Analyzing the National Cybersecurity Strategy

Kirk Turner

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Professor Bora Aslan

October 12, 2025

Cybersecurity is an ever-growing field that has become more important in recent times as technology continues to become increasingly abundant across the world. The growth of technical resources also opens the possibility for vulnerabilities to develop in new technological products, so it's important for people to produce ways to combat these ongoing vulnerabilities or cyber threats. One such example was enacted by the U.S. government on March 2, 2023 when an executive order was released by the Biden-Harris administration in attempts to create a more secure digital ecosystem on a nationwide scale. This policy is known as the National Cybersecurity Strategy, and it seeks to create a stronger link between public and private entities by reallocating the impacts of cyber threats from individuals to more capable and well equipped entities. This plan seeks to reach its goals through the implementation of new legislation and regulation, and it outlines five critical pillars, each aimed at achieving a certain objective: 1. Defend Critical Infrastructure, 2. Disrupt and Dismantle Threat Actors, 3. Shape Market Forces to Drive Security and Resilience, 4. Invest in a Resilient Future, 5. Forge International Partnerships to Pursue Shared Goals. The National Cybersecurity Strategy correlates directly to the protection of online users and systems through enhancing security, changing digital responsibilities, and creating a joint-effort to combat cyber attacks amongst public and private sectors.

A more thorough policy was needed to boost resilience and provide a different approach to securing the cyber realm due to the escalation in the number of cyber attacks taking place. The pandemic caused by the Corona Virus outbreak in late 2019 and early 2020 certainly impacted the total number of cyber attacks that took place as people were forced to transition to a remote, online environment for business and education. This abrupt shift provided an opportunity for threat artists to take advantage of end users and businesses who were not conditioned to

operating online (Griffiths, 2025). Further, the colonial pipeline ransomware attack that occurred in 2021 was an incident that shed light to the weaknesses within critical infrastructure systems and resulted in dire consequences to millions of people on the east coast. Therefore, by 2023, it was necessary for the executive branch to step into play and enact the National Cybersecurity Strategy as a means of mitigating and combatting the rising threats in cyberspace. There are two main methods this strategy revolves around to meet the objectives of each of the five pillars: the first method being to rebalance the responsibility to defend cyberspace, and the second is to realign incentives to favor long-term investments. The former method deals with the cooperation between entities who are unable to handle cyber threats on their own and larger corporations who are better suited to address and respond to incidents. This involves shifting the responsibility of cybersecurity from lesser businesses, local governments, and individuals onto those organizations that are more capable. The latter method addresses being proactive in investing into a stronger cyber realm, while still allocating resources to confront attacks that occur in real-time (National Archives, 2023). These two methods provide a new way to resist cyberattacks through collaboration and planning ahead to minimize future threats; by utilizing these means of operation, it's possible to achieve the goals associated with each of the five pillars of the National Cybersecurity Strategy.

The five pillars could be considered the foundation that this strategy rests upon with each pillar aligning different goals and ideals to provide a more resilient digital ecosystem. The first pillar, in specific, calls for a stronger method of securing critical infrastructure with the intent to enhance national security and public safety. Critical infrastructure can be defined as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on

> security, national economic security, national public health or safety, or any combination of those matters (Moteff & Parfomak, 2004).

Bolstering critical infrastructure systems may involve strengthening the fortitude of federal systems and their detection capabilities, updating federal response procedures, or integrating federal cybersecurity facilities to create a more widespread defense system (Scott, 2023). This pillar could be considered the most important as it represents the core of the United State's cyber threat resilience.

Without critical infrastructure, everyone in the country would be impacted in some way or form, and losing these vital systems could lead to a collapse in public health and safety. As aforementioned, the colonial pipeline ransomware attack is an example of a cyber incident that took place against a critical fuel pipeline running along the east coast of the U.S. A large number of people were heavily impacted by the attack, and it resulted in severe inflation of gas prices, fuel shortages, and widespread mania to those who were affected. Even though the timeline of this attack was relatively short-lived, it established a nationwide concern regarding national security and the vulnerabilities within critical infrastructure systems. Due to the consequences that may result from an attack against critical infrastructure, this pillar goes farther beyond simply protecting the technology linked to these systems as it also stabilizes public trust that people can rely on these systems to remain operational at any given moment.

An important aspect surrounding this pillar concerns the collaboration of private sector entities and the federal government. A significant portion of critical infrastructure systems are privately owned, therefore, the federal government must rely on the assistance of these private organizations in order to ensure the security of these infrastructure systems. Under this pillar, federal entities shall provide better cybersecurity practices to these critical sectors through new

protocols, regulations, and frameworks that are centered around security and uninterrupted operations (The White, 2023). The cooperation between federal and private sectors can allow for greater innovation towards critical infrastructure to occur, ensuring that these systems stay up to date and protected.

To conclude, the National Cybersecurity Strategy functions under methods of collaboration and investing in the future to ensure that the digital environment remains as secure as possible and new threats can be dealt with swiftly and accordingly. Securing critical infrastructure systems is a crucial section of this strategy as these various industries can impact the country as a whole. Citizens use many of these systems on a daily basis, and they place their trust in the federal government and private sectors that the infrastructure of this country remains secure and operational at all times. The success of this pillar and the strategy as a whole relies upon the shared responsibilities of public and private sectors as well as the ability for these entities to adapt and respond to virtual threats correspondingly.

References:

Griffiths, C. (2025, January 7). *The latest Cyber Crime Statistics* . AAG IT Services. https://aag-it.com/the-latest-cyber-crime-statistics/

Moteff, J., & Parfomak, P. (2004, October 1). *Critical Infrastructure and key assets: Definition and identification*. Defense Technical Information Center. https://apps.dtic.mil/sti/html/tr/ADA454016/

National Archives and Records Administration. (2023, March 2). *Fact sheet: Biden-Harris Administration Announces national cybersecurity strategy*. The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Scott, B. (2023, July 31). *National Cybersecurity Strategy*. Federal Communications Commission. https://www.fcc.gov/sites/default/files/ONCD%20National%20Cybersecurity%20Strategy%20-%20FCC%20BGP%20Wrkshp073123.pdf

The White House. (2023, March 1). *National Cybersecurity Strategy* . National Archives and Record Administration. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf