Digital Self-Defense:

Hack-Backing

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Bora Aslan

11 February 2024

Hack-Backing Definition

As cybercrime rises, there has been interest and attempts to show digital self-defense or hack-backing, where the victims hack back the attacker. Cybercrimes have been on the rise as technology evolves and becomes more dependent on our everyday lives. There are many ways people have approached cyber-related activities, such as defense, mitigation, and risk analysis. Cyber self-defense is the same as in the physical world, where there are multiple reasons one does it.

Development

Hack-backing was developed due to the rise in cyber threats. Cyberthreats can include, but are not limited to, malware, persistent threats, ransomware, etc. With the increase in technological advancement, the methods people and organizations use have evolved to prevent, detect, and react to threats. The NIST Cybersecurity Framework has guided best practices and standards related to cyber defense. The increased awareness of cyber threats also played a part. Strong passwords, cyber hygiene practices, awareness training, and consistent software updates have all played a part in encouraging people to be proactive in protecting themselves.

Scientific Policies

To advance scientific policies, research and development are completed, which requires support and funding. This takes a step forward to advance the technology and techniques used. This research and development can lead to partnerships between agencies and universities meant to modernize self-defense abilities. The treaty can bring people together to share this data and encourage collaboration. This collaboration entails researching research data, best practices, and threats over platforms while also coordinating projects. Lastly, these policies may involve cyber

requirements and standards for research, especially for confidential or sensitive information. Compliance helps with the security of the data.

National Policy Incorporation

Self-defense is essential for national cybersecurity strategies to manage cybersecurity risk and protection. This includes defensive actions, discouraging strategies, and cooperation to highlight durability and stop attacks. The frameworks involve the development and maintenance of defense capabilities, which involve threat intelligence, incident response, and workforce development. Partnerships can be created to strengthen defense by using the resources and strengths of all parties involved. These partnerships supplement sharing, analysis, and grouped responses. These efforts are not stationary but can be used internationally. This encourages stability, trust, and more partnerships. Treaties and agreements have been made to combat common goals such as threats and amplify defenses and cyber hygiene.

Reasons for Hack-Backing

Frustration with law enforcement can occur not only in the cyber world but in the physical world as well. Slow responses or not knowing what is being done behind the scenes can cause irritability and a lack of trust, making others want to take matters into their own hands. There are many speculations about the effectiveness of the justice system. This appears due to the lack of resources they tend to have and the lack of communication and support that comes across involving crimes, and not a lot of information is typically revealed.

Some take cyberattacks personally, making them want to seek revenge. This can apply to wanting them to experience the same as what they have gone through. A sense of control consumes people, making them helpful, which is not a feeling many can handle. Due to many

employers' policies, employees take it upon themselves to defend against threats, as many fear the repercussions that can be involved. On the same basis, many victims want to find the perpetrators and bring them to justice themselves, like vigilantes. Victims will feel a sense of righteousness and do not always understand the laws and regulations, resulting in this decision being unethical and possibly illegal in some places.

Summary

Overall, this policy has been developed to beat cyberattacks and increase advancements. There are a range of strategies, solutions, education and awareness, and best hygiene practices. This method plays a crucial role in protecting assets and upholding the CIA Triad of confidentiality, integrity, and availability, while also encouraging stability and protection. The lack of trust in solutions underlines the significance of improvement, education, and clarity in the field. By addressing the issues, the distrust and effectiveness of solutions can rebuild trust and protect against emerging threats.

References

Kesan, Jay P, and Ruperto P Majuca. "Hacking Back: Optimal Use of Self-Defense in Cyberspace - OII." *University of Oxford*, 2005, www.oii.ox.ac.uk/wp-content/uploads/old-docs/jay_kesan.pdf.

Martens, Philippe. "Self-Defence in Cyberspace: Hacking Back the Hacker." *Tilburg University*, Jan. 2021, arno.uvt.nl/show.cgi?fid=155524.

"NIST Cybersecurity Framework." *NIST*, 20 Sept. 2022, www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0.

Waxman, Matthew C. "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions." *Columbia Law School*, 2013, scholarship.law.columbia.edu/faculty_scholarship/845/.

Winstead*, Nicholas. "Hack-Back: Toward a Legal Framework for Cyber Self-Defense." *American University*, 26 June 2020, www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.