Cybersecurity Considerations Impacting the US Critical Infrastructure: An Overview

ACTRI Perspective

February 2022

Sith Slaughter

Introduction

Cybersecurity is one of the essential assets of everyday life. All the data that is within reach of *Internet of Things (IoT)* based devices is prized; the passwords that are stored on smartphones, the constant e-mails sent out with sensitive data, and connected appliances play an ever-growing role that affect people's lives. Therefore, it is imperative to act against cyberattacks that are aimed at critical infrastructure to ensure that data remains safe and that it is not exposed. Cyberattacks by state and nonstate groups and entities underscore the need to pay attention to the threat such groups may present long-term, including inherent differences in targeting motivations, strategies and tactics adopted and implemented by such groups. 1 This brief perspective offers a review and insight into dominant and pressing cyber-related threats aimed at critical infrastructure in the United States.

Cyber-Attacks Against Critical Infrastructure

Hackers have become more adept at digital assaults, yet many of the basic infrastructure frameworks still rely on legacy systems that are powerless against straightforward digital assaults. *Stuxnet*, *Havex*, *BlackEnergy 3*, and *Industroyer* are some examples of the most prominent attacks against critical infrastructure. 2 The malware that attacks these infrastructures have been intentionally and professionally designed as well.

Various IoT-based devices are implemented within critical infrastructure for practical communication. These IoT-based devices that are connected to the internet are expected to be at 75 billion by 2025 and the situation will likely worsen due to more attacks targeting critical infrastructure. 3 The best IoT-based solutions have drastically improved critical infrastructures. A device which has an IP address can connect to the internet and be exposed to virtually all IP-based cyber-attacks. Examples of IoT-based cyber-attacks around the world and the dangers they pose towards critical infrastructures are also further examined below.

- The Russian Foreign Intelligence Service (SVR) targeted a minimum of five government agencies, which included the U.S. State Department, Department of Homeland Security (DHS), Departments of Treasury and Department of Commerce. 4

- *SolarWinds:* Russian hackers accessed email accounts belonging to the head of the Department of Homeland Security. 5

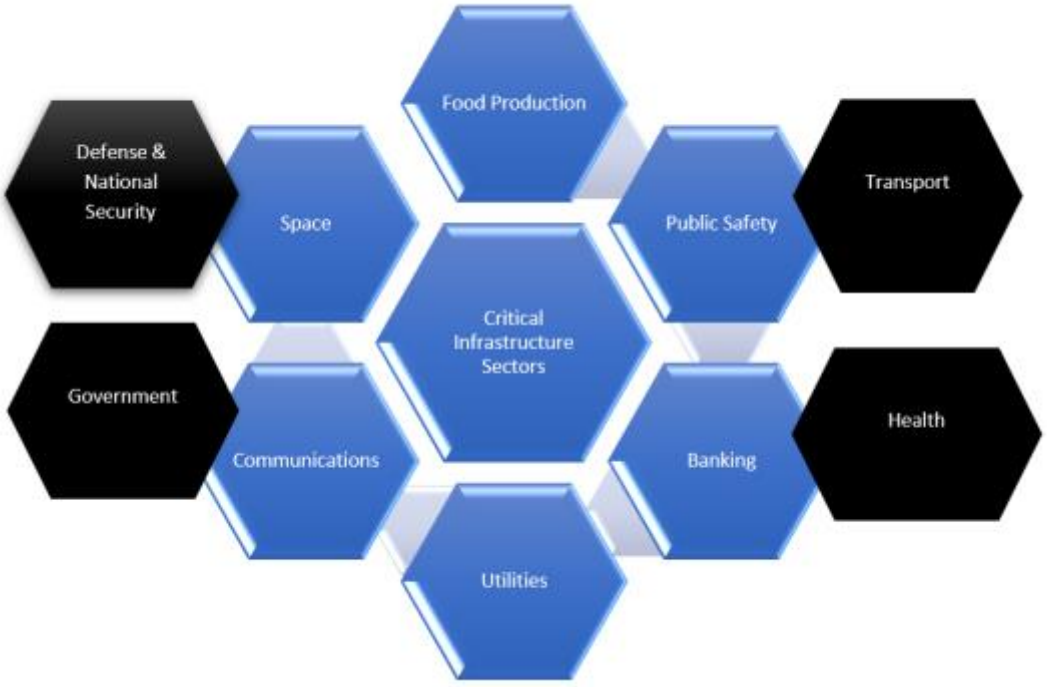
Within this context, the showcases of attacks demonstrate the weaknesses that are found throughout all critical infrastructure systems.

