Political Implications of the U.S. 2023 National Cybersecurity Strategy

Cayden Bass-Hensley

CYSE 425 Cyberstrategy and Policy

Bora Aslan

10/20/20204

How Politicians and Policymakers Have Addressed the Strategy

The 2023 National Cybersecurity Strategy (NCS) released by the Biden administration has significant political implications across party lines and branches of government. One of the most politically contentious aspects of the NCS is its call for increased regulation of critical infrastructure cybersecurity and shifting liability for insecure software onto companies (Alvarez et al., 2023). The Biden administration and many Democratic lawmakers argue this is necessary to improve the nation's cyber defenses, citing inadequate outcomes from voluntary measures. As stated in the strategy, "the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes" (Hamin et al., 2023).

However, Republican policymakers have strongly opposed granting the executive branch more regulatory authority over businesses. House Republicans expressed "staunch opposition to granting the executive branch additional authority to regulate business sectors (or for passing legislation that would impose liability on software companies)" (Shankar, 2024). Their position stems from a general aversion to government regulation of private industry and concerns about stifling innovation.

Why Politicians and Policymakers Came to These Conclusions

The political divide over the NCS reflects broader ideological differences about the role of government in cybersecurity and the balance between security and other priorities like economic growth and individual liberties. Democrats generally favor a more active government role, while Republicans prefer market-driven solutions with limited regulation.

Another politically charged issue is the strategy's approach to combating misinformation online. Some conservative lawmakers view this as government overreach that could infringe on

free speech. A federal judge in Louisiana even issued an order limiting government communications with social media platforms about removing content (Shankar, 2024). While the Supreme Court has temporarily frozen these restrictions, the debate over the government's role in online content moderation remains heated.

The NCS's emphasis on international cooperation and promoting a multistakeholder model of internet governance also has political ramifications. The Biden administration sees this as crucial for confronting adversaries and safeguarding global digital commerce. However, some politicians argue this approach could compromise U.S. sovereignty or interests.

Ramifications of These Decisions

These political dynamics have significant consequences. Partisan gridlock could delay or water down key initiatives, leaving vulnerabilities in critical systems. For example, Republican opposition contributed to the Environmental Protection Agency withdrawing a memorandum requiring states to assess cybersecurity risks for public water systems (Shankar, 2024). This leaves critical infrastructure vulnerable, as highlighted by subsequent Iranian-backed cyberattacks on U.S. water facilities.

Budgetary politics also impact the strategy's implementation. While President Biden requested increased cybersecurity funding across agencies, Republicans have pushed to slash domestic spending (Shankar, 2024). This has led to appropriations battles, with agencies like the Cybersecurity and Infrastructure Security Agency (CISA) receiving less funding than requested. Such budget constraints could hinder critical initiatives like IT modernization and strengthening cyber defenses.

Inconsistent policies across administrations could create uncertainty for businesses and international partners. However, areas of bipartisan agreement, like the need to counter foreign cyber threats, may see more sustained progress. Bridging these divides will be crucial for developing a coherent, effective long-term approach to national cybersecurity

Conclusion

The 2023 U.S. National Cybersecurity Strategy has exposed significant political divides, primarily along party lines. These disagreements over government's role in cybersecurity, regulatory approaches, and budget allocations have impacted the strategy's implementation and effectiveness. While partisan gridlock poses challenges, areas of bipartisan agreement offer opportunities for progress. Ultimately, the success of the national cybersecurity efforts will depend on policymakers' ability to navigate these political challenges while addressing evolving cyber threats.

References

Alvarez, D., Jehl, L., Chanin, N., & Putnam, A. (2023). The U.S. National Cybersecurity Strategy: Key Takeaways . https://www.willkie.com/-/media/files/publications/2023/theusnationalcybersecuritystrategykeytakeaways.pdf

Hamin, M., Herr, T., Loomis, W., Schroeder, E., & Scott, S. (2023). How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy. Atlantic Council. https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-us-national-cybersecurity-strategy-mark-up/

Shankar, N. (2024). The Biden Administration's National Cybersecurity Strategy: Opportunities and Challenges. Middle East Institute. https://www.mei.edu/publications/biden-administrations-national-cybersecurity-strategy-opportunities-and-challenges