Understanding the Active Cyber Defense Certainty Act: A Simplified Overview

Gavin L Williams

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Bora Aslan

2/11/2024

Introduction

In today's digital age, cyber threats are a growing concern for everyone. To address this, the United States proposed a law in 2017 called the Active Cyber Defense Certainty Act (ACDC), also known as the "hack back" law. This paper aims to explain the ACDC in simple terms, discussing why it was needed, what it does, and how it fits into the bigger picture of keeping our digital world safe.

What is the ACDC Act?

As described by Andrea (2020), "The ACDC Act proposes to amend the Computer Fraud and Abuse Act of 1986 (CFAA), a foundational United States cybersecurity law" (p. 3), which makes it illegal to access computers and networks without permission. "The main purpose of the ACDC is to exclude private entities that defend against cyberattacks by 'hacking back' against attackers from criminal liability under the CFAA" (Andrea, 2020, p. 3). The ACDC aims to enable people and companies that have been attacked to fight back. They can use certain techniques to track down the attackers, stop the attack, get back or delete stolen data, and watch what the attacker is doing. Before the ACDC, doing these things would have been illegal.

Why Was the ACDC Developed?

Cyberattacks are becoming more common and sophisticated, making traditional defenses like firewalls and antivirus programs not enough. The ACDC was introduced to give victims more power to defend themselves. By allowing victims to act against their attackers, the law aims to make cybercrime riskier for criminals and reduce the number of attacks.

How Does the ACDC Work?

According to Barnes (2018) in summary, under the ACDC "all active defense measures must be notified to the FBI" (p. 10). They are limited in what they can do: they cannot harm innocent people, steal data, or cause widespread disruption. The idea is to make sure that in trying to defend themselves, victims do not accidentally become attackers or cause collateral damage. After receiving confirmation from the FBI, those who wish to "hack back" are permitted to trace attacks, disrupt them, and recover or delete stolen data, but must avoid harming others, theft, or excessive disruption. These rules aim to prevent

retaliatory actions from escalating or breaking laws, requiring that defensive measures are directly related to the threat and proportionate in response (Barnes 2018, p. 10).

The ACDC in the Bigger Picture

The ACDC is part of a larger effort to improve cybersecurity in the U.S. It complements other laws and policies focused on preventing, detecting, and responding to cyber threats. The introduction of the ACDC act encourages a shift from reactive to proactive cybersecurity strategies. On an international level, the ACDC brings up questions about how countries should act in cyberspace, especially since it involves going beyond one's digital borders. This means the U.S. needs to be careful to avoid breaking international laws or causing international disputes.

Challenges and Concerns

Despite its good intentions, the ACDC has its concerns. According to Andrea (2020), "The main problem with the ACDCA is that it is ambiguous as to when a defender would be justified in using ACDMs against an attack" (p. 5). The ACDC only permits the use of ACDMs, active cyber defense measures, when the victim is the target of "persistent unauthorized intrusions", however the bill fails to define what is considered "persistent" or even what is considered an "intrusion" (Andrea, 2020, p. 5). According to Elliott (2018), the main argument suggests that hacking back could lead to more cyber conflicts or harm to innocent third parties if not used carefully. Others argue that focusing on defensive technology and international cooperation might be a better approach to fighting cybercrime. One of the most significant challenges in cyber defense is accurately identifying the attacker. Given attackers' skill in masking their identities, victims face the risk of mistakenly targeting innocent parties. By legalizing active defense measures, there's a concern that the ACDC could lead to an increase in cyber conflicts. Attackers may respond to "hack back" actions with even more severe attacks, leading to an "eye for an eye" scenario. (Elliott, 2018, pp. 1-3). With this act, there is a fine line between enabling self-defense in cyberspace and creating a cycle of retaliation.

Conclusion

The Active Cyber Defense Certainty Act is an innovative step towards empowering victims of cyberattacks. It offers a way to not just defend but also fight back against cyber threats, within certain legal boundaries. However, its success requires careful implementation and ongoing evaluation to ensure it adds positively to our overall cybersecurity efforts. As the digital landscape evolves, so will our strategies for protecting it, highlighting the need for continuous adaptation and cooperation on a national and international level. This proactive and collaborative approach is essential for a more secure and promising digital 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 2/8/2024.

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 2/9/2024.

Elliott, K. A. (2018). *Active Cyber Defense and Attribution in Cyber Attacks* (Doctoral dissertation, Utica College). https://www.proquest.com/openview/c4ad5003f5c82aa513bb250efaa4dcb1/1?pq-origsite=gscholar&cbl=18750. Accessed 2/9/2024.