Political Impact of Network Security Policy

George D Smith III

Cybersecurity, Old Dominion University

CYSE 425, Cyber Strategy and Policy

Francis "Skip" Hiser

August 26, 2025

Network security policy has traditionally served as a framework for safeguarding systems, protecting sensitive data, and ensuring the long-term stability of organizations. However, in today's interconnected world, cybersecurity policy has become inseparable from national and global politics. Recent U.S. executive orders emphasize how deeply network security concerns now shape national strategy and international posture (Nation's Cybersecurity, 2025). This paper explores how network security policy intersects with political decision-making, how it influences the United States government, and how it contributes to broader geopolitical strategies around the world.

Cyber Policy as a Political Tool

To understand why network security policies carry political weight, it is helpful to examine well-known cyber incidents. The Stuxnet attack, often cited as one of the most sophisticated cyber weapons ever deployed, demonstrates the potential for digital operations to cause real-world damage. Lachow (2011) notes that as Stuxnet becomes more publicly available, other actors—both nation-states and organizations—may attempt to replicate it. An attack of similar scale on U.S. critical infrastructure could disrupt essential industries, threaten national security, and destabilize public trust.

Given these risks, strong, reliable cybersecurity frameworks are not just technical necessities—they are political imperatives. Policymakers rely on them to mitigate threats that could have far-reaching economic and diplomatic consequences.

Network Security in Domestic Policy and Regulation

The United States maintains a wide array of regulations and federal guidelines grounded in network security principles. Policies such as HIPAA, FISMA, and CISA directives shape how government agencies and private organizations protect data, manage risk, and secure operations. These regulations also play a major political role, especially when tied to national concerns like election security.

Since 2016, election integrity has been a prominent issue in American political discourse. CISA has worked "collaboratively with those on the front lines of elections" (CISA, 2017) to strengthen cybersecurity protections and maintain public confidence. When election systems were officially designated as *critical infrastructure*, cybersecurity policy became directly linked to the preservation of democratic processes. This demonstrates how network security policy can intersect with civil liberties, public trust, and national governance.

Global Cyber Strategies and International Implications

Network security policy also influences international relations and global technology markets. Restrictions on foreign technology—such as concerns over Huawei and other Chinese-based telecommunications companies—highlight how cybersecurity policy can shape market access and geopolitical strategy.

While these measures are often justified by national security concerns, they also allow governments to strengthen domestic industries and control which foreign technologies can operate within national borders. In this way, cybersecurity policy becomes a strategic tool for shaping economic competition and safeguarding technological sovereignty.

Conclusion

Network security policy has evolved far beyond technical guidelines; it is now a central pillar of national and international political strategy. Domestically, it influences how governments regulate industries, protect critical infrastructure, and balance security needs with civil liberties. Globally, it shapes economic policies, technological competition, and power dynamics between nations.

As cyber threats grow more complex, the political impact of network security policy will only expand. Understanding these implications is essential not only for policymakers, but also for cybersecurity professionals who must navigate the intersection of technology, governance, and global strategy.

Sources

Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144. (2025, June 6). The White House. https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*, 118–126. http://www.jstor.org/stable/43133820

Election Security | Cybersecurity and Infrastructure Security Agency CISA. (2017). Cisa.gov. https://www.cisa.gov/topics/election-security