CYBER SECURITY THREATS ON CRITICAL INFRASTRUCTURES

By: Katie Barnes

BOSTON UNIVERSITY

MET CJ 620 02

November 26, 2021

Cyber Security threats on Critical Infrastructures

Introduction:

As Technology advances society has become increasingly dependent upon information technology. While technology delivers many benefits, it also introduces new vulnerabilities that can be exploited by anyone with the necessary technical skills. Cyberterrorism can be seen as an "act of disrupting critical infrastructure such as energy, transportation, and public facilities by using tools for the purpose of threatening the government or it's people" (Choi, Module 1). In wake of 9/11, the USA PATRIOT Act 2001 defines critical infrastructure as "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 of security, national economic security, national health or safety, or any combination of those matters (Choi, Module 1). This paper discusses the topic of infrastructure attacks, the history of infrastructure attacks, and prevention of such attacks. I chose this topic to discuss the history of critical infrastructures attacks, their capacity and destruction and how it impacts economic security, public trust, public health, and safety. On July 2021 the FBI and the U.S Cybersecurity and Infrastructure Security Agency (CSIS) released a statement exposing a spearfishing campaign by Chinese state-sponsored hackers between 2011 and 2013. The campaign targeted oil and natural gas pipeline companies in the United States (CSIS, 2021). Disruption to a cyber infrastructure can lead to serious consequences that affect the performance, reliability, security, and safety of the dependent infrastructures (Alcaraz & Zeadally, 2015 pg.54).

According to the European Commission, critical information infrastructure protection comprises programs and activities of infrastructure owners, manufacturers, users, operators,

research and development institutions, governments and regulatory authorities that aim to maintain the performance of critical information infrastructures in the event of failures, attacks, or accidents above a defined minimum level of service and to minimize damage and recovery time (Alcaraz & Zeadally, 2015 pg. 54). The threats of a cyber attack on critical infrastructures are to be taken extremely serious because of the connections of other critical infrastructure sectors that rely on one another. For instance, most of all critical infrastructures depend on products and services that are interconnected. These interdependencies could trigger cascading effects in multiple critical infrastructures when one critical infrastructure is disrupted, damaged, or destroyed (Alcaraz & Zeadally, 2015 pg.54). This includes the threat of public safety for an example, healthcare systems could be compromised, water supply could be disrupted or tampered with as well as homeland security. The dangers of critical infrastructure threats can be catastrophic if the cyber-attack was intentional to cause physical harm or could cause a major economic impact to a nation. “Technological progressions continually enable the increased use of computers and networks with high performance capabilities to preside over a plethora of human-managed industrial infrastructures activities like control, and automations in finance, aerospace, transport, health, and manufacturing (Uchenna et al., 2017)”. This means that with the push of a button by hacking a system of a major company or critical infrastructure a cyber hacker could potentially endanger the lives of many citizens, cause damage to facilities, steal data, steal company revenue or damage the reputation of a company. Although it is most likely not the company or institutions intent to allow a breach of security it can still happen even with top-of-the-line securities, Anti-virus programming or Firewalls. “Vulnerabilities delineate the points of weakness even in flawless institutions or networks (Uchenna, Hongmei & Tiwari, 2016).

Threat agents could include attackers, bot-network operators, criminal groups, foreign intelligence services, insiders, phishers, spammers, spyware/malware authors, terrorists, and industrial spies (Uchenna et al., 2017). “Notable attack techniques include phishing, social engineering, compromise of domain controllers, attack on exposed servers, attack on ICS clients, session hijacking, piggybacking on system’s virtual private network (VPN), exploiting firewall vulnerabilities, misconfiguration of firewalls, forged internet protocol addresses, bypassing the network security, physical access to the firewall, and sneaker net techniques. Degrees of damage can range from inconvenient downtime for ICS/IO and control equipment, and (or) enterprise systems to life-threatening destruction of critical infrastructures, three broad impacts of cyber-attacks on ICS infrastructure are identified, such as physical, economic, and social impacts (Uchenna et al., 2017)”.

Case Review:

With the broad adoption of digital technologies many businesses and government agencies have moved all control online. While attacks today have become more sophisticated and targeted to specific victims depending on the attacker’s motivation, for example for financial gain, espionage, coercion, or revenge; opportunistic untargeted attacks are also very prevalent (Lallie et al. 2021). On Tuesday July 20, 2021, The Biden Administration disclosed previously classified details about the breadth of state-sponsored cyberattacks on American oil and gas pipelines on from 2011 to 2013, Chinese-backed hackers targeted, and in many cases breached, nearly two dozen companies that own such pipelines, the F.B.I. and the Department of Homeland Security revealed in an alert (Perlroth & Sanger, 2021). “The intrusions were likely for future

operations and intellectual property theft. In other words, the hackers were preparing to take control of pipelines, rather than just stealing the technology that allowed them to function (Perlroth & Sanger, 2021)". The hackers attacked 23 operators of natural gas pipelines that were subjected to email fraud that is known as spear phishing, the agencies said that 13 were successfully compromised (Perlroth & Sanger, 2021). Few of the agencies were close to being compromised and several were unknown due to the absence of data. "Newly classified reports are a reminder that nation-backed hackers targeted oil and gas pipelines before cybercriminals devised new ways of holding operators ransom. Ransomware is a form of malware that encrypts data until the victim pays ((Perlroth & Sanger, 2021)". F.B.I seized back half of $4 million dollars in cryptocurrency, after criminals left part of the money visible in cryptocurrency wallets (Perlroth & Sanger, 2021). Moreover, according to the security firm FireEye, it is "strongly" believed that in one case, Chinese hackers had gained access to the controls, which could have enabled a pipeline shutdown or could potentially set off an explosion.

In direct response to ongoing cybersecurity threats from Russia and China on United States Colonial Pipelines systems, The Department of Homeland Security (DHS) and DHS'S Transportation Security Administration (TSA) announced the issuance of a second Security Directive that requires owners and operators of TSA designated critical pipelines that transport hazardous liquids and natural gas to implement several urgently needed protections against cyber intrusions (DHS, 2021 July 20). Homeland Security continues to monitor and work with public and private sectors to protect the safety of the American people from evolving threats to better ensure the pipeline sector takes necessary safeguards in their operations from rising cyber threats and better protect the national and economic security (DHS, 2021 July 20). The issue is that criminals have a long history of conducting cyber espionage on China's behalf. Many cyber

criminals have been protected from prosecution by their affiliation with China's Ministry of State Security (MSS), criminals turned government hackers conduct many of China's espionage operations (Cary, 2021). It is not surprising or shocking new phenomenon considering that Chinese hacking go as far back as 2006. For example, the U. S. Department of Justice issued an indictment that indicted that the simultaneous criminal espionage activity of two Chinese hackers (Cary, 2021). The cybersecurity company FireEye alleges that APT41, a separate cohort of MSS Hackers, began as criminal outfit in 2012 and transitioned to concurrently conducting state espionage from 2014 onward (Cary, 2021).

In theory, the United States Government thinks China may have been laying down groundwork for the future. Starting in 2015, Universities in China tried to standardize university cybersecurity degrees by taking inspiration from the United States' National Institute for Cybersecurity Education (Cary, 2021). Today, the National Cybersecurity Talent and Innovation Base is in Wuhan China and is capable of training and certifying 70,000 people a year in cybersecurity (Cary, 2021). According to Dakota Cary (2021) contributor to the TechCrunch article, she states that a more capable China will behave differently than the China we see today as they weed out cybercriminals with new hire hackers with even more expertise. Given China's resilience on illicit hackers to hide its criminal and espionage activities, the Ministry of Public Security has tolerated some cyber criminals' Chinese operations, despite the problems they cause (Cary, 2021). As China's security-backed hacking steadily sheds its veneer of criminality, we can expect to a see a slowdown over the next decade in cybercrime conducted by contract hackers and others connected to the state (Cary, 2021). As of May 2014, the United States Department of Justice put out a press release stating that the U.S. charged five Chinese Military hackers for Cyber Espionage against the U.S. Corporations and a Labor organization for

Commercial advantage. These events occurred between 2006-2014. The defendants: Wang Dong, Sun Kaliang, Wen Xinyu, Huang Zhenyu, and Gu Chuhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA) (DOJ,2014). The indictment alleges that Wang Sun, and Wen, among others known and unknown to the grand jury, hacked or attempted to hack into the U.S. entities named in the indictment, while Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g., domain accounts) used for hacking (DOJ, 2014).

According to the United States Department of Justice, "the indictment alleges that the defendants conspired to hack into American's entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprise (SOEs). In some cases, it alleges the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity (DOJ,2014)". According to the indictment, the military crew had trade secrets with a design with specifications, owned by the Westinghouse, which were related to the pipes, pipe supports, and pipe routing in a product namely the AP1000 nuclear power plant, that was produced for and placed in interstate and foreign commerce (Western District of Pennsylvania, 2014).

