cyber-terrorism attacks. Given the importance of critical facilities to daily living activities, these facilities are highly vulnerable to cyber-terrorism attacks.

It is difficult to quantify the potential losses to state facilities caused by a cyber-attack. As noted in the vulnerability assessment above, the physical facilities would not be damaged, other than the value of computer equipment damaged. The more significant loss would be to the functions of the facilities targeted and their value to the population of New Jersey during the period of malfunction.

Population and Economy

For the purposes of this Plan, the entire population of New Jersey is considered exposed to the effects of a cyber-terrorism attack. Because it is difficult to predict the particular target of cyber terrorism, assessing vulnerability to the hazard is also difficult. All populations who directly use a computer or those receiving services from automated systems are vulnerable to cyber terrorism. Although all individuals in New Jersey are vulnerable to an attack, certain types of attacks would impact specific segments of the population.

If the cyber-attack targeted the State's power or utility grid, individuals with medical needs would be impacted the greatest. These populations are most vulnerable because many of the life-saving systems they rely on require power. Also, if an attack occurred during months of extreme hot or cold weather, New Jersey's senior population (those 65 years of age and older) would be vulnerable to the effects of the lack of climate control. These individuals would require shelter or admission to a hospital. Other populations vulnerable to the secondary effects of cyber terrorism are young children.

If a cyber-attack targeted a facility storing or manufacturing hazardous materials, individuals living adjacent to these facilities would be vulnerable to the secondary effects, should the attack successfully cause a critical failure at that facility. Individuals living within 10 miles of a nuclear power plant would be vulnerable should an attack occur at that caused a failure at a facility. While these examples illustrate the vulnerability of specific populations to cyber-attacks, it is important to reiterate that because of the reliance on computerized systems, the entire population of New Jersey is vulnerable to cyber terrorism.

A significant portion of New Jersey's economy is exposed to the effects of cyber-terrorist attacks. Cyber-crimes against banks and other financial institutions can cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information can cost developed economies billions of dollars—how many billions is an open question. These losses could be considered simply the cost of doing business, or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage (McAfee, 2013).

The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. Cyber-crimes can cause damage to a company's brand and reputation, consumer losses from fraud, the opportunity costs of service disruption and "cleaning up" after cyber incidents, and the cost of increased spending on cybersecurity (McAfee, 2013).

In the United States, the costs of cyber terrorism is estimated somewhere between $24 billion and $120 billion annually. These costs represent approximately 0.2% to 0.8% of the total GDP in the United States (McAfee, 2013).

Given the proliferation of electronic commerce and the reliance on electronics, virtually all elements of New Jersey's economy are vulnerable to cyber-attacks. The secondary impacts of a significant attack would be devastating to the economy. For example, an attack that caused the loss of power to hundreds of thousands of businesses during peak holiday shopping months could potentially cost the State millions of dollars in tax revenue if these businesses were closed. Additionally, a disruption in New Jersey's manufacturing, agricultural, or tourism sectors would have devastating impacts on the economy. While it is difficult to quantitatively measure the economic impact of a cyber-terrorism attack, it is safe to say that the impact would be great, thus the economy is vulnerable to cyber-terrorism attacks.

Ecosystems and Natural Assets

Cyber-attack events do not generally impact the natural environment, unless facilities such as nuclear, electrical power, waste treatment, chemical, or petroleum plants are targeted, and a release occurs. These impacts are further discussed in Section 4.23 Terrorism.

Impact Analysis

Severity and Warning Time

A cyber attack can have potentially severe consequences as detailed in Table 4.15-3 below.

Table 4.15-3 Cyber Attack Impact Summary

Consideration	Description
General Public	No direct loss of life is expected from an attack. Indirect injuries or deaths may result from secondary effects to critical life-sustaining resources such as energy and water.
Response Personnel	No direct affects to the health and safety of response personnel are expected; however, critical response systems may be affected.
Property, Facilities and Infrastructure	Effects can range from annoyance to complete shutdown of critical infrastructures caused by infiltration of supervisory control and data acquisition (SCADA) systems. Secondary effects could disturb public welfare and property by denying services or providing false readings.
Economic	Because of the heavy reliance on the electronic transfer of economic and commercial information, the economy could be affected by communication difficulties.
Environment	Generally, cyber terrorism has no direct effect on the environment; however, the environment may be affected should a release of a hazardous material occur because of critical infrastructure failure.
Continuity of Operations	Severe effects to continuity of operations could result if a cyber-attack reached critical operational systems or systems that were needed to carry out the operation.
Reputation of the Entity	If exposed vulnerabilities were known and not reduced or eliminated before the attack, the entity would suffer major damage to their reputation for not taking action before the incident.
Delivery of Services	Cyber-attacks may affect delivery of services if the system was infiltrated and directed to malfunction by self-destructing or overloading.
Regulatory and Contractual Operations	Cyber-attacks would have no significant effect on regulatory or contractual obligations, other than the possible elimination of electronic records, which would affect both.

A cyber terrorism attack can occur with relatively little or no warning. The New Jersey Office of Homeland and Preparedness is charged with gathering intelligence and monitoring cyber-terrorism threats affecting the State. At the federal level, numerous agencies (such as FBI and CIA) are working collaboratively to thwart cyber-terrorism attacks. The warning time depends upon the ability of these agencies to recognize that a threat exists and their ability to stop the attack. Even with these agencies on task to monitor cyber threats, a cyberattack can occur with no warning.

Secondary Hazards

Because virtually all critical systems are reliant upon computer systems, the secondary hazards that could result from a cyber-terrorism attack could be devastating. For example, many of New Jersey's roadway systems rely on sophisticated traffic control systems that prevent gridlock and accidents daily. Without these systems, the risk of not only auto accidents increases, but also hazardous materials in-transit incidents. Additionally, a cyber-attack on a nuclear power plant could have devastating

consequences should the plant suffer an intentional catastrophic failure. A cyber-attack could also completely incapacitate the communications infrastructure not only in New Jersey but across the United States, leading to disturbing secondary consequences and hazards. Because the power grid is also largely controlled by computer systems, a widespread power outage is also a possibility. A failure of the power grid would impact individuals reliant on power such as those with medical needs. The number of critical systems reliant on computer systems are numerous, thus disruption of one or more of the systems would cause severe secondary-cascading hazards.