

# **Comprehensive Review of the National Cybersecurity Strategy**

## **A Comprehensive Review of the National Cybersecurity Strategy**

Isaac Flores

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Mehr

June 28, 2025

## **Comprehensive Review of the National Cybersecurity Strategy**

*Modern technology encompasses nearly every part of the lives of modern-day Americans. Because of this, the National Cybersecurity Strategy policy document has been carefully developed in the White House for the benefit of all American citizens. In particular, the fifth pillar involving the forging of international partnerships is of particular concern in today's emerging technological world. This paper analyzes why the National Cybersecurity strategy was developed, its function in today society, its application into a broader national policy in accordance with the interest of the United States of America, and the importance of the fifth pillar involving forming international partnerships.*

### **The Initial Need for a National Cybersecurity Strategy**

The demand for a Federally recognized national strategy policy has been a dire need for years. The demand and construction of this document came as a result of emerging offensive cyberspace operations conducted on the United States like the SolarWinds attack. Willett (2021) explains how the SolarWinds organization provided software called Orion to its clients that provided management of its information technology systems. Willett (2021) also explains how the hackers had infected the SolarWinds software infecting it with malware that compromised its clients. According to Willett (2021), the attack was attributed to Russia by the United States government. This attack that occurred in 2019, in addition to many others, caused uproar among American citizens as federal government actions were lacking. The continued dependency on a digital economy necessitates a national cybersecurity policy. Mayer and Lu (2025) explain how both the United States of America and China are two technopole superpowers compared to any other nation. A nation with a strong reliance on its digital market necessitates some form of cybersecurity strategy. In 2023, these concerns were met in the White House as President Joe

## **Comprehensive Review of the National Cybersecurity Strategy**

Biden was the first United States President who had a detailed and federally recognized document of the approach the United States would have with cybersecurity strategies moving forward. This policy became known as the National Cybersecurity Strategy of the United States of America.

### **The National Cybersecurity Strategy Explained**

The Biden-Harris administration designed the National Cybersecurity Strategy to address the cybersecurity aspects needing to be addressed involving the union of its public and private sectors. This complex document is separated into five pillars of cybersecurity. First, pillar one is associated with defending critical infrastructure. The White House (2023) explains how the administration has addressed this by improving regulations in oil, aviation, and rail sectors. Second, pillar two is associated with dismantling threat actors. The White House (2023) explains how disrupting capabilities are to be designed to make offensive cyber operations non-profitable and ineffective at accomplishing objectives. Third, pillar three involves improving security and resilience in market forces. The White House (2023) explains how its approach to security in market forces involves designing secure devices and making laws to address the risk of loss of data due to cybersecurity bugs. Fourth, pillar four involves investing in a resilient future. Within the context of cybersecurity, this concept can involve making present investments in technology like the internet and the digital economy. The White House (2023) explains how investing in a resilient future involves investments in conducting research development and demonstration with artificial intelligence, encryption, and cloud technology as it will be worked on by federal organizations. Fifth, pillar five is associated with foreign international partnerships. This involves international diplomacy being placed as a priority moving forward to ensure peaceful relations with other nations.

## **Comprehensive Review of the National Cybersecurity Strategy**

### **Application into a Broader National Policy**

The National Cybersecurity Strategy is a great policy within the borders of the United States of America and the cyberspace world. However, this policy fits within the broader national policy of the United States and fulfills its interests in many ways. This policy, specifically pillar five, supports the improvement of diplomatic efforts with other nations. For example, the United States continues to be and is currently involved in an armed conflict between Israel and Iran. Karsh (2023) explains how the Israel and Iran conflict has occurred since 179 with the founding of the Islamic Republic of Iran. This has long been an issue that has failed to be accurately dealt with. The National Security Strategy is a crucial policy to securing international security and supports national diplomatic policies with other nations within the context of cybersecurity. Another aspect of the United States national policy is supporting the economy, specifically its labor market. Givens (2019) provided a brilliant analysis of statistics in his review exploring the current supply and demand imbalance for cybersecurity professionals. The National Cybersecurity Strategy supports an improved labor market as the proposed cybersecurity policy provides ample employment opportunities to support its strategy in a variety of federal enterprises like the U.S. Cyber Command and the Cybersecurity and Infrastructure Security Agency.

