Digital Self-Defense Standpoints:
Societal Impacts on Hacking-Back

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Bora Aslan

14 April 2024

What are the social implications of hacking-back?

Throughout the series of these papers regarding hacking back the definition, political, and ethical implications have been discussed. All these factors have played a part in the implementation of hacking-back for public use. By allowing this policy to be implemented for everyday use, the risk of normalization occurs. Utilizing the hacking back for everyday use can normalize offensive tactics and promote the wrong behavior online. This can lead to escalation or potential geographical issues with other countries or nations. Initiatives may contribute to a cyber arms race per se as adversaries attempt offensive and defensive capabilities to outmaneuver each other. This arms race could divert resources away from proactive cyber defense measures and provoke a cyber war.

How did public factors affect the current legality of hacking-back?

The public's awareness and concerns regarding this policy influenced advocates, policymakers, international discussions, and more. Officials were forced to address the issue due to increased talk and awareness, as well as increased public pressure. Advocacy groups and cybersecurity professionals pressured for actions and decisions to be made due to the tremendous effect it could have on the US with no regulation. These groups advocated for clear legal frameworks that define the parameters of allowed cyber defense measures, balancing the need for self-defense with the risks of escalation and unintended consequences.

What are the potential consequences for the community?

The major complications stay the same, no matter the view on the topic. The lack of trust in law enforcement, along with the escalation, can cause more harm than good. Additionally,

hacking-back initiatives may circumvent legal channels and undermine due process, raising questions about fairness and accountability. Ethical concerns do vary even among policymakers, as some oppose and some support. However, the decision at this time was to ban cyber self-defense unless it is for government use due to the potential crossfire it may put others in. Legalizing hacking back could escalate cyber conflicts as individuals and organizations retaliate against attackers.

Authors Reflection

This author believes that while it may feel good to stand up for oneself there is currently no way to safely do so. With no frameworks and regulations regarding safety measures, it can cause more panic. By implementing this policy in its current state, the US opens itself up for more vulnerabilities which can allow more attacks to occur. While the urge to retaliate against threats is understandable, the lack of frameworks and regulations for safe and responsible cyber defense measures renders such actions unrealistic currently. Instead, the focus should be on developing comprehensive strategies that prioritize the prevention and detection of cyber threats while focusing on transparency, accountability, and international cooperation.

References:

Berinato, S. (2022, November 8). *Active defense and "Hacking back": a primer*. Harvard Business Review. https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer

Hack-Back: Toward a legal framework for cyber Self-Defense. (2020, June 26). American University. https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm

Hardik Gandhi, Note, *Active Cyber Defense Certainty: A Digital Self-Defense in the Modern Age,* 43 Okla. City U. L. Rev. 279 (2019)

Porch, A. M. (n.d.). *Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act*. USD RED. https://red.library.usd.edu/sdlrev/vol65/iss3/6/?utm_source=red.library.usd.edu%2Fsdlrev%2Fvol65%2Fiss3%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages

School, S. L. (2018, June 1). *Cross-Border Data Access and Active Cyber Defense: Assessing legislative options for a new International Cybersecurity Rulebook | Stanford Law School*. Stanford Law School. https://law.stanford.edu/publications/cross-border-data-access-and-active-cyber-defense-assessing-legislative-options-for-a-new-international-cybersecurity-rulebook/

View of Legal Framework of Right of Self Defense in Cyber Warfare: Application through Laws of Armed Conflict. (n.d.). https://www.ojs.jdss.org.pk/journal/article/view/189/107