

General Review of the National Cybersecurity Strategy March 2023

William Xue

Old Dominion University School of Cybersecurity

CYSE 425W: Cyber Strategy and Policy

Professor: Teresa Duvall

November 5, 2023

A cybersecurity strategy is a set of guidelines, procedures, and standards that an organization implements to safeguard its computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, destruction, and response to cyberattacks. This paper will generally review “The National Cybersecurity Strategy” of the White House March 2023. The selection of this policy is motivated by its global significance, given the United States' position as a technological leader and its extensive reliance on digital infrastructure, making it crucial to comprehend how the strategy was developed, how it will be implemented, and where it fits into the larger national and global cybersecurity landscape.

According to the White House (2023), the National Cybersecurity Strategy includes 5 pillars: (1) Defend Critical Infrastructure, the strategy urges the U.S. to boost critical infrastructure's resilience to cyberattacks, working with public-private partners to spot and fix weaknesses, and draft and enact incident response plans. (2) Disrupt and Dismantle Threat Actors, this strategy calls for the U.S. to be more proactive in disrupting and dismantling cyber threats, working with allies and partners to share intelligence, levy sanctions, and take other law enforcement actions against cybercriminals. Galinec et al. (2017) supported that applying security practices related to defensive actions involving or relying upon information technology and/or OT environments and systems. (3) Shape Market Forces to Drive Security and Resilience, this strategy acknowledges the private sector's crucial role in enhancing cybersecurity. It urges the U.S. to collaborate with industry partners to establish and implement security standards, and to promote the adoption of best practices. (4) Invest in a Resilient Future, this strategy calls for the U.S. to invest in the R&D of new cybersecurity technologies and capabilities, including next-gen tools, improving cyberattack detection and response methods, and training a new generation of cybersecurity professionals. (5) Forge International Partnerships to Pursue Shared Goals, this strategy

acknowledges cybersecurity as a global challenge requiring a global response. It urges the U.S. to collaborate with allies and partners on intelligence sharing, cybersecurity operations, and common norms and standards.

The National Cybersecurity Strategy was created to address the growing cyber threats and attacks facing the U.S. government, businesses, and citizens. The increase in cyber espionage, ransomware attacks, and the potential for digital warfare underscored the urgent need for a comprehensive cybersecurity policy. According to Rizal and Yani (2016), the government needs to anticipate cyber threats by formulating cyber security strategies and creating comprehensive plans to defend against cyberattacks.

The National Cybersecurity Strategy is applied through many approaches. First, the strategy emphasizes collaboration between government agencies and the private sector to strengthen cybersecurity measures to enhance cyber defense. Second, the strategy adopts a proactive position by imposing consequences on those who participate in malicious cyber activities to perform deterrence. Third, the policy places importance on improving incident response capabilities to minimize the impact of cyber incidents and enable rapid recovery.

The National Cybersecurity Strategy is a key part of the U.S.'s broader national security framework. It aligns with national policies and initiatives, such as the National Security Strategy and the National Defense Strategy, to ensure that cybersecurity is a core part of national security. This strategy has international implications, as cyberspace has no borders, and threats often come from foreign actors. Sunkpho et al. (2018) mentioned that the countries should work together to implement cybersecurity policies and laws to promote innovation and economic growth, while also protecting national security and citizens' privacy. The U.S. currently collaborates with allies

and international organizations to share information, conduct joint cyber exercises, and establish norms of responsible state behavior in cyberspace.

The U.S. National Cybersecurity Strategy is a crucial policy framework that protects the country's digital assets and critical infrastructure. It was developed in response to the rising cyber threats and the recognition of cybersecurity's essential role in national security. The strategy's multifaceted approach, covering defense, deterrence, incident response, and international cooperation, highlights its importance in protecting the U.S. and contributing to global cybersecurity efforts. In an era when cyberspace is critical to national and international security, this policy serves as a shining example of resilience, cooperation, and strategic vision.

Pillar one of the National Cybersecurity Strategy March 2023 focuses on defending critical infrastructure. This pillar urges the U.S. to boost critical infrastructure's resilience to cyberattacks, working with public-private partners to spot and fix weaknesses, and draft and enact incident response plans. Hemme(2015) argued that “critical infrastructure is highlighted as a growing potential vulnerability and recognized that the United States has to view the U.S. national infrastructure from a security perspective due to its importance to national and economic security”. This pillar asks for a strong and flexible defense system to protect both government resources and the critical infrastructure of the private sector. Defending the energy infrastructure, financial markets, transportation networks, and power grid, for instance. It emphasizes how crucial it is to recognize weaknesses, evaluate risks, and put preventative measures in place in order to stop cyberattacks.

To defend critical infrastructure, the National Cybersecurity Strategy March 2023 refers to a few methods that the government should take as follows: First, the government should work with

private partners to develop and implement cybersecurity standards and best practices and identify and patch the vulnerabilities. Second, the U.S. should invest in research and development to develop new cybersecurity technologies to improve the security of the nation's industrial control systems (ICS) to keep the technologies up to date. This pillar encourages the adoption of best practices and standards in an effort to strengthen ICS security, given its susceptibility to cyberattacks. Third, the government should improve the country's cyber workforce and enhance the exchange of threat intelligence between the public and commercial sectors.

This National Security Strategy also acknowledges the crucial role that territorial, state, municipal, and tribal governments have in protecting critical infrastructure. In order to provide these governments, with the tools and assistance, they require to safeguard their critical infrastructure systems, the federal government will collaborate with them. The National Cybersecurity Strategy is a comprehensive and ambitious approach to protect the country's critical infrastructure from cyberattacks. The strategy focuses on strengthening critical infrastructure systems' resilience is crucial since it will assist in ensuring that the country can survive even the most sophisticated cyberattacks and recover from them.

In summary, defending critical infrastructure is an essential element of larger national policies that include public safety, innovation in technology, resilience, economic stability, and international relations in addition to national security. The safeguarding of critical infrastructure systems and services is not only a cybersecurity objective but also a multidimensional aim that contributes to the overall well-being and security of the nation. By securing critical infrastructure, the strategy reinforces the foundation upon which the broader national policy objectives rest, ultimately ensuring the safety, prosperity, and resilience of the United States in an increasingly interconnected and digitally driven world.

References

- Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defense: National level strategic approach. *Automatika*, 58(3), 273–286.
<https://doi.org/10.1080/00051144.2017.1407022>
- Hemme, K. (2015). Critical Infrastructure Protection: Maintenance is National Security. *Journal of Strategic Security*, 8(3), 25–39. <http://www.jstor.org/stable/26465242>
- Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, 4(1), 61-78.
- Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity policy in ASEAN countries. In *17th Annual Security Conference* (pp. 1-7).
- The White House. National Cybersecurity Strategy. (n.d.). <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>