President Trump's Cybersecurity Strategy for America

Derrick Amissah

OLD DOMION UNIVERSITY

CSE425

Professor Bora Aslan

September 27, 2026

Abstract

In March 2026, the White House published a new U.S. cybersecurity strategy, President Trump's Cyber Strategy for America (White House, 2026). Prior to this strategy, U.S. cybersecurity has cycled through a model of highly prescriptive policies, voluntary sharing between the private sector and government, and a reactive posture that regarded cyber incidents as an inherent risk of business. This strategy represents a shift away from these previous policies and links cybersecurity to national security, economic engagement, the business community, and the influence of the United States in cyberspace (EDUCAUSE, 2026).

This paper will detail the government's current approach to cybersecurity and its relationship to national security. More specifically, this paper will detail the first of the government's primary objectives: Shape Adversary Behavior. This paper will use industry sources, congressional studies, and government strategies to analyze the impact of more effective deterrence, more support for the private sector, and offensive cyber capabilities in creating a more enduring influence in today's cyber domain.

Overview of the Strategy

President Trump's Cyber Strategy for America was released by the White House in March 2026 in response to the increasing national security impact posed by foreign state and criminal actors in cyberspace (White House, 2026). This strategy represents a shift in the perception of cybersecurity from a regulatory or IT function to a core component of government authority and national security. The strategy emphasizes cyber defense, response to incidents that pose risks to critical infrastructure and the American public, and the importance of protecting the nation.

This strategy links defense, technology, and economics. The U.S. will employ military, economic, intelligence, diplomatic and other tools to defend the nation's cyberspace. Six pillars form the foundation of this strategy. The first is to shape adversary behavior by decreasing compliance and excessive regulation. The second is promoting common-sense regulation with AI, post-quantum cryptography, cloud, and zero trust. The third is to modernize and secure federal government networks including energy, supply chains, data centers, finance, and infrastructure. The fourth pillar is securing critical infrastructure ensuring U.S. leadership in cutting edge technologies such as quantum computing, blockchain and artificial intelligence. The fifth is sustaining superiority in critical and emerging technologies that involve countering adversary activity through offensive and defensive activity to disrupt malicious and criminal activity. Lastly, building talent and capacity, this strategy focuses on enhancing the cyber workforce through linkages between the DoD and industry. (Mayer Brown, 2026) All these aims contribute towards a comprehensive strategy that will promote resilience and economic development, encourage innovation, and prevent excessive regulation or undue pressure on small businesses (SBS Cyber, 2026).

Integration into Broader National Policy Frameworks

The goals of the 2026 strategy can be better understood through the lens of U.S. legal, economic, security and other policies. Prior U.S. cybersecurity policies have placed excessive burdens on critical sectors while failing to prevent foreign actors from conducting disruptive, hacking, spying and other malicious cyber activity. The current strategy under the Trump administration marks a shift towards less burden on critical sectors, increased response to malicious cyber activity, and an enhanced capacity for securing U.S. businesses and systems (PwC, 2026).

From the perspective of economic policy, the plan identifies excessive regulation as a hindrance to competition, innovation and businesses in the United States. The government is advocating for "common-sense regulation" that will help standardize cybersecurity across federal, state and international levels as well as between the private sector and government. Moving away from a system that focuses on compliance with regulations by ticking boxes, this plan instead encourages organizations to demonstrate their own ability to defend their systems and react to cyberattacks. The plan also emphasizes the importance of securing U.S. supply chains for critical technologies, decreasing reliance on foreign technology and ensuring the development of critical technologies within the United States (EDUCAUSE,2026). Additionally, it seeks to restrict the use of software and hardware from foreign sources that may pose a security risk to U.S. government and business operations.

In addition, the strategy shows the link between economic security and national security by way of new technologies. The strategy is not overly cautious about specific technologies like blockchain or artificial intelligence. Rather, these technologies are viewed as essential and American industry is expected to dominate and manage them. Changes to the strategy have been analyzed by the Congressional Research Service in relation to existing funding, statutes, and executive orders (Congressional Research Service, n.d). Technological leadership is linked to national security in the strategy. The U.S. is expected to be safe and economically secure if the U.S. also leads in technological advances.

Shape Adversary Behavior

Pillar 1: Shape Adversary Behavior. This is the foundation of the 2026 strategy. This is a new framework for U.S. cyber defense and cyber deterrence. Historically, cyber defense has meant protecting government systems from cyber-attacks; deterrence has been achieved via diplomacy, economic pressure, or system protection. Pillar 1 introduces the concept of preventing threats before they cause meaningful consequences (SBS Cyber, 2026). This pillar enables the continuous identification, disruption and attenuation of adversary activity in cyberspace instead of only response to a cyber incident. (White House, 2026)

Preemptive and Offensive Operations

This strategy authorizes the federal government to employ the full range of U.S. government offensive and defensive cyber capabilities to identify and disrupt threats prior to entry into U.S. systems (White House, 2026). This will involve degrading the cyber capabilities of foreign

government actors, including APTs from adversarial nations, and disrupting foreign criminal cyber operators involved in extortion and ransomware attacks. Additionally, intelligence and cyber agencies will be authorized to attack threats in the adversary's cyberspace rather than waiting for a threat to cause a crisis.

Stopping Financial Support and Cyber Infrastructure

Pillar 1 also seeks to undermine the capital and infrastructure that enables cyberattacks and those that commit to them. It seeks to block illicit cyber ecosystems and facilitate safe transit of funds or safe locations for criminals. Numerous cybercriminals utilize offshore hosting, ransom payments by ransomware, and cryptocurrency to avoid law enforcement while generating illicit income. Reducing access to these services and capital can make cybercrime less appealing, more costly, and more difficult for criminals (Mayer Brown, 2026).

Business and Government Cooperation

A significant shift within Pillar 1 is the release of plans to "unleash the private sector by providing incentives" for the detection, reporting and disruption of malicious cyber assets (PwC, 2026). Previously private sector businesses were primarily concerned with securing themselves from cyber threats. There was also a limitation on information sharing and potential legal implications. The 2026 strategy allow greater collaboration between the government and the private sector. Critical infrastructure operators, banks, technology companies and other businesses are encouraged to collaborate with government agencies in identifying and sharing information about cyber threats and to assist in disrupting cyber threats before causing further harm.

This active approach comes with some difficulties. Allowing private actors to defend against cyberattacks complicates the distinction between governmental and private defensive operations. There is concern that although proactive defense may provide a more rapid level of system protection from attacks, it can also pose potential legal issues. There is potential for inadvertent harm to other systems, legal questions involving international involvement, and potential liability for companies. Regardless, there is a notable shift within Pillar 1 towards recognizing that passive defense is insufficient. Effective cybersecurity involves not only defense, but also the prevention and discouragement of those that pose a threat to U.S. cyberspace.

Conclusion

The new Cyber Strategy for America by President Trump represents a significant shift in the U.S. approach to meeting and mitigating cyber risks (White House, 2026). It emphasizes more robust counteractions by state, non-state, and criminal entities that pose a risk to U.S. cyberspace. In Pillar 1: Shape Adversary Behavior the strategy highlights an increased level of proactivity over merely defensive responses to cyber activity. This proactivity is achieved

through offensive cyber capability, disruption of criminal networks, and engagement with the private sector (SBS Cyber, 2026). Additionally, the strategy emphasizes the enhancement of technology and rules to further bolster the security of U.S. cyberspace (EDUCAUSE, 2026). Implementation of the strategy across government entities, businesses and lawmakers will rely on partnerships, international engagement, effective policy and leadership, and coordination.

References

Congressional Research Service. (n.d.). *CRS product IN12667*. U.S. Congress. https://www.congress.gov/crs-product/IN12667

EDUCAUSE. (2026, April 7). Trump administration releases cyber strategy. *EDUCAUSE Review*. https://er.educause.edu/articles/2026/4/trump-administration-releases-cyber-strategy

Mayer Brown. (2026, March 9). *Trump administration releases Cyber Strategy for America and related executive order on combatting cybercrime*. https://www.mayerbrown.com/en/insights/publications/2026/03/trump-administration-releases-cyber-strategy-for-america-and-related-executive-order-on-combatting-cybercrime

PricewaterhouseCoopers [PwC]. (2026, March 17). *President Trump's cyber strategy for America*. https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/trump-cyber-strategy.html

SBS Cyber. (2026, March). *White House cyber strategy 2026: Key takeaways*. https://sbscyber.com/blog/white-house-cyber-strategy-2026-key-takeaways

The White House. (2026). *President Trump's cyber strategy for America*. https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf