Policy Analysis Paper 5

Owin Ifill

Cybersecurity: Old Dominion University

CYSN 425: Cyber Strategy and Policy

Professor Teresa Duvall

1, December 2024

Assessing the Effectiveness of Cybersecurity Foreign Policy

As cybersecurity threats continue to evolve in the digital age, it is vital to assess the effectiveness of cybersecurity foreign policies. This paper fuses insights from three scholarly articles to evaluate these policies, focusing on diplomatic efforts, capacity-building initiatives, and the integration of cybersecurity into broader foreign policy. Additionally, it examines the ethical, political, and social considerations involved in assessing policy effectiveness.

Scholarly Evaluations of Cybersecurity Foreign Policy

Van der Meer (2015) showcases the importance of diplomacy in enhancing international cybersecurity. He argues that diplomatic tools such as negotiation and collaboration are key to establishing global cybersecurity norms and building trust among nations. Although these efforts are critical, he notes that differing national priorities can complicate international cooperation, making unified agreements challenging.

Pawlak (2016) emphasizes the role of capacity-building in strengthening global cybersecurity resilience. The article argues that providing resources and training to nations with weaker cybersecurity infrastructures is essential for mitigating cyber threats. These capacity-building initiatives, which are integral to foreign policy, enable countries to address cyber vulnerabilities. However, Pawlak cautions that disparities in technological resources can undermine the effectiveness of such programs, especially in less-developed countries.

The National Committee on American Foreign Policy (NCAFP, 2014) explores the evolving U.S. cybersecurity foreign policy. The report stresses the need for a strategic approach that integrates cybersecurity with national security and diplomatic efforts. It advocates for strong

international partnerships to share intelligence and develop coordinated responses to cyber threats. While collaboration is critical, the report also highlights the challenges of reconciling differing national interests, which may hinder the development of unified cybersecurity policies.

Policy Implications

The insights derived from these sources point to several key implications for improving cybersecurity foreign policy. First, strengthening diplomatic channels for cybersecurity cooperation is essential. Diplomatic tools must be leveraged to create binding international norms and frameworks for cyber conflict resolution (Van der Meer, 2015). Second, capacity-building efforts should be prioritized, with a focus on reducing technological disparities between countries. Building the cybersecurity capabilities of all nations is vital for global security (Pawlak, 2016). Lastly, integrating cybersecurity into broader foreign policy is necessary for addressing the complex nature of cyber threats, ensuring that cybersecurity policies align with national and international objectives (NCAFP, 2014).

Proposed Assessment Methodology

To effectively assess the impact of cybersecurity foreign policy, a mixed-methods approach is essential, combining quantitative and qualitative analyses to provide a holistic evaluation. Quantitative metrics can measure tangible outcomes, such as trends in cyber incidents targeting critical infrastructure and participation rates in international capacity-building programs. These indicators provide a clear picture of progress and areas needing improvement. On the qualitative side, stakeholder interviews with policymakers, cybersecurity experts, and

international organizations offer insights into the practical challenges and successes of policy implementation. Additionally, case studies of specific cyber incidents can reveal how effectively the policy mitigates threats and promotes cooperation. Scenario-based simulations add another layer of analysis, allowing policymakers to test the policy's responsiveness to hypothetical cyber crises. This comprehensive approach ensures a thorough evaluation of the policy's effectiveness in addressing cyber threats while identifying areas for refinement.

Ethical, Political, and Social Considerations

Ethical, political, and social considerations must be central to assessing cybersecurity foreign policy. Ethically, policies must respect privacy rights and ensure that surveillance practices do not infringe on civil liberties. Politically, the policy should balance national security concerns with international cooperation, ensuring that diplomacy prevails in resolving conflicts. Socially, cybersecurity initiatives must address inequalities, ensuring that developing nations have access to the resources needed to build robust defenses (Pawlak, 2016).

Conclusion

In conclusion, assessing the effectiveness of cybersecurity foreign policy requires a comprehensive approach. Based on the literature from Van der Meer (2015), Pawlak (2016), and the NCAFP (2014), a mixed-methods evaluation, combining both quantitative and qualitative metrics, is crucial for understanding policy outcomes. While there have been strides in international cooperation and capacity building, further refinement is necessary to address

disparities in resources and reconcile differing national interests. The ongoing evaluation and adaptation of policies will be essential for maintaining global cybersecurity resilience.

References

- National Committee on American Foreign Policy (NCAFP). (2014). Cybersecurity, US foreign policy, and a changing landscape: A new generation speaks out. American Foreign Policy Interests, 36(1), 44-53. https://doi.org/10.1080/10803920.2014.890107
- Pawlak, P. (2016). Capacity building in cyberspace as an instrument of foreign policy. Global Policy, 7(1), 83-92. https://doi.org/10.1111/1758-5899.12260
- Van der Meer, S. (2015). Enhancing international cyber security: A key role for diplomacy. Security and Human Rights, 26(2-4), 193-205. https://doi.org/10.1163/18750230-02602001