Tim Klein

04/03/2024

CYSE 425W

Professor Gladden

National Cybersecurity Strategy - Protecting Critical Infrastructure

There is a constant and rapid pace at which modern cybersecurity threats evolve and find new methods to exploit. Cybersecurity threats to the global community are never static and also can not be fully quantified. There was a day long past that hacking tools were not readily accessible to potential bad actors. This is not the case today, sophisticated hacking tools are readily available to basically anyone who goes searching for them. This makes the bar of entry for a potential hacker as simple as a computer and an internet connection, easily accessible today in much of the world as well. This combined with continued developing exploits and hacking tools means that there is never a steady ground.

The previous two decades have been essentially a child's first steps as the digital space grew from a niche community to an everyday platform used in endless aspects of modern life. Now the United States deems it necessary to take the knowledge gained and develop a modern cybersecurity apparatus. The objective of the current Administration is for Americans to have a robust confidence in the defenses and policies in place to protect not just infrastructure but the entire digital economy, as the two are

hand in hand. Confidence in the digital spaces of commerce and trade allows for the economy to function and grow. Not only does this relate to the general commercial function of the country but also ties into the value of the Dollar. The more safe and stable a digital market the United States creates, a more stable dollar. This is due to various economic entities using the dollar because of its proven stability. So being, the United States is critically invested to protect critical infrastructure, even just from the economic perspective.

To protect its infrastructure the United States is modernizing its approach from being relatively reactionary in the past to preemptive about not just current threats but mitigating future ones as well. The United States seeks to allow for various law enforcement agencies to work together to combat cyber crime. Previously this interagency cooperation was much more difficult and covered in red tape. When being faced with countless attacks and threats in the digital space, the United States seeks to lead the way in cybersecurity defense and culture.

Developing frameworks based on knowledge that has been tried and true.It is the base of the pillar of cooperative effort. This is where the concept is built and cooperative efforts move out from a shared system. Having a robust cyber defense apparatus also includes an informed culture surrounding cybersecurity practices. Meaning that our professionals who work with these infrastructure systems are knowledgeable about the potential cyber vulnerabilities and how to mitigate them. The human factor is one of the largest, if not the most significant vulnerability many systems

have. As the expertise to manipulate a person is far less involved and technical. A policy framework establishes a general, cultural defense against the human factor vulnerabilities.

American infrastructure in particular finds itself vulnerable to cyber attacks. A devastating attack could potentially disable major utility systems and cost many lives as a result. A vast amount of infrastructure is dependent on computerized systems which creates a possible vulnerability. It is the doubled nature of computerized systems, they can be exploited digitally and much of the time from nowhere near the physical infrastructure itself. The current Administration has made significant headways in major infrastructure fields like aviation, water, and gas with the combined assistance of agencies such as the Environmental Protection Agency (EPA) and the Transportation Security Administration (TSA).

In a growing effort to close ranks, cyber defense wise, the United States has set up CISA. They are the center for combining joint efforts between the public and private sectors for cyber defense. This is done to combine efforts, if there are critical needs, SRMAs (Sector Risk Management Agencies) will provide protection and all agencies have daily involvement in the cyber defense of our critical infrastructure systems. As we've seen in previous cyber attacks, like NotPetya, oftentimes the direct government agencies are not directly targeted. However, the private sector companies which work for the government are, as there were often not government protection fully extended.

CISA and SRMAs provide a deliberate and proactive solution to ensure that there is an umbrella of cyber security.

Like the command structure for any large military endeavor, there needs to be command centers to strategize and coordinate efforts. There is a plan to build Federal Cybersecurity Centers which will act as these command centers. This is planned to be an expansive build out of the current system. A more evolved form for the large-scale strategy of being able to effectively provide protection to critical infrastructure digital assets and provide the widespread help which is needed.

The central command is called the Joint Cyber Defense Collaborative. This organization was established to bring a combined strength to the defensive approach. This way there can be a balance between the needs of the Federal government and the needs of the private sector and other international partners. Since the threat is non-localized, the defense must be as well.

A coordinated effort needs an effective, responsive game plan when a major cyber attack occurs which requires the government to intervene. While the private sector handles many attacks themselves, there needs to be a very clear plan of action when needed. While still being designed, there has been a founding of the Cyber Incident Reporting for Critical Infrastructure (CIRCIA). This is an organization which collects information from cyber attacks on our infrastructure for further analysis, then action. A methodical approach to developing future response plans needs to have

sufficient data. CIRCIA aims to give this methodology to prevent unorganized scrambling when a major incident occurs.

Modernization is necessary for the United States to lead the way in the future of cyber security for our critical infrastructure. This is not just technologically speaking either. There needs to be a national coming to terms with the realities of cyber security. From Federal employees learning to identify phishing emails to modernizing internal computerized systems there is a plan underway by the Federal government to create the cyber defenses needed to protect the critical infrastructure, which is the heartbeat of our country. New threats many times will not come in physical forms but rather as bad actors seeking to exploit our cyber defensive capabilities to be able to control or damage infrastructure systems. The 2023 National Cybersecurity Strategy seeks to create a trusted defense which allows for the future success of the nation.

Works Cited

- *Defending U.S. critical infrastructure from nation-state cyberattacks researchers combine cyberdefense expertise, network analysis, artificial intelligence, and collaborative-autonomy algorithms to defend the nation's industrial control systems.* Defending U.S. Critical Infrastructure from Nation-State Cyberattacks. (n.d.). https://str.llnl.gov/2022-03/gleason
- House Committee on Energy and Commerce. (2023, May 16). *Protecting critical infrastructure from cyberattacks: Examining expertise of sector specific agen...* YouTube. https://www.youtube.com/watch?v=3QxuxRIztPQ
- Lembright, M. (2023, October 6). *Defending critical infrastructure on the Cyber Battlefield*. Federal Times. https://www.federaltimes.com/opinions/2023/10/06/defending-critical-infrastructure-on-the-cyber-battlefield/
- Mariani, J., Li, T., Weggeman, C., & Kishnani, P. K. (2023, June 12). *Incentives are key to breaking the cycle of cyberattacks on Critical Infrastructure*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html