Ethical Implications of the Active Cyber Defense Certainty Act

Gavin L Williams

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Bora Aslan

3/31/2024

Introduction

The Active Cyber Defense Certainty Act (ACDCA) represents a significant shift in cybersecurity legislation, proposing to allow private entities more options in defending against cyber threats. The main ethical concerns of this policy are complex, covering both the chance for better security and the risks of overreach or causing unexpected consequences. Allen Zhou (2018) explains that, with the introduction of the "Active Cyber Defense Certainty Act (AC/DC Act) which would allow victims of cyber attacks to execute vigilante justice" these attacks "If legalized, it is not hard to imagine how the lines for what constitutes a cyberattack and what counts as reasonable retribution becoming blurred" (Zhou, 2018, p. 4).

Ethical Implications

The ethical implications of the ACDCA are complex and diverse. On one hand, it acknowledges the evolving nature of cyber threats and the necessity for stronger defense mechanisms. Under this act, companies would have the power to track, identify, and mitigate threats in a proactive manner. This capability, however, introduces significant ethical concerns. The act of pursuing threats beyond one's network involves the risk of intruding on the privacy and rights of individuals, potentially escalating cyber conflicts and setting examples for digital vigilantism. Georg A Thomas (2017) explains that "While it is true that the act of attacking an organisation or individual with malicious intent in the first place is not ethical, simply attacking back in self-defence may also not be ethical" (Thomas, 2017 p. 2). These actions also raise questions about accountability and the potential for misuse of power. While many argue that the ACDCA is an unethical approach to bettering cybersecurity. A study conducted by Kim Withers et al. (2020) showed that "the majority do not find it unethical to "hack back" adversaries in

nation-states and that private companies should be given the right to retaliate without prosecution" (Withers et al. 2020, p. 1819).

Cost and Benefits

The ACDCA offers real benefits, primarily by boosting our cybersecurity defenses and deterring would be attackers with the prospect of proactive pursuit. These efforts could notably reduce the occurrence of successful cyber-attacks. However, the associated costs of these benefits warrant careful consideration. There is a risk of misuse, an escalation of cyber conflicts into more serious confrontations, and concerns over privacy and civil liberties that present significant obstacles. Additionally, the implementation of the act might unintentionally affect innocent parties and could be exploited for malicious objectives.

Rights Protection and Limitation

The ACDCA aims to protect the right of entities to defend their networks and data. This right is crucial in an era where digital assets are integral to the functioning of society. Thomas (2017) writes that, "In the context of governments hacking back (or initiating an attack) it can be argued that this is ethical because a government is using the approach to defend the people it represents, often in the millions" (Thomas, 2017, p.2). However, the act's approach to defending these rights potentially infringes upon other fundamental rights, particularly privacy. The actions authorized by the ACDCA could lead to surveillance and data collection practices that affect individuals not directly involved in these cyber threats.

Individual's Rights

In the ACDCA, establishing a balance between boosting defense capabilities and preserving individual rights is challenging. The act tends to prioritize offensive strategies without adequate measures to prevent excesses. Addressing this issue requires the introduction of firm

oversight, clear transparency requirements, and specific limits on active defense actions is crucial. By implementing these adjustments, it would be possible to ensure that these actions will not compromise personal freedoms and rights.

Conclusion

The Active Cyber Defense Certainty Act introduces a significant evolution in cybersecurity policy, aimed at enabling more proactive defenses against cyber threats. While the benefits of this act are clear, such as enhanced security and the potential deterrence of cybercrime, the ethical and rights related implications present substantial challenges. Balancing the empowerment of entities to defend themselves with the protection of individual rights and privacy requires careful consideration and well-designed implementation. Ultimately, the ACDCA's success will depend on its ability to enhance cybersecurity ethically while safeguarding individual freedoms. Moving forward, it is essential that this act’s framework is regularly reviewed and updated with emerging technological trends and ethical concerns.

Citations

Thomas, G. (2017, October). On the offensive: is ‘hacking back’ethical?. In *Higher Degree by Research Symposium*. https://www.researchgate.net/profile/Georg-Thomas-2/publication/320445115_On_the_offensive_is_'hacking_back'_ethical/links/5ac1ccf045851584fa75acb2/On-the-offensive-is-hacking-back-ethical.pdf. Accessed 3/29/2024.

Zhou, A. (2018). Bringing the Fight to Them. https://www.cs.tufts.edu/comp/116/archive/spring2018/azhou.pdf. Accessed 3/29/2024.

Withers, K., Parrish, J., Ellis, T., & Smith, J. (2020). Vice or virtue? exploring the dichotomy of an offensive security engineer and government “hack back” policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1813–1822. https://doi.org/10.24251/hicss.2020.224. Accessed 3/30/2024.