National Cybersecurity Strategy & Pillar Five

Nicholas Dorsey

Old Dominion University

CYSE 425W

Md Morshed Alam, PhD

March 7, 2026

Introduction

The United States published the National Cybersecurity Strategy in March 2023 to deal with cyber threats that are on the rise. The strategy creates a coordinated state plan that will defend digital infrastructure, mitigate cyber threats, and enhance economic and national security. It puts the individuals and small organizations as well as the smaller organizations less responsible and leaves the big institutions, technology providers, and the federal government with more responsibility. The strategy sets its objectives in five pillars. They involve protection of important infrastructure, frustrating threat actors, influencing market dynamics, investing in a resilient future, and building global alliances. The overall strategy is summarized and then followed by the analysis of Pillar Five, which is based on international cooperation.

National Cybersecurity Strategy, General Review

The plan acknowledges the fact that cyber threats have become more sophisticated and dangerous over the past few years. Breaking into networks has now become advanced, using advanced tools by state-sponsored actors and organized criminal groups. They attack government systems and critical infrastructure systems. The attacks put the country's economy under a big threat. They also pose a threat to the citizens and undermine national security. The increasing number of ransomware and impactful cyber activities indicates that the threat environment keeps changing. Consequently, the plan focuses on the fact that there is an urgent necessity for more national action.

The document describes how voluntary cybersecurity work cannot deal with these intricate risks. Numerous organizations do not have the resources to invest in powerful security measures. Small organizations find it difficult to stand up and fight well-established rivals. Due

to this disproportion, the plan will entail firmer central leadership and more defined standards of accountability. According to it, the federal government should be at the forefront of the establishment of expectations (The White House, 2023). The strategy also encourages the collaboration of the public and the private. By doing so, the country will be able to create a more stable and strong digital space.

The former pillar is aimed at protecting critical infrastructure. It demands enhanced cybersecurity principles in industries like energy, healthcare, transport, and finance. The strategy guides federal agencies to establish clear specifications and have critical infrastructure owners accountable. It also stimulates the exchange of information between the government and the private sector. This strategy will make sure that organizations that deal with critical services have good security measures in place.

The second pillar will endeavor to disrupt and break down threat actors. The US will deploy all its national power instruments, such as law enforcement, to tackle malicious cyber actors. The plan focuses on the disruption of ransomware organizations and international enemies in advance (The White House, 2023). It also enhances greater cooperation among national and foreign law enforcement officials to detect and put cybercriminals to shame.

The third pillar attempts to influence the market forces to create resilience and security. The strategy holds that the existing market is not rewarding companies in the development of secure software. Rather, it tends to pass the burden of insecurity to users. To counter this imbalance, the federal government will encourage secure-by-design principles and seek liability frameworks for software products. Others under this pillar are that improved transparency and cybersecurity labeling programs are provided to enable consumers to make informed choices.

The fourth pillar is an investment in a strong future. The plan will involve long-term investments in cybersecurity research and development, workforce development, and novel technology. It puts stress on the necessity to obtain next-generation technologies like artificial intelligence and quantum computing (The White House, 2023). It also emphasizes the need to develop a diverse and competent cybersecurity talent force to overcome talent gaps.

In general, the strategy is an indication of the change in the cybersecurity policy of the country. It changes its attention to the proactive approach. It puts on the shoulders of those who are in a better position to mitigate risk. It also incorporates cybersecurity in the wider economic and national security planning. Nonetheless, cyber threats do not adhere to boundaries. Consequently, international collaboration is necessary. This requirement is the direct cause of Pillar Five.

Analysis of Pillar Five

Pillar Five aims at establishing effective international collaboration in order to encourage responsible state conduct in cyberspace. The US is striving to establish an international climate within which responsible behavior is reinforced and irresponsible acts are penalized. This pillar acknowledges that cyber threats are usually beyond national frontiers (The White House, 2023). Due to this, no nation can respond to these threats on its own.

The second significant objective of Pillar Five is to strengthen the international norms and legislation. The United States has attempted to enforce rules of responsible behavior by the state in cyberspace through the United Nations. There are processes like the UN Group of Governmental Experts and the Open-Ended Working Group that have concluded that the current international law covers cyberspace (Grattan, 2026). The United States reinforces the demands of state behavior and stability by endorsing such structures.

The other important initiative is the expansion of collaboration against cybercrime. The approach reinforces the Budapest Convention on Cybercrime, which upgrades international cooperation on cybercrime cases. With the help of this convention, countries can exchange evidence, align legal standards, and react better to cross-border cyber incidents (Segal, 2016). The cooperation of international law is more effective in counteracting transnational cybercriminal networks.

The Pillar Five is also focused on the issue of authoritarian patterns of Internet governance. The strategy cautions against the fact that there are certain governments that push the vision of cyberspace where openness and freedom are curtailed. The United States tries to challenge this vision by establishing alliances that favor a secure Internet (The White House, 2023). This objective is in line with the larger aim of protecting digital rights and transnational digital repression.

The plan also focuses on the need to act jointly to inflict punishment on bad players. It advocates seamless sanctions, diplomatic actions, and attribution of cyberattacks in public. International responses are more effective in the deterrence strategy due to the increased political and economic expenses of malicious behavior (Lindsay, 2015). By acting as a united front, different countries communicate more than when one country takes action on its own.

Pillar five is also based on capacity building. A lot of nations do not have the technical capacity and experience to counter cyber threats. The United States will assist allies in improving their cybersecurity efforts via training, technical aid, and information exchange. Capacity building fosters resilience for the whole world and makes cybercriminals less safe. According to Grattan (2026), cybersecurity is a problem of collective action. Unless the weaker states are able

to protect their networks, they will be used by the attackers. The enhancement of the global capacity is therefore helpful to every nation.

Pillar Five is an expression of a realistic perception of the cyber domain. Cyberspace bridges economies, governments, and transboundary societies. Bad people take advantage of these relationships. Thus, universal collaboration is necessary for good cybersecurity (Segal, 2016). Nevertheless, there are problems with this pillar as well. The cooperation is complicated by political distinctions and legal differences. There are those countries that are opposed to the standards advocated by the United States and its allies. Other individuals might not trust information-sharing systems.

Nevertheless, Pillar Five provides a holistic approach despite such challenges. It incorporates norm development, diplomacy, and capacity building. It also relates cybersecurity to the greater foreign policy agenda. Through incorporating cybersecurity in alliances and partnerships, the United States enhances cybersecurity and geopolitical relationships.

Conclusion

The National Cybersecurity Strategy gives a clear outline of how to deal with contemporary cyber threats. It transfers the risk to the institutions capable of handling them. The five pillars collaborate to defend the critical infrastructure and form international partnerships. Pillar Five is an important element of the strategy. The cyber threats are cross-border, and the nations cannot act in isolation. Through encouraging international standards and developing global capability, the United States aims to establish a safer cyberspace.

References

Grattan, L. (2026). Understanding Cyberspace as a Vector in US-Russian Strategic Competition. https://dspace.cuni.cz/handle/20.500.11956/206717

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7–47. https://direct.mit.edu/isec/article-abstract/39/3/7/30310

Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. Hachette UK.

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