The National Cybersecurity Strategy

Samantha Riggs

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 29th, 2025

The National Cybersecurity Strategy was officially released in 2023. This strategy focuses on and builds itself upon five pillars: defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future, and forging international partnerships to pursue shared goals. This national policy builds upon pre-existing strategy and policy by adding to and adapting the contents to better fit the current state of national cybersecurity concerns. Nations around the world are investing significantly in cybersecurity, recognizing its indispensability in countering cyber threats and ensuring the comprehensive protection of their citizens, infrastructure, and future sustainability (AlDaajeh & Alrabaee, 2024).

Collaboration is essential to the creation of successful cybersecurity strategies and policies. Different ideas, perspectives, and expertise are all integral to this success. This specific strategy "recognizes that robust collaboration, particularly between the public and private sectors, is essential to security cyberspace." (National Archives and Records Administration, n.d.). Furthermore, it addresses the need shifting of burden concerning cybersecurity from smaller entities like small businesses and local agencies and onto qualified, best-positioned organizations. It also works to increase and realign current incentives to favor long-term investments in cybersecurity matters.

This strategy also fits into the broader picture of the cybersecurity efforts on a national level. It was made in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), which has their own strategic plan that aligns with the National Cybersecurity Strategy. While the National Cybersecurity Strategy focuses on more overarching, all encompassing goals, CISA's strategy goes further into how exactly the goals set in the National Cybersecurity Strategy will be executed. This collaboration exemplifies how integral the collaboration in

national policy is to properly address the complex, ever changing landscape of the modern cyberspace.

One of the main driving factors behind the development of this policy is the need for an updated national strategy to address modern cybersecurity concerns brought forward by an increase in digital dependency. The cyberspace of today allows for connection and collaboration between individuals, businesses, and even nations. As a result, almost every industry, along with general aspects of everyday life, has modern technology integrated within it, for better or for worse. While there are many pros to this improvement and continued development of the cyber world, it leaves more opportunities and incentives for malicious actors to infiltrate various industries for their own gain. One industry that faces an increased cybersecurity concern due to this integration is national critical infrastructure.

Another factor is the advantage that collaboration and partnerships play in successful cybersecurity strategies. The National Cybersecurity Strategy encourages relationships between the private sectors (organizations, businesses, and government agencies), with the public sector (the general public and small businesses). Additionally, this collaboration is also promoted on an international level between the United States and other nations of the world. The threat that the modern technological age poses proves to be a global issue; therefore global cooperation is a necessity to ensure cyber safety and security.

The first of the five pillars of the National Cybersecurity Strategy focuses on defending industries within the national critical infrastructure sector. This pillar states the need to establish cybersecurity regulations and requirements in these critical sectors in addition to streamlining existing regulations. Additionally, the strategy recognizes a strategic objective of updating federal incident response plans in the event an attack by establishing which agencies need to be

contacted and what actions need to occur, essentially providing a “game plan” of sorts should a cybersecurity event ever occur.

There are sixteen critical infrastructure sectors categorized by CISA that the organization notes that “their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” These sixteen sectors are as follows: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government services and facilities, healthcare and public health, information technology, nuclear reactors and waste, transportation systems, and water systems. This list exemplifies just how many integral industries are encompassed within the term “critical infrastructure” and highlights the enhanced need for assured cybersecurity measures.

In a theoretical scenario, say that a cyber attack on the emergency services sector. This sector is meant to maintain public safety and ensure that life saving measures are performed quickly and efficiently in a variety of emergency situations. CISA breaks this particular sector into five subsectors: emergency management, emergency medical services, fire and rescue services, law enforcement, and public works. Regardless of which subsector or combination of subsectors are affected by this successful theoretical attack, the resulting consequences would be detrimental. A loss of emergency service communication is a notable one. Without the ability for the public to contact the appropriate authorities in the event of an emergency, physical, mental and emotional damage to the nation’s citizens would be immeasurable. This is just one example as to how integral critical infrastructure is to society, and how its dismantling due to a cyberattack would affect the safety of everyone in the nation.

To conclude, the National Cybersecurity Strategy is a national cybersecurity effort that works to address cyber concerns on a national level. This strategy makes an effort to add to current existing policy and introduce new policies as well. Defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future, and forging international partnerships to pursue shared goals are five pillars that the strategy identifies as key areas of focus. By focusing on these five pillars the strategy establishes, an all-around policy that promotes collaboration and establishes a strong foundation is formed.

References

AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, *141*, 103845. https://doi.org/10.1016/j.cose.2024.103845

Cisa Cybersecurity Strategic Plan: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.-a). https://www.cisa.gov/cybersecurity-strategic-plan

Critical Infrastructure Sectors: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.-b). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

National Archives and Records Administration. (n.d.-a). *National Cybersecurity strategy | ONCD | The White House*. National Archives and Records Administration. https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

National Cybersecurity Strategy. (n.d.-c). https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf