Midterm Paper on National Cybersecurity Strategy March 2023

Ian Hagmann

School of Cybersecurity, Old Dominion University

CYSE 425: Cybersecurity Strategy and Policy

Francis Hiser

11/2/2025

Midterm Paper on National Cybersecurity Strategy March 2023

In this paper, I will be giving an overview of the US National Cybersecurity Strategy (NCS) document that came out in March 2023, explaining how pillar two is applied in a specific setting, and analyzing how the document fits into a broader national policy.

Overview of National Cybersecurity Strategy

The National Cybersecurity Strategy document opens with a note from the president at the time, Joe Biden, about how much digital technology has changed our lives and the need for cybersecurity. Next, the introduction goes into strategic opportunities for the US when it comes to emerging technologies and trends as well as the evolution of malicious actors. Then the five pillars that make up most of the document are introduced being:

(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, and (5) Forge International Partnerships to Pursue Shared Goals.

To follow the goals of the pillars, two fundamental shifts must be made: to rebalance the responsibility to defend cyberspace between smaller organizations or individuals and large organizations, and to realign incentives to favor long-term investments over short-term ones. The introduction closes with a section on a plan to build on existing policy.

Pillar One, to defend critical infrastructure, is about refining and creating regulations for critical infrastructure, encouraging public and private sector collaboration on a nation-wide network, fusing federal cybersecurity centers for better coordination, and updating federal cyber security and incident response.

Pillar Two, to disrupt and dismantle threat actors, describes better collaboration on federal disruption campaigns, heightening the ability of the private and public sector to work together on catching adversaries, accelerating information sharing and victim notification, preventing US infrastructure from being used maliciously, and undermining the potential for profit from ransomware.

Pillar Three, shaping market forces to drive security and resilience, focuses on the private sector with holding accountable those who hold our personal data and those that knowingly provide flawed cybersecurity products or services, improving the security of IoT devices on the market, shifting liability to entities that fail to secure their software, supporting security through federal grants and other incentives, and possibly supporting the cyber insurance market in case of a catastrophic event.

Pillar Four, to invest in a resilient future, seeks to make stronger the general security of the internet, provide federal cybersecurity research and development, prepare for the repercussions of quantum computing on cyber security, secure the electric grind, support desirable digital identity solutions, and expand the cyber workforce in the US.

Pillar Five, forging international partnerships to pursue shared goals, aims to create a coalition to counter threats over the internet, strengthen the security of those coalition partners, bolster our ability to aide allies during cyber attacks, hold accountable the nations that aren't behaving responsibly in regard to cyber, and secure global supply chains in both a physical and digital sense.

Pillar Two: Disrupt and Dismantle Threat Actors

The last objective of Pillar Two is to counter cybercrime and defeat ransomware. The motivation to use ransomware comes from the hope that some victims will pay the ransom to get their data back. Victims will only pay the ransom if there is some trust that they will receive a working decryption key. If enough actors that employ ransomware do not hold up their end of the deal, then no victims would pay and ransomware would fall out of use except for purely destructive purposes. According to Zakaria (2023), "32% of companies pay the ransom demands to recover their data, further enabling cybercriminal groups to operate like legitimate businesses." The U.S. doesn't want to take an offensive approach to solving this problem, so the only other way is to prevent ransomware from being profitable by tracking the payments. Another approach could be to have people make effective backups, but that is not foolproof or truly a solution to the problem.

One of the initiatives listed in the National Cybersecurity Strategy Implementation Plan (2024) is to, "Support other countries' efforts to adopt and implement the global anti-money laundering/countering the financing of terrorism (AML/CFT) standards for virtual asset service providers." The U.S. Treasury is responsible for leading multiple agencies in working with international partners in the Financial Action Task Force. The idea is to help with adoption of the anti-money laundering and countering the financing of terrorism standards which can disrupt ransomware payments and other illicit movement of money. The U.S. would provide technical assistance to Financial Action Task Force members that need it and encourage other members to do the same.

Most of the time, ransomware payments are expected in the form of cryptocurrency to a specific wallet address, which is a long string of number and letters. When it comes to seizing cryptocurrency as proceeds from a crime, it is necessary to prove that the crypto being forfeited is directly traced to a crime (Christiansen & Jarrett, 2019). Criminals are doing all they can to make it difficult to trace the ransom payments. Even once the cryptocurrency is traced, it can still be a challenge to explain how in a courtroom. Seizing cryptocurrency has to be tackled differently depending on where the wallet is and the nature of it. If it is physical, then cooperation will be needed to make a boots on the ground arrest and seizure. If the wallet is digital and held by a U.S.-based organization, then a simple seizure warrant will be issued to the organization. A wallet that is digital and overseas would require the cooperation of that nation's government.

Broader National Policy

Much of the NCS document talks about already existing agencies, regulations, policies, and executive orders. Specifically, the introduction's section "BUILDING ON EXISTING POLICY" names Executive Orders (EO) 14028, 14017, 13800, 13691, and 13636. EO 14028, "Improving the Nation's Cybersecurity," follows much of the same ideas with greater intelligence sharing, modernizing federal cyber security, supply chain security, federal response to incidents, and more. EO 14017 is also about supply chains but is focused on American ones. Executive Orders 13800, 13691, and 13636 are about federal networks and critical infrastructure, information sharing, and critical infrastructure cybersecurity respectively. The section also talks about how the 2023 NCS replaces the 2018 one but continues its priorities.

References

Christiansen, N. B., & Jarrett, J. E. (2019). Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset Asset Forfeiture and Money Laundering. *Dep't of Just. J. Fed. L. & Prac.*, *67*(3), 155–180. https://heinonline.org/HOL/PrintRequest?handle=hein.journals/usab67&collection=journals&div=49&id=639&print=section&sction=49

The White House. (2023). *NATIONAL CYBERSECURITY STRATEGY*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House. (2024). *NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf

Zakaria. (2023). Cyber Threat Actors Review. *CRC Press EBooks*, 84–101. https://doi.org/10.1201/9781003404361-5