The Ethics of Network Security Policy

George D Smith III

Cybersecurity, Old Dominion University

CYSE 425, Cyber Strategy and Policy

Francis "Skip" Hiser

August 26, 2025

The U.S. National Cybersecurity Strategy (2023) presents a comprehensive framework requiring “tighter regulations, enhanced roles for the private sector, and stronger public–private collaboration to address escalating cyber threats.” While these ideas promise benefits, it also raises ethical concerns regarding rights, the separation of tasks, and possible corruption of political powers. This paper will focus on the ethics of Network Security Policy by assessing costs and benefits and looking at which rights are protected or limited.

Costs and Benefits

My policy benefits include improved security against cyberattacks and better protection of critical systems and data. The policy also “increases accountability for companies and promotes advancements within cybersecurity practices” (Backman & Stevens, 2024). By enforcing security standards, this policy aims to reduce damage from breaches, data theft, and threats to national security. However, costs are severe. Compliance burdens fall mainly on the private sector entities with limited resources. Mandatory standards and liability for breaches may drive up costs for small businesses, possibly increasing prices to consumers.

Rights Protected vs. Rights Potentially Limited

My policy seeks to protect rights such as privacy and security, pushing for stronger protections of data and holding entities accountable for breaches. It also reinforces rights to property and economic rights. With that being said, there is risk to rights including privacy, freedom of speech, autonomy, and due process. Measures such as expanded surveillance, requirements for identification/authentication especially for foreign users. information sharing mandates, and liabilities can all impose limits. My policy emphasis on national security and potential offensive cyber operations raises risks of overreach or misuse.

Conclusion

The U.S. National Cybersecurity Strategy carries significant ethical implications. Its benefits, improved security, and prevention of harm are real. But so are the costs: economic burdens, possible innovation suppression, and most importantly, potential encroachments on privacy, autonomy, and civil liberties. My sources speak on the necessity of balancing rights and duties. For my policy to ethically work, it must have clear oversight, ensure an equal divide of measures, preserve individuals’ autonomy, and guarantee mechanisms of transparency.

Sources

Fucci, D., Romano, S., Baldassarre, M., Caivano, D., Scanniello, G., Thuran, B., & Juristo, N. (2022). A Longitudinal Cohort Study on the Retainment of Test-Driven Development. *ArXiv*, *1*(1). https://arxiv.org/pdf/1807.02971.pdf

Backman, S., & Stevens, T. (2024). Cyber risk logics and their implications for cybersecurity. *International Affairs*, *100*(6), 2441–2460. https://doi.org/10.1093/ia/iiae236