- *Hafnium:* Dubbed as "potential espionage mission," 6 the hack took place in February of 2021 and targeted Microsoft's Exchange email service. Vulnerabilities in Microsoft software enabled the hackers to gain access to the servers for email and calendar service, affecting thousands of people globally. It is believed the attack was carried out by Hafnium, a China-sponsored group. 7

- *Unnamed American Water Authority*: Hackers took control of a US water authority's cellular network. Cellular routers were used to increase data bills by "15,000%, from $300 monthly to well over $50,000 over a two-month period." 8 This stands in stark contrast to past hacking attempts focused on interrupting the water supply or seeking to poison the water.

Other relevant attacks include but are not limited to *Iranian Cyber Attack on New York Dam (Iran-sponsored), Moderna* (China-sponsored), *Unnamed US Natural Gas Operator,* and *San Francisco's Municipal Transportation Agency (MUNI) Light-Rail System.* 9, 10, 11 Although IoT-based applications empower more productive performance and correspondence through critical infrastructures, this can also lead to numerous security vulnerabilities, thus increasing the likelihood of cyber-attacks. To comprehend the seriousness of the circumstance, it is crucial to assess the impact and outcomes of the referenced cases. Within this context, the showcases of attacks demonstrate the weaknesses that are found throughout all critical infrastructure systems.

Fig. 1. Major Critical Infrastructure Sectors



Source: Department of Homeland Security (DHS) & Cybersecurity and Infrastructure Security Agency (CISA)

Common Types of Cyber-Attacks: Countermeasures

Cyber-kinetic attacks aim at IoT-based applications and Industrial Control Systems (ICS). These types of attacks compromise human life, one's physical well-being or the ecosystem. The type of attacks that are used range from being simple to being extremely difficult and complex. The most-well known techniques utilized in these cyber-attacks include *malware, phishing, Denial-of-Service (DOS) Attack, password attack, access control and hacking.* For instance, between 2014 and 2020, the United States charged a number of Iranian nationals for their malware, phishing, and DDos attacks. 12 Similarly, in light of recent development in Ukraine, the DHS has warned against Russia potentially engaging in cyberattacks against the United States, ranging from "low level denial of service attack to 'destructive' attacks targeting critical infrastructure." 13

Cyber-attacks are recurring frequently and it is becoming increasingly difficult to seize and mitigate them. With that said, there are numerous methods to counter cyber-attacks and successfully eliminate them. The simple safeguard procedures have a major significance in terms of decreasing the impacts of existing and future attacks. Some of the most renowned strategies to lessen cyberattacks in IoT-based critical infrastructures include *encryption*, *backdoors and login process*, and *internet Protocol fast hopping*." 14

A number of prominent cyber-attacks took place during President Trump and current President Biden's administration. 15 President Biden's newly issued Executive Order 14028 is expected to strengthen the nation's cybersecurity effort as it proactively targets the rampant malicious cyber campaigns and pursues government-private sector partnerships. 16 As noted by the White House, "Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." 17 The current cybersecurity trend is likely to influence and strengthen private-public relationship to counter cybersecurity threats doth domestically and internationally. 18

About the Author

Sith is a Research Intern at the American Counterterrorism Targeting and Resilience Institute (ACTRI), researching cybersecurity and cyberterrorism related topics. He is pursuing a Bachelor of Arts in Intelligence and Security Studies, with a concentration in Counterterrorism and a minor in Cybersecurity at The Citadel, The Military College of South Carolina. Sith is a member of Young Professionals in Foreign Policy (YPFP), a nonprofit organization that focuses on building the next generation of diverse foreign policy leaders. He has actively participated in YPFP's peer-led discussion groups and capacity-building programs.

