Midterm Project

Austin Cupp

Old Dominion University School of Cybersecurity

CYSE 425W: Cyber Strategy and Policy

Professor Duvall

October 15th, 2023

General Review of the National Cybersecurity Strategy March 2023.

The National Cybersecurity Strategy March 2023 published by The White House is a plan intended to strengthen the cybersecurity posture of the United States over the long term by achieving two major fundamental shifts in the cybersecurity ecosystem (Lostri & Pell,2023). The two fundamental shifts the strategy keys in on is “Ensuring that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk” and “Increasing incentives to favor long-term investments into cybersecurity” (The United States Government, 2023a). Outlined in the strategy are several specific efforts set to take place over the next three years that will be of interest to federal contractors, those who own and operate critical infrastructures, and technology companies (Cassidy et al., 2023). These efforts will allow the United States to have methods in place to strengthen cybersecurity infrastructure, acquire funding to be put towards the cybersecurity ecosystem, handle incidents, and respond accordingly, and develop an engagement plan to “discourage nations from acting as safe havens for ransomware criminals and strengthen international cooperation in countering transnational cybercrime” (Cassidy et al., 2023). In the strategy are five pillars that were put into place to outline the short and long term “next steps” for the United States cybersecurity ecosystem by outlining sixty-five federal initiatives (Lostri & Pell, 2023). The roles and responsibilities for these initiatives according to the strategy are to be assigned to and carried out by various federal agencies (Lostri & Pell, 2023). The first of the five pillars in the NCS 2023 strategy is the “Defend Critical Infrastructure” pillar, which outlines the importance of “defending the systems and assets that constitute our critical infrastructure,” which is “vital to our national security, public safety, and economic prosperity” as stated in the

strategy itself (The United States, 2023b). Detailed in the pillar is the plan to update the National Cyber Incident Response Plan in a method that allows the government to respond in a coordinated manner and inform the private sector and SLTT partners on how to get help during a cyber incident (The United States Government, 2023a). Noted in the pillar also is the Cybersecurity and Infrastructure Security Agency (CISA) will lead a process to update the National Cyber Incident Response Plan (NCIRP) to more fully realize the policy that "a call to one is a call to all" (The United States Government, 2023a). Guidance will be made clear to external partners on the roles and capabilities of Federal agencies in incident response and recovery (The United States Government, 2023a). The second pillar is the "Disrupting and Dismantling of Threat Actors," which outlines how the United States will combat against threat actors and cybercrime as a whole. Within the text of the pillar is the discussion of how the FBI will work with private, public, federal, and international sector partners in order to combat against the cybercrime ecosystem (The United States Government, 2023a). The CISA is now tasked with leading a complementary initiative that will provide cybersecurity services, cybersecurity training, pre-attack planning, technical assessments, and incident responses to entities who are at high risk of being attacked by a cybercriminal, such as banks and hospitals, to make them less likely to be affected and to reduce the duration and scale of impacts if they are a victim of a cybercrime (Cassidy et al., 2023). The third pillar in the NCS is "Shape Market Forces to Drive Security and Resilience," where it is stated that the U.S. "must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk" (The United States Government, 2023b). Those who are most vulnerable to be a victim of a cybersecurity attack; this pillar wants to shift the consequences of poor cybersecurity away from

them, and instead place them on a non-vulnerable entity with a strong internal cybersecurity ecosystem (The United States Government, 2023b). Another main key of the pillar is to increase software transparency in a manner that allows those who market their software to better understand their supply chain risk and to hold the supply chains themselves accountable for secure cyber development practices (Lostri & Pell, 2023). Doing so will enable the software to be more resilient and secure. Furthermore, as more IoT devices are created and become more commonly used in the world today, there is a need to make sure they are secure and resilient against any threats and bad actors. Pillar number four in the NCS is to "Invest in a resilient future". The pillar begins by discussing the importance that investments and resources are today for the cybersecurity ecosystem in order to enable the flourishing and resilient digital future for tomorrow (Hughes, 2023). Also detailed is how the U.S. can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action (Poremba, 2023). Securing the technical foundation of the internet, as well as the reinvigorating of federal research and development for cybersecurity are outlined as being key points in the pillar as well. The final pillar in the NCS is Forge International Partnerships to Pursue Shared Goals, where it is recognized by the United States that cybersecurity objectives must be pursued on a global scale (Lowery &McAndrew, 2023). Policies and solutions that help safeguard cyberspace "must reflect close collaboration with our partners and allies" (The United States Government, 2023a). The U.S. also seeks to bring about "a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly" (Lostri & Pell, 2023). Helping to achieve this vision five strategic objectives, which are building coalitions to counter threats to the digital

ecosystem, building coalitions to reinforce global norms of responsible state behavior, expanding the United States capacity to assist allies and partners, strengthening international partners' capacity, and securing global supply chains for information, communications, and operational technology products and services (Lostri & Pell, 2023). This strategy was developed to help bolster the United States cybersecurity and cyber ecosystem as a whole and help craft response teams in the case of a cyber incident and cyber threats. A long-term goal is detailed as to how the United States will work internally and globally to ensure that threat actors are mitigated and deterred, ensure the cybersecurity systems are resilient, and those who supply systems do so in a manner that keeps the country safe. Having the five pillars in place allows the strategy to be universally accepted as an effective method to bolstering the United States cybersecurity and cyber ecosystem. This strategy fits in perfectly with a policy that I have taken a notice to, which is the AI Bill of Rights. Two key points outlined in the AI Bill of Rights are Data Privacy and Safe and Effective Systems. The strategy ties in directly with both key points because to maintain a high level of data privacy, the systems that contain the data need to be safe and resilient. Having systems that are "unsafe" or have an unsatisfactory level of security opens the risk that a threat actor may acquire the data in an unauthorized manner, which would cause the organization to have a major cyber incident and put the person who "owns" the data at risk. Having the NCS strategy not only helps ensure that the United States critical cyber infrastructure is safe, but it also enables for other policies, such as the AI Bill of Rights, to be more effective and it helps safeguard the United States citizens whose data is in cyber ecosystem.