### **Importance of Pillar Five**

Pillar five is of major importance due to its application to the world outside of the United States. In particular, the White House (2023) mentions its application of norms to ensure peace and measures to improve the confidence of United Nation members to support the General Assembly. Furthermore, the pillar involves the Declaration for the Future of the Internet involves the alliance of over 60 nations supporting a free and secure digital internet in the future. In

## **Comprehensive Review of the National Cybersecurity Strategy**

addition, the inclusion of the Quadrilateral Security Dialogue is another alliance designed to improve information sharing and incident response to attacks. Compared to others, this pillar involves cooperation in a variety of ways supporting a unified cybersecurity alliance. Another important aspect of this pillar involves its policies regarding the strengthening of its third-world country allies. Lythreatis et al. (2022), explain how news media groups and organizations have identified the digital divide increasing during the pandemic. This is referencing the COVID-19 pandemic that occurred about five years ago and about two years before the Nation Security Strategy was released. Lythreatis et al. (2022) further explain how the pandemic required varying people of different backgrounds to shift to a digital approach to meet their employment obligations. This is important to consider as international companies with employees from different nations may have difficulties matching the technology capabilities of other nations. This issue is addressed in pillar five's plans of the National Security Strategy. The White House (2023) explains how the United States military will aid allied nations in building their cybersecurity capability to prepare those nations to add to the cybersecurity values of the United States. With pillar nations unable to defend themselves from technology giants like Russia and Iran. This may also lessen the digital divide between nations in the future. Furthermore, the issues regarding lack of attribution to many cybersecurity attacks are addressed in pillar five. The White House (2023) explains its new diplomatic efforts involve attributing cybersecurity attacks to the nation responsible while providing consequences for the actions taken. With pillar five in effect, it will aim to hold nations accountable for their wrongdoings toward other nations.

### **Conclusion**

The National Security Strategy of the United States of America was originally developed in response to various state-sponsored attacks, its need for the United States to protect its digital

## **Comprehensive Review of the National Cybersecurity Strategy**

economy, and its need to be addressed by a federally recognized document. The National Security Strategy has five pillars with each of those pillars focused on protecting one aspect on a national scale. Securing infrastructure, preventing threat actors, improving security and resilience of market forces, investing a resilient future, and making alliances with foreign nations are all strategies addressed as part of the Biden-Harris administration's attempts at securing the United States. The National Security Policy supports the current interest of the United States to establish peace with other nations. One example involves the Israel and Iran conflict. Within that context pillar five is of major importance as it involves the building of its allies like Israel to protect themselves and encourage diplomatic efforts with other nations within the context of cyberspace. The manpower required to meet the plans of the National Security Strategy can support and improve the labor market with increased employment that can close the supply and demand imbalance of cybersecurity professionals. Pillar five continues to be of major international importance due to its inclusion of the United Nations alliance and the Declaration for the Future of the Internet alliance to build a more inclusive internet in the future. Pillar Five's plans to support third-world countries help it decrease the digital divide currently present and strengthen their ability to respond to attacks by other nations. Pillar five is needed due to its strategies to attribute cyberspace attacks to the responsible state and provide consequences with legal sanctions. The National Security Strategy continues to remain relevant for academic study and may be the most important cybersecurity document in the history of the world.

## Comprehensive Review of the National Cybersecurity Strategy

### References

- Givens, E. W. (2019). *Perception versus Reality: The Perceived Cybersecurity Workforce Shortage in the United States* (Doctoral dissertation, Capitol Technology University).
- Karsh, E. (2023). The Israel-Iran conflict: between Washington and Beijing. *Israel Affairs*, 29(6), 1075-1093.
- Lythreatis, S., Singh, S. K., & El-Kassar, A. N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, 175, 121359.
- Mayer, M., & Lu, Y. C. (2025). Global structures of digital dependence and the rise of technopoles. *New Political Economy*, 1-20.
- White House. (2023, March). *National cybersecurity strategy*.  
<https://www.cybercom.mil/Portals/56/Documents/Mission%20and%20Vision/National-Cybersecurity-Strategy-2023.pdf>
- Willett, M. (2021). Lessons of the SolarWinds Hack. *Survival (London)*, 63(2), 7–26.  
<https://doi.org/10.1080/00396338.2021.1906001>