Political Implications of Cybersecurity Incident Response Policy

Donte Staves

School of Cybersecurity, Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Professor Francis Hiser

September 28, 2025

Abstract

Cybersecurity Incident Response (CIR) has become a cornerstone of national security strategy in the United States, with Cybersecurity Incident Response Teams (CSIRTs) leading efforts to contain and reduce cyberattacks. While largely driven by technical needs, CIR policy has significant political implications, specifically concerning federal authority, bureaucratic governance, interagency coordination, and international cooperation. Politicians and policymakers influence and are also influenced by how CIR frameworks are implemented, debated, and measured. This paper examines these political dimensions by analyzing how decision-makers justify policy actions, what strategic or ideological factors shaper their responses, and what broader governance implications emerge. Drawing from political science and cybersecurity literature, it argues that CIR is not only a technical solution but also a politically embedded strategy that is shaped by institutional interests, public accountability, and international norms.

Keywords: cybersecurity, CSIRTs, governance, federalism, accountability, cyber diplomacy

Introduction

Amid growing cyber threats from state and non-state actors, Cybersecurity Incident Response (CIR) has emerged as a crucial component of U.S. cybersecurity policy. Federal efforts typically revolve around the development and deployment of Cybersecurity Incident Response Teams (CSIRTs) to rapidly detect, analyze, and reduce cyberattacks. But CIR is not solely a technical process, it is a political tool. How these teams are funded, deployed and integrated into larger security frameworks reveals much about the underlying political motivations and

consequences. This paper explores the political implications of CIR policy in the United States, focusing on the challenges of centralization, bureaucratic performance, human supervision, and international cooperation.

Federal Centralization and Diplomatic Tensions

One of the most prominent political debates surrounding CIR concerns the balance that is between federal agencies and other stakeholders like state governments and private infrastructure owners. Moynihan (2009) explores how crisis response mechanisms such as the Incident Command System (ICS) reflect network governance models, where various actors must coordinate rapidly. In practice, CIR often leads to a centralization of power within federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS). This can possibly lead to diplomatic friction, as state and local governments might feel sidelines or under-informed during federal incidents response efforts. Politicians must handle this tension appropriately, often promoting centralization as necessary for national defense while trying to maintain state autonomy.

Metrics, Performance, and Political Legitimacy

The effectiveness of CIR is constantly assessed through performance metrics. This can include statistics about detection rates, incident response times, and post-incident recover. But these metrics are not neutral. As Sritapan et al. (2011) explain, the creation and presentation of metrics are fundamentally political acts. Lawmakers and agency heads may selectively use metrics to justify budget increases, organizational reforms, or public trust in federal systems. On

the opposite end, poor performance indicators can lead to political backlash, Congressional hearings, or agency restructuring. Therefore, CIR metrics become not only tools for accountability but for political survival and competition among agencies.

Human Decision-Making and Policy Supervision

Even with automation and machine learning advancements, CIR is still heavily dependent on human decision-making. Spring and Illari (2021) display that human analysts play a central role in interpreting cyber incidents, determining how severe they are, and recommending responses. This reliance introduces the potential such things like human error, bias, and inconsistency. Politically, this creates pressure to make sure that CIR teams are properly trained, ethically managed, and held accountable. Some policymakers argue for quick and autonomous response capabilities, while others emphasize transparency and supervision to ensure civil liberties and prevent abuse of power, especially in incidents that involve private-sector data.

Global Cooperation and Strategic Diplomacy

In the context of in international cybersecurity, CSIRTs usually operate as branches within a global information-sharing network. According to Dsouza (2017), their role in cyber diplomacy is increasingly important as cyber threats cross national borders. Political decisions must be made in regard to which countries the U.S. collaborates with, what intelligence is shared, and under what conditions. These decisions are not solely technical, they demonstrate larger geopolitical strategies. For example, partnerships with NATO or Five Eyes countries are politically uncontroversial, but cooperation with nations such as China or Russia raises concerns

of espionage, trust and national sovereignty. Policymakers must weigh national interests against the diplomatic risks of cyber cooperation.

Conclusion

Cybersecurity Incident Response, in particular through the use of CSIRTs is far from just purely a technical policy. It is a politically charged arena shaped by federalism, bureaucratic competition, international diplomacy, and public accountability. The way politicians and policymakers address CIR reveals deeper tensions in American governance. This is shown in security and liberty, efficiency and transparency, and national control versus global cooperation. Recognizing the pollical implications of CIR is necessary for crafty policies that are both effective and democratically legitimate.

References

Dsouza, Z. (2017). Are cyber security incident response teams (CSIRTs) redundant or can they be relevant to international cyber security. *Fed. Comm. LJ*, *69*, 201.

Moynihan, D. P. (2009). The network governance of crisis response: Case studies of incident command systems. *Journal of public administration research and theory*, *19*(4), 895-915.

Spring, J. M., & Illari, P. (2021). Review of human decision-making during computer security incident analysis. *Digital Threats: Research and Practice*, *2*(2), 1-47.

Sritapan, V., Stewart, W., Zhu, J., & Rohm Jr, C. E. (2011). Developing a metrics framework for the federal government in computer security incident response. *Communications of the IIMA*, *11*(3), 5.