Endnotes

1. Pomerlau, M. "State vs. non-state hackers: Different tactics, equal threat." Defense Systems. Retrieved December 2021, from https://defensesystems.com/cyber/2015/08/state-vs-non-state-hackers-different-tactics-equal-threat/190572/*; Carafano, J. J. " Fighting on the cyber battlefield: Weak states and nonstate actors pose threats. The Heritage Foundation. Retrieved December 2021, from* https://www.heritage.org/defense/commentary/fighting-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats*; L. Horwitz, "Internet of Things-The future of IoT miniguide: The burgeoning IoT market continues," July 2019. Cisco.*

2. G. Tuna, R. Das, and V. C. Gungor, "Communications Technologies for Smart Grid Applications: A Review of Advances and Challenges," in Smart Grid Analytics for Sustainability and Urbanization, pp. 215–235, 2018.

3. Brown, P. "75.4 billion devices connected to the internet of things by 2025." Electronics360. Retrieved January 2022, from https://electronics360.globalspec.com/article/6551/75-4-billion-devices-connected-to-the-internet-of-things-by-2025

4. McKay, H. " Russia's suspected hacking operation targeted 5 US agencies, 18K entities." Fox News. Retrieved December 2021, from https://www.foxnews.com/tech/foreign-hacking-public-private-entities-breached

5. L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," Manufacturing Letters, vol. 2, pp. 74–77, Apr. 2014.

6. Hern, A. "What is the Hafnium Microsoft hack and why has the UK linked it to China." The Guardian. Retrieved February 2022, from https://www.theguardian.com/world/2021/jul/19/what-is-the-hafnium-microsoft-hack-and-why-has-the-uk-linked-it-to-china

7. Toh, M. " Microsoft says a group of cyberattackers tied to China hits its Exchange email server." CNN. Retrieved February 2022, from https://www.cnn.com/2021/03/03/tech/microsoft-exchange-server-hafnium-china-intl-hnk/index.html

8. Weinberg, A. (2021, July 28). Analysis of top 11 cyber attacks on critical infrastructure. FirstPoint. Retrieved December 3, 2021, from https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/.

9. Cimpanu, C. " DHS says ransomware hit US gas pipeline operator." ZDNet. Retrieved January 2022, from https://www.zdnet.com/article/dhs-says-ransomware-hit-us-gas-pipeline-operator/

10. Ibid.

11. Kerner, M. S. " Cyber-attack knocks out San Francisco transit system fare terminals." eWeek. Retrieved December 2021, from https://www.eweek.com/security/cyber-attack-knocks-out-san-francisco-transit-system-fare-terminals/

12. Ranger, S. " Disk-wiping malware, phishing and espionage: How Iran's cyber attack capabilities stack up. " ZDNet. Retrieved December 2021, from https://www.zdnet.com/article/hard-disk-wiping-malware-phishing-and-espionage-how-irans-cyber-capabilities-stack-up/

13. Barr, L., & Margolin, J. " DHS warns of Russia cyberattack on US if it responds to Ukraine invasion. "ABCNews. Retrieved February 2022, from https://abcnews.go.com/Politics/dhs-warns-russian-cyberattack-us-responds-ukraine-invasion/story?id=82441727

14. Data Encryption Pros and Cons. Spam. (n.d.). Retrieved December 3, 2021, from https://www.spamlaws.com/pros_cons_data_encryption.html*; Krylov, V., & Kravtsov, K. " DDoS attack and interception resistance IP fast hopping based protocol." Ads, Harvard University. Retrieved December 2021, from* https://ui.adsabs.harvard.edu/abs/2014arXiv1403.7371K/abstract

15. Marks, J. " The cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say." The Washington Post. Retrieved January 2022, from https://www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/*;*

16. Biden-Harris Administration prioritizing cybersecurity. JD Supra. (n.d.). Retrieved December 3, 2021, from https://www.jdsupra.com/legalnews/biden-harris-administration-2101896/.

17. The United States Government. (2021, May 12). Executive order on improving the nation's cybersecurity. The White House. Retrieved December 3, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*.*

18. "State actors - United States Department of Homeland Security. (n.d.). Retrieved December 20, 2021, from https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf