Ethical Implications of the National Strategy to Secure Cyberspace

Morgan Brown

School of Cybersecurity

Cyber Strategy and Policy

Professor Cooper

September 20, 2026

I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community, it is my responsibility to turn in all suspected violations of the Honor Code.

Introduction

The National Strategy to Secure Cyberspace (NSSC), issued by the Bush administration in 2003, established a national framework for protecting cyberspace and critical infrastructure. The strategy emphasized cooperation among government agencies, private organizations, and individual users because much of the infrastructure requiring protection was privately operated. Although this approach sought to strengthen national security, it also created ethical questions concerning privacy, individual rights, government authority, and accountability. Zimmer (2004) identifies tensions between securing cyberspace and preserving the decentralized nature of the Internet, while Burstein (2008) discusses the difficulty of promoting cybersecurity information sharing while protecting privacy and civil liberties. This paper examines the NSSC's ethical implications by considering its costs and benefits, the rights it protects or potentially limits, and whether its approach appropriately addresses individual rights.

Ethical Implications

The NSSC's emphasis on cybersecurity created a tension between collective security and individual freedom. Zimmer (2004) explains that greater government involvement in securing cyberspace raised concerns about state power and the open nature of the Internet. Security measures intended to protect users and infrastructure could therefore affect individual autonomy and freedom in cyberspace.

The strategy's reliance on cooperation between government and private organizations also created ethical questions concerning responsibility and accountability. McCarthy (2018) describes cybersecurity as existing between public security objectives and private interests, including property rights and civil liberties. Distributing responsibility between government and

private organizations can improve cybersecurity efforts, but it can also make accountability less clear when security decisions affect individuals.

Costs and Benefits

A major benefit of the NSSC was its emphasis on cooperation. McCarthy (2018) explains that public-private partnerships distribute cybersecurity responsibilities among organizations with different resources and forms of authority. This approach can strengthen cybersecurity without placing privately operated infrastructure entirely under government control.

However, greater information sharing can create ethical costs. Burstein (2008) discusses the conflict between facilitating cybersecurity research and information access while maintaining privacy protections. Access to information may improve the ability to identify and address cyber threats, but it can also increase the possibility that personal information could be accessed or used in unintended ways. The NSSC therefore presents a balance between the benefits of stronger security and the potential costs to privacy and civil liberties.

Rights and Civil Liberties

The NSSC can protect individuals by promoting the security of systems and information on which they depend. At the same time, cybersecurity practices may affect privacy and other civil liberties. Burstein (2008) demonstrates that cybersecurity information sharing can create tension with privacy protections when personal or communications data become relevant to security efforts.

Government involvement also raises questions about individual autonomy and freedom. Zimmer (2004) identifies concerns about expanding state involvement in cyberspace and its potential effects on the decentralized characteristics of the Internet. McCarthy (2018) similarly raises questions about how authority should be distributed between government and private

organizations. These concerns demonstrate that cybersecurity policies may protect certain interests while placing limits or burdens on others.

Balancing Security and Individual Rights

The NSSC's approach recognizes the need to improve cybersecurity, but its implementation presents unresolved ethical tensions concerning individual rights. Burstein (2008) illustrates the difficulty of balancing information access with privacy, while Zimmer (2004) identifies concerns about the relationship between cybersecurity and individual freedom. McCarthy (2018) adds that dividing cybersecurity responsibilities between public and private organizations complicates questions of authority and accountability.

An ethical approach to cybersecurity requires consideration of both security objectives and their effects on individuals. Protecting critical infrastructure and information can benefit the public, but those objectives should be pursued while limiting unnecessary effects on privacy, liberty, and autonomy. The ethical challenge is therefore maintaining effective cybersecurity while ensuring that individual rights remain an important consideration.

Conclusion

The NSSC created ethical considerations alongside its efforts to strengthen national cybersecurity. Its cooperative approach offered benefits for addressing cyber threats while creating questions about responsibility, privacy, and accountability (McCarthy, 2018). The strategy also raised concerns about balancing information sharing and cybersecurity with privacy and civil liberties (Burstein, 2008) and about the effects of increased government involvement on individual freedom (Zimmer, 2004).

Ultimately, the ethical implications of the NSSC demonstrate that cybersecurity involves more than protecting networks and infrastructure. It also requires consideration of how security measures affect individual rights. The ethical issues surrounding privacy, liberty, autonomy, and accountability illustrate the importance of balancing cybersecurity objectives with the rights and interests of individuals.

References

Burstein, A. J. (2008). Toward a culture of cybersecurity research. *SSRN Electronic Journal*, *22*(1), 167–222. https://doi.org/10.2139/ssrn.1113014

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

Zimmer, M. T. (2004, March). *The tensions of securing cyberspace*. Valauskas, Edward J. Firstmonday.Org. https://firstmonday.org/ojs/index.php/fm/article/download/1125/1045