Prevention Strategies:

The second Security Directive requires that owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review (DHS, 2021 November 10). As of November 10, 2021, The Department Homeland Security (DHS, 2021 November 10) reports that the department is not aware of any imminent or credible threat to a specific location in the United States. They continue to state in a press release that through the remainder of 2021 and into 2022, domestic violent extremists (DVEs), including racially or ethnically motivated violent extremists and anti-government/anti-authority violent extremists, will continue to pose a significant threat to our homeland (DHS,2021 November 10).

For the government to help secure our networks they must continue to offer new technologies and cyber security trainings to both public and private sectors. It is essential for both sectors to share intelligence to protect a Nation. While Wuhan China stays up to par with their cybersecurity education it is imperative for the United States to do the same by offering top tier education and training. Institutions can offer certificates, degrees and on the job trainings, including additional courses for those already experienced in cybersecurity. It’s time for more citizens to get involved in their country and become educated about the dangerous of exploited data that can potentially harm public health or safety. Promoting a sharing information about education in cyber security is a start and spreading awareness of the threats to our personal data is important as well. Better prevention strategies in the United States government agencies need to be put in place as far as safeguarding the critical infrastructures of America. Facilities need

more security put in place both human security, Firewalls, Anti-virus programs, a network authentication protocol such as Kerberos that offers mutual authentication, where both the user and server can affirm one another's identity (Choi, Module 4). Security agents should have top of the line job trainings to stay on top of the latest trends. Knowing all the latest techniques as far password cracking, brute force attacks, password sniffing, privilege escalation, system encryption, steganography, and rootkits are important to learn about. As many hackers use programs to hack systems so it is essential to learn how to use these programs and what to expect to defend a company against it if these programs or techniques are used. Since cyber intervention can weaken public confidence in the government's ability to maintain basic services, public order, and financial stability (Choi, Module 4).

Types of cyber interventions may include

- Executing DDoS attacks on critical infrastructure systems.
- Using malware to infect critical infrastructure departments to disrupt systems, steal, delete, and modify data and/or interrupt services; and
- Spreading false information, fake news, and propaganda to undermine the authority of the country and cause an expected response by the government and the target population (Choi. Module 4).

Organizations should help to reduce risk levels by, performing due diligence, provide forensic data, and generate reports that can be used as technical indicators (Choi, Module 1). When a business or organization recognizes crucial vulnerabilities and executes mitigation actions before they are exploited it is central to risk management (Choi, Module 1). Moreover, it is crucial for businesses and organizations to run comprehensive vulnerability assessments and periodically updating passwords to have a much safer and secure computing environment (Choi, Module 1).

References

Alcaraz, C. Zeadally S. (2015) Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection, 8:8, 53-66

Cary, D. (2021) China's Next generation of Hackers Won't be Criminals. That's a Problem. *TechCrunch Global Affairs Project*. Retrieved from https://techcrunch.com/2021/11/12/chinas-next-generation-of-hackers-wont-be-criminals-thats-a-problem/

Choi, K. (2021). Module 1: *Overview of Cyberterrorism & Cybersecurity Vulnerability*. Boston University

Choi, K. (2021). Module 4: *Chinese Espionage Cases & System Hacking*. Boston University

CSIS (2021). *Center for Strategic and International Studies* (CSIS) [Lecture notes]: Boston University

Lallie, S. H, Shepard, A. L, Nurse, R.C. J, Erola, A, Epiphaniou, G, Maple, C, Bellekens, X. (2021) Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic. Computers &n Security Vol.5, 2021 June. Retrieved from https://www-sciencedirect-com.ezproxy.bu.edu/science/article/pii/S0167404821000729

Perlroth, N., Sanger, D. (2021). China Breaches Dozens of Pipeline Companies in Past Decade, U.S. Says, *The New York Times*, Retrieved on November 27, 2021, From: https://www.nytimes.com/2021/07/20/us/politics/china-hacking-pipelines.html

The United States Department of Justice. (2014). *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.* [Press release]. Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui (2014). United States District Court Western District of Pennsylvania. Retrieved from https://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf

Uchenna P. Daniel Ani, Hongmei (Mary) He & Ashutosh Tiwari (2017) Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, Journal of Cyber Security Technology, 1:1, 32-74, DOI: 10.1080/23742917.2016.1252211