Assessing the Effectiveness of the National Strategy to Secure Cyberspace

Morgan Brown

School of Cybersecurity

Cyber Strategy and Policy

Professor Cooper

October 11, 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 (President of the United States, 2003). Assessing its effectiveness requires examining whether it addressed the concerns that prompted its development and whether its approach influenced subsequent cybersecurity policies. This paper evaluates the NSSC through scholarly assessments, its lasting influence, and the political, ethical, and social implications examined in the previous papers.

Expert Assessments

Zimmer (2004) examines the tension between the NSSC's security objectives and the decentralized structure of the Internet. His analysis suggests that strengthening cybersecurity can conflict with the Internet's established architecture and values. McCarthy (2018) examines how public-private partnerships distribute authority and responsibility between government and private organizations, highlighting challenges involving accountability and individual rights. Clinton (2015) identifies practices intended to improve government-industry cybersecurity partnerships, addressing difficulties associated with implementing effective cooperation. Together, these studies suggest that the NSSC's cooperative approach addressed an important national need but required effective coordination and clearly defined responsibilities to achieve its objectives.

Assessment Method

I would assess the NSSC using three criteria: its effectiveness in addressing original cybersecurity concerns, its influence on subsequent policies, and its lasting benefits and limitations. First, I would examine historical evidence concerning cyber incidents, infrastructure

vulnerabilities, and improvements in preparedness and incident response following the strategy's introduction. The number of attacks alone would not determine success because cyber threats and adversaries' capabilities change over time. I would instead examine whether the strategy contributed to improved defensive capabilities and coordination.

Second, I would examine how subsequent cybersecurity strategies adopted, modified, or moved away from the NSSC's priorities. Its continued influence would suggest that it provided a useful foundation, while changes intended to address its limitations would identify areas where its original approach was insufficient. Finally, I would evaluate its political, ethical, and social consequences, including accountability between government and private organizations, protection of individual rights, and differences in cybersecurity preparedness. These criteria would allow me to assess both the strategy's practical contributions and the consequences of its approach.

Policy Implications and Overall Assessment

Based on these criteria and my research throughout the previous four papers, I would consider the NSSC partially successful. Its primary strength was establishing cybersecurity as a national responsibility and promoting cooperation among government agencies, private organizations, and individuals. Clinton's (2015) analysis supports the importance of developing effective government-industry partnerships, while McCarthy (2018) demonstrates that distributing cybersecurity responsibilities creates challenges involving authority and accountability.

The NSSC's limitations also affect my assessment. As discussed in my political implications paper, relying on cooperation did not guarantee consistent implementation across privately operated infrastructure. My ethical analysis identified concerns involving privacy and

individual freedom, while my social analysis demonstrated that organizations and individuals have different resources and capabilities for managing cybersecurity risks. Zimmer's (2004) analysis further suggests that security measures must account for the decentralized characteristics of the Internet. These findings indicate that establishing national priorities was valuable, but did not resolve every challenge associated with protecting cyberspace.

I would also consider the NSSC's influence on later policies when determining its overall success. However, continued influence alone would not prove effectiveness, just as the development of newer strategies would not necessarily establish that the NSSC failed. A stronger conclusion would require evidence showing which elements were retained, which were revised, and whether those changes improved cybersecurity outcomes. Based on the available research, I consider the NSSC more successful as an initial national framework than as a comprehensive solution to cybersecurity challenges.

Conclusion

The NSSC's effectiveness should be assessed through its original objectives, influence on subsequent policies, and political, ethical, and social consequences. The scholarly research identifies both the value of cooperation and the difficulties associated with Internet openness and divided responsibility. Ultimately, I consider the NSSC partially successful because it established national cybersecurity priorities, but its approach left challenges involving implementation and accountability. Its significance lies in providing a foundation for subsequent cybersecurity policies while illustrating areas requiring continued improvement.

References

Clinton, L. (2015). Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security*, *8*(4), 53–68. https://doi.org/10.5038/1944-0472.8.4.1456

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

President of the United States. (2003). *The National Strategy to Secure Cyberspace*. https://www.govinfo.gov/content/pkg/GOVPUB-PR-PURL-LPS28730/pdf/GOVPUB-PR-PURL-LPS28730.pdf

Zimmer, M. T. (2004). The tensions of securing cyberspace. *Firstmonday.Org*. https://doi.org/https://doi.org/10.5210/fm.v9i3.1125