Digital Self-Defense Principles:

Ethics Regarding Hacking-Back

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Bora Aslan

31 March 2024

What are the ethical implications of hacking-back?

There are multiple concerns regarding hacking back that range from beneficial to dangerous, as even ethical hacking has mixed perspectives. One obvious point is based on others who believe they have the right to defend themselves. No one likes feeling defenseless, and with such sensitive information on the line, it is natural to want to fight back or stand up. This can lead to more dangerous complications, as mentioned in the previous papers. In one of these other entries, another concern was regarding never fully knowing who is on the other side and risking the harm of innocents. However, to expand on this, while there is a rightful concern about others being affected, the other consideration is the fear of the unknown. Unlike a physical alteration, you cannot see who the offender is and are unsure what other resources are at their disposal. The last major implication is the debate on whether hacking back is beneficial, as it is still undetermined since it was mentioned in early 2010.

What are the costs and benefits for societal groups?

One benefit has already been discussed which is the belief of self-defense. Along the same lines, it is assumed that hacking back the offenders can result in the minimization of future attacks. It is believed that showcasing one's abilities will make the threats reconsider while improving their public reputation as it can show clients good faith and strong defenses. However, If a business fails to stop the defense or harms others in the process it can have a great impact on the reputation and instead of glowing reviews, legal repercussions can be involved. While the benefits do seem tempting, they can also be seen as threatening or challenging which in turn can encourage hackers to defeat or ruin the reputation if ever succeeded. Lastly, the steps taken to defeat the offender can accidentally expose more vulnerabilities not just for the organization, but in others as well. If the vulnerability lies within a particular virus protection software, for example, any other company using the virus protection may become a new target.

How does this prohibit or benefit individual rights?

Legislation plays a majority in the decision regarding the topic of cyber self-defense. While individuals have the right to ensure their security others have the right to freely express themselves. Cyber self-defense is not limited to ongoing threats. If implemented it can be directed towards individuals freely expressing their voice which an organization may take as a threat without an actual attempt. Not only does this apply to the right to expression but can also apply to opposing political views or discriminatory reasoning. Even if an attack is made, in the US there is a right to privacy no matter if provoked. A company implementing self-defense may only attempt to target the information stolen or identify the offender, but in technical aspects, it is an invasion of privacy as well as if any information not relating to the threat is found.

Authors Reflection

In this author's opinion, cyber-self-defense is very useful and can be very beneficial to society. However, due to the lack of guidance or rules regarding this, it is unsafe to be used at this time. Support is given to those whose reasoning is to stand up for themselves and what they believe in. The lack of regulations regarding this topic due to such a debate still ongoing it is not safe to be implemented at this time. With no framework built on this, it is dangerous due to the multiple implications reflected in the cost-benefit analysis completed. In this current environment it is unsafe for everyday use and at this time can cause more harm than good. This does not imply that hacking-back should never be permitted but instead means that when the correct guidance or framework is completed along with restrictions in place this author will fully support the decision. Hacking overall can be a dangerous line as many individual rights can be violated, but if it includes personal feelings, there may be greater room for error which can affect the county altogether.

References:

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/

Johansen, R. (2023, October 13). *Ethical Hacking Code of Ethics: Security, risk & issues*. Panmore Institute. https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

Lin, P. (2024). Ethics of Hacking Back: Six arguments From armed conflict to Zombies. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4682398

Politics, G. B. F. N. (2016, September 26). Hacking back is ethical in the cyber frontier. *Council on Foreign Relations*. https://www.cfr.org/blog/hacking-back-ethical-cyber-frontier

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/