

A Collaborative Defensive Approach: The National Cybersecurity Strategy

The National Cybersecurity Strategy, released by the White House, highlights a comprehensive plan to strengthen the nation's cybersecurity posture. The strategy basically aims to achieve the President's vision for a digitally enabled future by creating a digital ecosystem that is equitable and inclusive, promotes prosperity, and aligns with democratic ideals (The White House, 2023). Furthermore, the strategy was developed to protect the nation's critical infrastructure from potential cyber threats, reduce or mitigate cyber risks, and improve resilience against cyberattacks.

As digital technology continues to grow, and has become deeply integrated into everyday life, it has also created the opportunities for cybercriminals to exploit vulnerabilities found in them. With the rapid advancement of technology, the cyber criminals continue to be better, becoming more sophisticated, thereby cyber threats continue to increase over time. In order to combat this challenge, there was a need for effective cybersecurity plans and strategies that could be implemented in both the private and public sectors. These strategies are intended to provide protection and benefits to businesses, private institutions, government organizations, as well as individuals. This growing need for stronger cybersecurity measures ultimately led to the creation of the National Cybersecurity Strategy, which is built around five major pillars. This essay will provide an overview of the National Cybersecurity Strategy, along with a detailed analysis of one of its five major pillars, "Defend Critical Infrastructure."

Over time, technological developments have created new opportunities and emerging trends. While these advancements bring significant benefits to society, they also increase exposure to cyber risks. Today, almost every sector, from healthcare and education to banking, retail, and even household security systems, is connected to the internet. The potential impact

and devastation of cyberattacks on civilian life are unimaginable. Furthermore, in the context of cyber warfare, nations develop and deploy tools to target and attack their adversaries in order to gain political, economic, or strategic advantage. U.S. adversaries such as China, Russia, North Korea, and Iran possess the capability and resources to conduct cyber operations that could compromise U.S. cyberspace and pose significant risks to national security. Therefore, it is crucial for the U.S. government to exercise due diligence in protecting and defending cyberspace from potential threats and attacks. As technological systems become increasingly complex, the National Cybersecurity Strategy serves as a critical framework to address these challenges and enhance national digital resilience.

One of the important aspects of the strategy is the rebalancing the responsibilities of defending cyberspace among different entities. The key idea is to shift the cyber defense responsibilities toward more capable and reliable entities, rather than smaller organizations that may lack the resources necessary to effectively secure themselves, such as local governments and small businesses. For instance, the responsibility for protecting data and ensuring the reliability of critical systems is placed on the owners and operators of those systems, as well as on the companies that design and provide the technological products and services used by these organizations. Additionally, the government also plays a critical role in safeguarding and protecting the shared digital ecosystem. More specifically, its role is to protect its own governmental systems, secure the critical infrastructure, and support private operators in safeguarding their networks. Overall, the strategy emphasizes a model of shared responsibility among government institutions, private companies, and businesses in order to defend and strengthen the nation's shared digital ecosystem.

Another important aspect of the strategy is the realignment of incentives to promote long-term investments in cybersecurity and digital resilience. This includes encouraging society and organizations to prioritize security in the design and operation of their systems. Basically, the strategy emphasizes incentivizing to encourage decision-making that strengthens the resilience and defensibility of the digital ecosystem for the future.

As mentioned above, the National Cybersecurity Strategy is built around five major pillars that guide national cybersecurity policy. Each pillar addresses a distinct aspect of cybersecurity, yet together they form a coordinated strategy aimed at enhancing public safety, safeguarding critical infrastructure, and promoting the economic prosperity of the United States and its allies (The White House, 2023).

The five pillars upon which the National Cybersecurity Strategy is built are: 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. For the purpose of this essay, we will focus on the first pillar of the strategy: Defend Critical Infrastructure.

The first pillar, Defend Critical Infrastructure, is one of the most significant components of the National Cybersecurity Agency, since it focuses on protecting the critical systems and services that are essential for modern society. Critical infrastructure include power grids, water treatment facilities, healthcare, transportation, and financial institutions. Any kind of attack on these critical infrastructure can have severe consequences. For instance, an attack on a power grid could cause widespread electricity outages, while an attack on healthcare systems could disrupt and dismantle patient care. One such major cyberattack on healthcare occurred in May 2017 was experienced in May 2017, the 'WannaCry ransomware attack,' , which infected over

230,000 computers, caused billions in damages, and disrupted critical systems in hospitals across the U.K (Fortinet, 2025). These types of incidents demonstrate how critical cybersecurity is, as it directly impacts public safety and national security. As a result, protecting critical infrastructure has become one of the highest priorities in the national cybersecurity strategy.

This pillar places a great emphasis on the idea of collaborative defense. Since the critical infrastructures are widely operated by private entities, federal agencies along with state and local governments must collaborate with respective stakeholders from these organizations to better protect the systems.

Another aspect of this pillar is to develop minimum cybersecurity requirements specifically for these critical infrastructure systems. Since cyber threats continue to evolve and pose significant risks, it is crucial to establish baseline cybersecurity standards rather than rely on voluntary practices. This will ensure that essential infrastructures are continuously protected and safeguarded.

Information sharing among private and public organizations also plays an important role in defending infrastructure systems. Additionally, the strategy also emphasizes coordination among federal agencies. Government organizations such as intelligence agencies or law enforcement play different roles in defending infrastructure systems. By improving coordination and clearly defining responsibilities, the government can respond more quickly and effectively when cyber incidents occur, ultimately strengthening resiliency.

In conclusion, the national cybersecurity strategy serves as a critical tool that both private and public sector organizations can leverage to strengthen their cybersecurity postures and better protect their critical infrastructure against persistent cyber threats.

References:

Fortinet. (2025). *What is WannaCry? WannaCry Ransomware Attack Case Study*. Fortinet.

<https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack>

The White House. (2023). *NATIONAL CYBERSECURITY STRATEGY*.

<https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>