Midterm Paper The National Cybersecurity Strategy: Pillar One The National Cybersecurity Strategy

Christopher Sicle

Old Dominion University School of Cybersecurity

CYSE 525: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 29, 2025

The National Cybersecurity Strategy

Introduction

Released late in the Biden administration term in 2023 was the National Cybersecurity Strategy (NCS). With the rise of cyber threats worldwide, the goal is to enhance and improve the US digital ecosystem (The White House, 2023). The strategy recognizes that the internet has quickly become a way of life for Americans and, at its current pace, will be woven into every aspect of our lives, if not already. The strategy addresses a broad threat landscape surrounding ransomware, nation-state cyber threats, supply chain attacks, and vulnerabilities in critical infrastructure by promoting a proactive defense model. Instead of placing the burden of cyberdefense on individuals, small businesses, and/or municipal governments, NCS moves the needle closer to organizations that are better equipped to handle it, such as the Federal government, critical infrastructure companies, and major tech companies(The White House, 2023).

Objectives and Challenges

The theme that surrounds NCS is that it is a shared responsibility. Before the implementation of NCS, it was observed that the brunt of responsibility was carried by those who aren't in the best position to mitigate cyber risk. Hence, the importance of moving the responsibility to larger, more capable entities. The strategy is also forward-looking, addressing long-term investments in workforce development, zero-trust architecture, and global cooperation. Additionally, NCS builds upon and expands upon earlier policies, such as Executive Order 14028 (Improving the Nation’s Cybersecurity). The objectives were formulated in response to the numerous challenges our cyber world faces—one of the areas experiencing explosive growth

is the targeting of critical infrastructure and supply chains. Additionally, there have been increasing threats from our adversaries and state-sponsored agents.

Five Pillars of NCS

The NCS is structured around five strategic pillars, each designed to address a different area of the national cyber defense challenge. The first pillar, "Defend Critical Infrastructure," focuses on updating and modernizing federal infrastructure systems(The White House, 2023). Also, the implementation of a minimum security requirement and overall enhancement of the relationship and cooperation of the public and private sectors.

The second pillar, "Disrupt and Dismantle Threat Actors", looks to increase the difficulty and price for malicious actors with the implementation of higher-trained and equipped law enforcement and intelligence gathering entities.

The third pillar, "Shape Market Forces to Drive Security and Resilience", aims to reform software liability laws, promote secure-by-design principles, and shift economic incentives to favor better cybersecurity practices, such as having cyberattack insurance.

The fourth pillar, "Invest in a Resilient Future", places a significant emphasis on research and development for the future, such as creating an effective cybersecurity workforce pipeline and innovating in encryption software so that we can stay ahead of threat actors. Also, there is a need to increase private sector innovation investment to help materialize the next generation.

The fifth pillar, "Forge International Partnerships", focuses on strengthening alliances, promoting democratic norms in cyberspace, and countering the rise of digital authoritarianism.

In summary, the 2023 National Cybersecurity Strategy marks a transition from reactive, fragmented cybersecurity efforts toward a strategic, integrated, and future-proof model. It acknowledges that effective cybersecurity must be both a public good and a shared

responsibility. Its success will depend on long-term implementation, cross-sector collaboration, and the ability to adapt as threats evolve. In the next sections, we will take a deep dive into Pillar 1, which focuses on defending our critical infrastructure(Lewis, 2021).

Pillar 1 - Defend Critical Infrastructure

Introduction

The first pillar of the NCS focuses on the foundational protection of one of the nation's most valuable assets: Critical Infrastructure. With critical infrastructure protecting the American way of life, it is considered one of the most targeted assets by threat actors. These infrastructure systems, including energy, water, transportation, healthcare, and communications, are essential for national security, economic stability, and public safety(Lewis, 2021). With digital technology increasingly integrated into modern infrastructure, the strategy acknowledges the cyber risks associated with deterring threats of malicious attacks and the response required to maintain infrastructure integrity.

Change of Standard

One of the main staples being established by the NCS is the shift of voluntary compliance to mandatory standards in the critical infrastructure sector. Before this, the US Government established a voluntary framework known as the NIST Cybersecurity Framework. However, with recent major attacks, such as the 2021 Colonial Pipeline ransomware attack, which disrupted the flow of fuel over most of the East Coast(Lewis, 2021). The attack quickly demonstrated that recommended voluntary cybersecurity measures are no longer sufficient to protect infrastructure. The strategy therefore supports a regulatory approach that gives sector risk management agencies (SRMAs), such as the Department of Energy (DOE), the Department of Homeland Security

(DHS), and the Department of Health and Human Services (HHS), the authority to impose and enforce minimum security requirements.

Cybersecurity and Infrastructure Security Agency (CISA) Role

The Cybersecurity and Infrastructure Security Agency (CISA) plays a lead role in implementing pillar one infrastructure cybersecurity. CISA facilitates public-private collaboration, shares threat intelligence, and supports incident response(CISA, 2022). CISA and the NCS focus on a "whole of nation" effort where the federal and local government and private sector work together to reduce systemic risk. CISA's Joint Cyber Defense Collaborative (JCDC) is a key initiative in this context, bringing together federal and private sector partners to develop and exercise coordinated defense plans(CISA, 2022).

Resilience and Incident Reporting

Another critical portion of pillar 1 is strong resilience and operational integrity. The strategy acknowledges that breaches will be inevitable; hence, the shift focuses on disaster and threat response to cyber infrastructure. Recognizing that even the best defences cannot stop the rapidly changing ways of attack is a massive step towards improving the overall integrity of threat response operations. The strategy calls for investments in zero-trust architecture, redundant systems, and incident reporting requirements to enhance a timely national response from the responsible organizations or companies. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 aligns with this effort by mandating the timely disclosure of cyber incidents, thereby opening the door to faster threat detection and a more coordinated response(CISA, 2022).

Conclusion

Covered was just one of the five pillars that represent the National Cybersecurity Strategy, which highlights the need to secure our nation's infrastructure to withstand the next cyber threat. The strategy doesn't just focus on major development infrastructure; it also emphasizes equitable protection for rural, small, and underfunded providers by utilizing federal funding and grants. Focusing on risk, the NCS emphasises that critical infrastructure is the core of our homeland defense. U.S. aims to reduce the attack surface and mitigate cascading failures across the economy. In doing so, the strategy reinforces cybersecurity as a national security imperative.

References

Cybersecurity and Infrastructure Security Agency. (2022). “Strategic plan: FY 2023–2025”. https://www.cisa.gov/sites/default/files/2022-09/CISA_Strategic_Plan_2023-2025.pdf

Lewis, J. A. (2021). Cyber threats to critical infrastructure: Lessons from the pandemic. “Journal of Cybersecurity & Digital Trust”, 2(1), 45–59.

The White House. (2023). “National cybersecurity strategy”. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf