National Cybersecurity Strategy: An Analysis of Shaping Market Forces

Danielle Caplinger

Old Dominion University

CYSE 425W: Cyber Strategy & Policy

Professor Hiser

March 29, 2026

National Cybersecurity Strategy Overview

Released in March of 2023 by the Biden-Harris administration, the National Cybersecurity Strategy is a policy framework that establishes two foundational shifts in the United States' perspective and approach in cyberspace. First, emphasis is placed on rebalancing the defense of cyberspace to make organizations that are better equipped to do so with higher responsibility. Additionally, a forward-looking approach is proposed in order to balance cyber defense from emerging threats while planning for a future where resiliency is key (The White House, 2023). Together, these shifts reflect an evolution of policy regarding cyberspace to better align the United States' capabilities where they are most effective. As such, understanding why these shifts were necessary and how its five pillars interact is essential to fully comprehend key cyber policy decisions in the years following.

Development of the NCS

As with any policy initiative as comprehensive as the 2023 National Cybersecurity Strategy, it was not made without cause. Instead, the NCS was created to better align the United States' ability to protect and defend cyberspace in an increasingly interconnected world where threats are becoming more frequent, widespread, technically complex, and potentially catastrophic. In the strategy itself, attention is called to the evolution of malicious cyber activity "from nuisance defacement, to espionage" and all the way to "cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy" (The White House, 2023). This increasingly volatile threat environment has made actionable policy a necessity where existing approaches were failing. As Soliman and Jindal note, the strategy "recognizes the present realities where end users bear a disproportionate burden for reducing such risks and, in an ambitious outlook change, seeks a legislative mechanism to enforce liability

on providers when they fail to meet basic security standards" that can prevent such threats (Soliman & Jindal, 2023). In order to best address and correct these issues, the National Cybersecurity Strategy is built around five key pillars: defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals (The White House, 2023). When combined, these pillars form a coordinated framework that serves to shift the advantage in cyberspace back to those defending it and away from the market conditions that had long been exploited by adversaries.

Pillar 3: Shaping Market Forces

As previously mentioned, the 2023 National Cybersecurity Strategy is centered around five key pillars. Of these five, the third pillar is focused on shaping market forces in order to drive security and resilience. The strategy describes this as an active shift of the effects of inadequate cybersecurity protections from those vulnerable to those directly responsible for keeping data and systems secure. For example, market incentives often prompt businesses to favor cost-effectiveness or speed over security that leaves vulnerabilities exposed and lacks a 'security-by-design' product approach. To illustrate, many of the factors "leading up to the SolarWinds cyberattack in 2020" were "short-term profit motives and cost-cutting measures" (Kianpour & Raza, 2024). In order to best reshape such priorities to create a more secure market-driven environment, incentives must be implemented. For this purpose, regulations can be used that "incentivize businesses to invest in cybersecurity" in ways that can greatly mitigate cyber risk (Kianpour & Raza, 2024). This regulatory push is a major shift from prior cyber policy that heavily relied on voluntary compliance that, as Kosseff notes, failed to directly address cybersecurity challenges and produced imprecise rules with little effectiveness.

In shaping these market forces to prioritize cybersecurity, however, there are significant challenges to be addressed. At its core is the need to navigate the fine balance between security and innovation. As described in the National Cybersecurity Strategy, "Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers" (The White House, 2023). Implementing this in practice is complicated by the fact that too many existing cybersecurity laws merely require "reasonable" cybersecurity practices and "punt the question to a judge or jury," leaving companies without clear enforceable standards to meet (Kosseff, 2023). As such, the strategy proposes using legislation regarding liability criteria in order to encourage manufacturers to incorporate cybersecurity best practices into all stages of their production cycle. Doing so would greatly decrease their risk both from technical adversaries and from regulatory fines or other legal consequences. Together, these proposals represent the most structurally ambitious element of the strategy, and one whose success will have significant implications for the broader national policy landscape.

Broader National Policy Context

The implications of the 2023 National Cybersecurity Strategy, and the third pillar in particular, extend well beyond a singular piece of policy. This strategy was developed alongside and is closely integrated with other significant domestic policy investments in this space including the Bipartisan Infrastructure Law, National Security Memorandum 5: Improving Cybersecurity for Critical Infrastructure Control Systems, and Executive Order: 14017: America's Supply Chains (The White House, 2023). Each of these initiatives depends on a secure and resilient digital foundation to succeed where a compromised supply chain or vulnerable energy grid does not just represent a cybersecurity failure, but a failure of national

economic and industrial policy as a whole (Kianpour & Raza, 2024). In this way, the third pillar's effort to hold software manufacturers accountable while reshaping market incentives extends beyond a regulatory proposal and becomes a prerequisite for a future version of American manufacturing and technological leadership that these investments represent (Soliman & Jindal, 2023). As observed by Kosseff, there has historically been a lack of cohesive legal frameworks for effective addressing of cybersecurity challenges with the precision and timeliness they demand. However, the National Cybersecurity Strategy represents the most serious legislative attempt to truly close that gap. This strategy signals a fundamental shift in how the United States government is altering its role in the digital economy from a passive observer to an active guide to a more secure and resilient future in cyberspace. The success of such an endeavor will not just mean differing regulations for applicable companies, but a stronger and more secure digital world for every citizen and the United States as a whole.

References

Jindal, D & Soliman, M. (2026, January 8). *The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?*. Middle East Institute. https://mei.edu/publication/2023-national-cybersecurity-strategy-how-does-america-think-about-cyberspace/

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, 5. https://link.springer.com/article/10.1365/s43439-024-00111-7

Kosseff, J. (2023). Upgrading Cybersecurity Law. *Houston Law Review*, *61*(1), 51–90. https://houstonlawreview.org/article/90792-upgrading-cybersecurity-law

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