Digital Self-Defense Implications:

Political Views on Hacking-Back

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Bora Aslan

03 March 2024

What are the concerns or implications of hacking-back?

There are concerns regarding hacking, ranging from ethical to political to social. These different concerns all play a part in the use and implementation of this technique. Supporters argue that it is necessary to defend and deter future attacks. They believe that showing strength and disrupting their goal will show that the U.S. is not weak and limit the threats that can occur moving forward. However, opponents of this technique believe it will encourage attackers as it will be seen as a challenge. Politicians believe it could break domestic and international laws. Also, discovering the specific hacker can prove difficult, and without certainty, innocent people can be affected instead of the guilty party.

How have the politicians approached this topic?

In an article written by Nicholas Winstead, he makes a comparison between cybercrime and shoplifting. In certain stores, you can tackle the thief or grab the items being stolen before they have left the store (Winstead, 2020). Cybercrime does not allow this to happen in similar situations that translate online. The Active Cyber Defense Certainty (ACDC) bill proposed by representatives Tom Graves from Georgia and Kyrsten Sinema from Arizona stated that companies could engage in “active defense,” enabling them to gain authorized access to stop the attack (Berinato, 2022). Among debates by representatives in 2018 regarding this proposed bill, Senator Whitehouse of Rhode Island stated that a test will be implemented against the NIST framework to enhance results on how to move forward regarding cybersecurity (Beavers, 2018).

What is the outcome of the verdict?

Hacking back is still under debate to this day. Generally, it is frowned upon, and unless it is authorized, it is illegal. The primary law, “The Computer Fraud and Abuse Act (CFAA),” governs computer crimes in the U.S. Authorizing access to another's computer is illegal without prior permission. This concept applies even in response to a cyberattack. However, clear legal guidelines have not been released, allowing room for debates and disagreements both locally and internationally. In January 2024 alone, there have been six known substantial breaches, according to the Center for Strategic and International Studies.

How did the policymakers arrive at the decision?

Many reasons resulted in the veto of the ACDC bill and the illegality of cyber self-defense. Governor Nathan Dela from Georgia stated that this bill would spread the technique to where it cannot be contained as every company will begin to participate. There are no proper guidelines as to where this technique could be used for competition and could become exploited (Beavers, 2018). The opposing views brought more compelling deterrence from enabling cyber self-defense throughout the country. The fear of many attempting to become vigilantes without the proper training and innocent people being affected became too grave. Lastly, international laws being broken can cause more harm than a cyberattack if the nation attacked believes the error is too grave. The one company attempting to approach this will not be the main target if this occurs; the United States will be.

What does this mean for the public?

Overall, hacking-back has not been legalized, as there are guidelines made for public use. This approach can have serious consequences that would not just affect one person or company, making the risk too high to move forward at this time. Compared to the shoplifting similarity mentioned above, not all companies employ this. Some organizations believe in not letting workers get involved due to the possibility of harm. This does not mean that cyber self-defense will be forbidden forever, but that careful consideration must take place first and a framework must be built before allowing public access.

References:

Beavers, O. (2018, August 21). The Hill. *The Hill*. https://thehill.com/policy/cybersecurity/402807-dem-senator-to-propose-congress-should-consider-allowing-companies-to/

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

Giles, M. (2020, April 2). Five reasons "hacking back" is a recipe for cybersecurity chaos. *MIT Technology Review*. https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/

Messerschmidt, J. E. (n.d.). *Hackback: Permitting retaliatory hacking by Non-State actors as proportionate countermeasures to transboundary cyberharm*. Scholarship Archive. https://scholarship.law.columbia.edu/national_security_law/5/

Nobles, C. N. (2023). A scoping review of hacking back in cybersecurity. *ResearchGate*. https://www.researchgate.net/publication/372935724_A_Scoping_Review_of_Hacking_Back_in_Cybersecurity

Significant Cyber Incidents | CSIS. (n.d.). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

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