Social Implications of the Active Cyber Defense Certainty Act

Gavin L Williams

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Bora Aslan

4/14/2024

Social Implications

The ACDC Act amends the Computer Fraud and Abuse Act, allowing cyberattack victims to attack back, signifying a shift towards active defense in cybersecurity. However, this development has significant social implications. Primarily, it challenges existing privacy norms by allowing entities to "hack back," potentially leading to increased digital surveillance and intrusion. The normalization of active defense measures could transform cybersecurity into a shared responsibility, creating a societal shift toward increased digital awareness. Patrick Neal (2019) mentions that “corporate decision-makers’ still believe there is a social contract based on the notion that information affects the safety and security of society” (Neal, 2019, p. 17). This implies that there is a perceived obligation among corporate leaders to protect information, not just for their own interests but as a societal responsibility.

Leading Social Factors

The growing complexity and number of cyber threats highlight the critical need for the ACDCA. The history of cyberattacks shows that traditional defense methods are becoming inadequate, resulting in the need for a shift in cybersecurity practices and legal measures. Furthermore, significant cyber incidents have raised public concern and made cybersecurity a key issue in political discussions, stressing the urgency for enhanced protection. As our lives increasingly rely on digital processes, the need for a solid legal framework to protect these digital environments becomes more apparent, making the case for the importance of the ACDCA even stronger.

Social Consequences

The ACDCA effects extend beyond just policy, influencing individual behavior and societal values. It introduces the concept of legally responding to cyber threats with active

defense, which could lead to a societal shift in how we view cybersecurity. People might start to see a more vigilant, even aggressive, approach as necessary. This change could influence how online communities interact, with increased security measures potentially affecting the level of trust and openness that we see online. Additionally, there are broader social implications regarding digital trust and ethics. Some argue that active defense strategies should be a last resort in the realm of digital security. Jay Kesan and Carol Hayes (2010) explain that the "three primary methods for addressing cyber intrusions (criminal sanctions, litigation, and purely defensive remedies), thus must all be found to be unavailable, impractical, or ineffective in order for active defense to be the socially optimal solution" (Kesan and Carol, 2010, p. 329). Additionally, active security measures can undermine a person's freedom of privacy. Thus, it is crucial that we reevaluate how we balance the need to defend against cyber threats with the demand to maintain digital privacy and freedom.

Cultural and Subcultural Influences

The creation of the ACDCA is strongly shaped by the digital culture, which prioritizes being open, working together, and innovating. This act brings many cultural improvements, for example, Anthony Glosson (2015) mentions how "placing the burden of identifying and deterring attackers entirely on law enforcement, therefore, "inefficiently stretch[es] government resources"" (Glosson, 2015, p. 15). Therefore, by allowing private companies greater ability to deter attackers it could alleviate some of the responsibilities of law enforcement and other sectors. However, the act has sparked a range of responses from various groups, showing different views on cybersecurity, digital rights, and privacy. Tech activists and cybersecurity companies have particularly contrasting opinions, showing the complicated balance between the need for security and the importance of freedom and privacy. Furthermore, the societal values

surrounding privacy and security significantly influence the acceptance and implementation of policies, highlighting the complex relationship between social norms and cybersecurity regulations.

Conclusion

The Active Cyber Defense Certainty Act marks a pivotal point where cybersecurity collides with societal values, touching on the complex relationship between privacy, security, and social norms. Its impact extends far beyond just cybersecurity, influencing our views on privacy, our level of alertness online, and the balance of power in the digital world. This policy plays an important role in shaping the digital aspect of our society. It encourages us to consider how to balance technological advancement with the preservation of social well-being, emphasizing the need for a thoughtful approach to cybersecurity that respects fundamental values such as privacy and freedom.

Citations

Glosson, A. (2015). Active defense: An overview of the debate and a way forward. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191394. Accessed 4/6/2024.

Kesan, J. P., & Hayes, C. M. (2010, October). Thinking through active defense in cyberspace. In *Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options* (pp. 327-342). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691207. Accessed 4/6/2024.

Neal, P. (2019). *Protecting the information society: Exploring corporate decision makers' attitudes towards active cyber defense as an online deterrence option* (Doctoral dissertation, Royal Roads University (Canada)). https://www.proquest.com/openview/a8a97535665c999c31d4b0b55958ecaf/1?pq-origsite=gscholar&cbl=18750&diss=y. Accessed 4/5/2024.