PILLAR ONE: DEFEND CRITICAL INFRASTRUCTURE

The defend critical infrastructure pillar is the first pillar in The National Cybersecurity Strategy March 2023, and it outlines the importance of "defending the systems and assets that constitute our critical infrastructure," which is "vital to our national security, public safety, and economic prosperity" (The United States Government, 2023b). This pillar is aimed at crafting a model that equally distributes the risks and responsibilities of collaboration defense while delivering "a foundational level of security and resilience for our digital ecosystem" (The United States Government, 2023a). The pillar discusses how those who own and operate critical infrastructure need to have cybersecurity protections in place so that any potential threats and bad actors have extreme challenges in disrupting any infrastructure if they attempt to do so (Lostri & Pell, 2023). By having the protections in place, it will lead to the effective collaboration between safeguarding against threats and bad actors and being able to response to a cyber incident (The United States Government, 2023b). Outlined are how new cybersecurity requirements in critical sectors have been put in place and new cyber authorities will be required to set regulations that lead to more efficient and safer cybersecurity practices at scale in other sectors (Maruyama, 2023). The work private sectors have done to engage in collaborative defenses is also discussed, and how the public-private sector has collaborated to increase preparedness and promote effective measures against bad actors and malicious activity (Cassidy et al., 2023). The pillar details how the United States must build new and

innovative cyber capabilities so those who own and operate critical infrastructure, product vendors and service providers, and Federal agencies have the ability to collaborate with each other at speed and scale. It is also outlined within the pillar how incidents shall be dealt with, which is by federal response efforts that "need to be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners" (The United States Government, 2023b). In the pillar also is the discussion that the Federal Government itself must better support the defense of critical infrastructure by making its own systems more defensible and resilient, and how the current administration in office is committed to improving Federal cybersecurity through long-term efforts. Noted also is how new cybersecurity regulations and implementations can be a model for critical infrastructure across the United States regarding digital systems (Maruyama, 2023). I chose this pillar to review because of the detail that is given to the defense aspect of critical cyber infrastructure in the United States digital ecosystem. Having strong defenses in the digital ecosystem is a must due to how many bad actors attempt to gain unauthorized access to systems, whether they are federal government, public, or private sector systems. In the last excerpt of the pillar, it is discussed how the federal government can bolster the defense of critical infrastructure by making its own systems more resilient and defensible (The United States Government, 2023b). This is a key point as our government's digital ecosystem for example, contains a litany of military secrets, information related to and about the economy, and personal data relating to the citizens of the United States. Having weak cyber defenses would allow breaches and other cyber events to occur at a constant basis and would put the citizens of the United States at a large risk to have personal data compromised. This increases the need for coordinated and tightly integrated federal response efforts involving

the private sector and State, local, Tribal, and territorial (SLTT) partners, which is discussed in the NCS. Having response efforts in the case of a threat occurring is key to being able to mitigate and quickly eliminate the threat from the system that is under attack. Overall, this pillar to me is extremely important due to the emphasis placed on discussing and outlining the need to have a strong cybersecurity system, effective collaboration to bolster defense efforts, an effective way to respond to malicious activity and bad actors and how to prevent further damage if a cybersecurity event does occur, and how the government can improve its own systems to help better defend critical infrastructure.

References:

Cassidy, S. B., Fein, A., Huffman, R., Karbassi, S., Skeath, C., & McMurrough, M. (2023, July 21). *White House releases implementation plan for the National Cybersecurity Strategy*. Inside Privacy. https://www.insideprivacy.com/cybersecurity-2/white-house-releases-implementation-plan-for-the-national-cybersecurity-strategy/

Hughes, C. (2023, March 2). *2023 National Cybersecurity Strategy. A Societal Inflection Point*. Resilient Cyber. https://resilientcyber.substack.com/p/2023-national-cybersecurity-strategy

Lowery, J., & McAndrew, E. (2023, March 10). *Key takeaways from the US National Cybersecurity Strategy*. JD Supra. https://www.bakerlaw.com/insights/key-takeaways-from-the-us-national-cybersecurity-strategy/

Lostri, E., & Pell, S. (2023, September 19). *The Biden Administration's Implementation Plan for the national cybersecurity strategy*. lawfaremedia. https://www.lawfaremedia.org/article/the-biden-administration-s-implementation-plan-for-the-national-cybersecurity-strategy

Maruyama, M. (2023, March 4). 米国 国家サイバーセキュリティ戦略を発表. まるちゃんの情報セキュリティ気まぐれ日記. http://maruyama-mitsuhiko.cocolog-nifty.com/security/2023/03/post-d88249.html

Poremba, S. (2023, May 9). *The Biden Administration's 2023 cybersecurity strategy*. Security Intelligence. https://securityintelligence.com/articles/the-biden-administrations-2023-cybersecurity-strategy/

The United States Government. (2023a, March). *National Cybersecurity Strategy March 2023* . The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The United States Government. (2023b, July 13). *Fact sheet: Biden-Harris Administration publishes the National Cybersecurity Strategy Implementation Plan*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/#:~:text=Pillar%20One%20%7C%20Defending%20Critical%20Infrastructure&text=1)%3A%20During%20a%20cyber,know%20how%20to%20get%20help.