Political Implications of the Active Cyber Defense Certainty Act

Gavin L Williams

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Bora Aslan

3/3/2024

Political Overview

The political implications of the Active Cyber Defense Certainty Act (ACDCA) are complex and have stirred considerable debate among lawmakers and cybersecurity experts. Robert Andrea (2020) states that "the ACDCA aims to allow private entities that are victims of computer network attacks to take defensive cyber measures against their attackers, a concept referred to as "hacking back." Although it represents a novel approach to a complicated issue, ambiguities in the ACDCA could create additional complications" (Andrea, 2020, p. 2). While offensive cyber strategies may be the future of cybersecurity, there is concern that it could lead to a rise in offensive cyber operations that are difficult to control, potentially causing harm to innocent third parties and escalating into international cyber conflicts. Additionally, there is concern that the ACDCA might undermine efforts to establish global norms against aggressive cyber activities, as it could be seen as justifying such behavior. Thus, while the ACDCA is intended to strengthen cyber defense capabilities, its political implications are commonly questioned for concern.

Tom Graves and Krysten Sinema Introduction of the ACDCA

Chris Cook (2018), attorney at the U.S. Department of Justice, states that representatives Tom Graves and Krysten Sinema introduced the ACDCA as a bipartisan bill, "The proposal would allow private companies (and individuals) to go into foreign networks to gather intelligence and do research on unauthorized intruders and determine who is responsible and how the penetration occurred" (Cook, 2018, p. 207). They argued that the bill was necessary, stating that technology has surpassed public policy, and that the laws need to catch up. The ACDCA seeks to make significant updates to the Computer Fraud and Abuse Act to allow the use of limited defensive measures that extend outside of one's network to monitor, identify, and

stop attackers. Representatives Graves and Sinema have stressed the critical need for laws that allow for cyber retaliation as a defense and deterrence strategy. They believe current defensive tactics are outdated against the advanced cyber threats we face today. By supporting the ACDCA, they argue that it enables companies to more effectively counter cyber-attacks and enhances overall national cybersecurity by allowing them to track and analyze the methods used by these criminals. This shift towards offensive cyber strategies is a significant change and has raised extensive discussions among experts in cybersecurity.

Andrea Little Limbago's view on the ACDCA

Cook (2018) mentions how Andrea Little Limbago, "the chief social scientist at the cybersecurity firm Endgame" (Cook, 2018, p. 218), Limbago's analysis contributes to the policy discussion around the ACDCA. She raised concerns that by including the word "intentionally" in the ACDCA, "by adding this layer of assurance, the drafters have actually expanded the scope of what a defender can do on an attacker's network" (Cook, 2018, p. 218). This could possibly lead to more aggressive actions and increase the chances for escalation. This highlights the delicate balance and attention to detail these policymakers must make when enabling these defense mechanisms to prevent unintended consequences.

James Lewis view on the ACDCA

James Lewis at the Center for Strategic and International Studies has voiced opposition to "hacking back" and aggressive cybersecurity measures. Dennis Broeders (2021) writes that Lewis "calls hacking back 'a remarkably bad idea that would harm the national interest'. Moreover, he says that 'encouraging corporations' to compete with the Russian mafia or Chinese military hackers to see 'who can go further in violating the law, is not a contest American companies can win" (Broeders, 2012, p. 4). He argues that encouraging such practices could

harm national interests and put American companies at a disadvantage in a legal contest against foreign cyber adversaries. Moreover, he points out that if the U.S. were to be openly accepting of hacking back, it might undermine efforts to establish international norms against unauthorized hacking, potentially changing the rules of the cyber battlefield in undesirable ways.

Conclusion

In conclusion, the Active Cyber Defense Certainty Act marks a pivotal moment in cybersecurity legislation, reflecting a significant shift towards empowering private entities with offensive cyber practices. While the intentions behind the ACDCA are to strengthen the cyber defenses of businesses and individuals against ever increasing cyber threats, the act raises critical discussions regarding the balance between offensive capabilities and legal constraints, the potential for international conflict, and the compliance to global cyber norms. This act continues to be a topic of intense discussion among specialists, decision-makers, and legal experts. Some advocate for its necessity, some request a note of caution, and others oppose it entirely due to the potential for harm. However, the success of the ACDCA will ultimately depend on how it is applied and how the landscape of cybersecurity will evolve in the future.

Citations

Andrea, R. (2020). Hackback to the Drawing Board: Ambiguity and Risk in the Active Cyber Defense Certainty Act. In *Boston College Intellectual Property and Technology Forum* (Vol. 2020, pp. 1-10). https://lira.bc.edu/files/pdf?fileid=fa2a36da-090f-4436-a271-5be1411b9967. Accessed 3/1/2024.

Cook, C. (2018). Cross-border data access and active cyber defense: Assessing legislative options for a new international cybersecurity rulebook. *Stan. L. & Pol'y Rev.*, *29*, 205. https://law.stanford.edu/wp-content/uploads/2018/08/SLPR_Cook.pdf. Accessed 3/1/2024.

Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line?. *Journal of Cybersecurity*, *7*(1), tyab010. https://academic.oup.com/cybersecurity/article/7/1/tyab010/6199903. Accessed 3/2/2024.