Digital Self-defense: The Future Cybersecurity Problem

Giao Dinh

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Lora Pitman

December 7th,2020

As trying to deal with the existing cybersecurity problems, there are unexpected new growth issues due to the improvement of advanced technology systems growth worldwide. Suffering, afraid, and worry are common words used to characterize how was the victim or the target felt in the past. The flow of protecting oneself from cyber attacks continues when the victims or targets want to protect themself as a way to gain their rights over attackers. Although the idea of fighting back the unknown attackers via the digital world is worse in cybersecurity, it is still existing and achieves waves until now. However, some restrictions apply when applying it in reality due to the new update Active Cyber Defense Certainty (ACDC) Act to the Computer Fraud and Abuse Act (CFAA). Back to the existing problems, there are hundreds of thousands or more than millions of cases of device vulnerabilities associated with hacking: phishing, malware, ransomware, spoofing, encryption, adware, brute force attack, and something else. The targets usually are government officials, businessmen, entrepreneurs, but they also focus on the coronavirus and its vaccine. From 2017 to 2018, the expansion of ransomware increasing widespread over, which United Stated has detected attackers for nine percent (Herrera Silva et al., 2019). Besides, in April 2018, there was an attack on TaskRabbit and affected more than three million users of this website because their information was scooped. The hackers were using AI as a method to control the huge botnet of performing distributed denial-of-service (DDoS) attack on the website servers (Bocetta, 2020). However, this is also one of the existing and a warning to the human future on the growth of Cybercrime into the artificial intelligence world, which has a tremendous potential to evolve to computer security in unexpected ways.

Digital self-defense also knowns as a different way to name hacking back. Hacking back is how the target or the victim is tracing back the attacker's IP who hacked their devices and attacked them. Reason for all because they want to take revenge on the attackers by their skills

programming or asking for help from one who knows about it. According to McGuigan (2019), the victim will strike back precisely the target and causes enough damage to retrieving the stolen information that essential and sensitive. Besides, this is also the way to gather evidence and destroy the stolen or compromised data or files. Under the Active Cyber Defense Certainty Act, which can notice as a hacking back bill, there is a change to the Computer Fraud and Abuse Act (CFAA) on how the victim reasonable to hunting the attackers back as following ACDC Act's key provisions to legally hacking back, but the victim needs to notify the FBI and get the notification acknowledgment before doing this (Susssman, 2019; McKenna, 2019). Meanwhile, the Active Cyber Defense Certainty Act also specifies reasons why the victim actions should be allowed to tracing the attacker as the following: prove the attribution of an attack, disrupt the attack but not damage other's computers, and detector the attacker's behavior (Sussman, 2019; Active Cyber Defense Certainty Act, 2019). It also means the victim or defender cannot use the bill as an excuse to take an act of revenge on the other's computer to disrupting, damaging, or destroying the attackers' network, data do not belong to victims, and computers but also including any causing physical injury or financial loss (Active Cyber Defense Certainty Act, 2019).

As mentioning earlier, the Active Cyber Defense Certainty Act is seen as hacking back bill which enhances cyber investigating, identify attribution, and authorized to access data from systems over the sea but does not violate the United States Code or other law and international treaties (Cook, 2018; Active Cyber Defense Certainty Act, 2019). It also means creating more opportunities to purify the manual and more directions when evolving into defending systems and cyber technology. Therefore, hacking back is no longer prohibited but legal as long as the actor does not violate the law. The actors will be engaged in this policy are the private sector

(United States business and companies), citizen, and the nation-state. The private sector actors will keep their customers and other essential data secure from any unexpected attack by unauthorized IP addresses, United States residents, or foreigners. To tracing the attackers or hackers, both citizens and the United States businesses must have to "report the crime to law enforcement" first and attempt to improve their defensive measures that according to ACDC Act if they are the victimized (Active Cyber Defense Certainty Act, 2019). Cybercriminals develop their skills and new tactics to monetizing by their criminal acts due to the absence of the current law for defenders' cyber tools and methods. Therefore, the actors who are cyber defenders must be qualified and extremely cautious when performing cyber defense techniques and avoid any damages as the result of failing. If the actors who responsible for performing cyber defense techniques to hacking back which do not qualify as stated by ACDC Act, they will be sanction depends on how much damages they made. This policy going to affecting the victims act as the cyber defenders on the defensive measure to who qualified to hack back the attackers or hackers for causing any damages or monetizing from stolen data. It will impact only on the U.S citizens and residents who perform cyber defense techniques but also legally allow them to trace back the attackers over the sea-based on the Active Cyber Defense Certainty Act. According to Chris Cook (2018), international law is only or mostly focus on nation-states, which talking about the nations' rights to self-defense but not private actors. Hence, this policy also has some limitations due to international law.

In the case of running this policy, the funding will be costly to implement due to the rising of cyber attacks recently during the impacts of the Covid-19 pandemic. According to the Kaspersky statistics website, the United States is listing in the fourth rank of the most nation cyber attacked recently per second. There are other nations also facing with breaching

information and monetizing from stolen data by hackers crossing overseas. For instance, Vietnam also is listing in the ninth rank, in which most cases of cyber-attack are about hacking Facebook accounts. According to Gandhi (2019), there are about one and half million cyberattacks yearly with totaling four thousand per day. This also shows there are more efforts need to improve for this policy sides with the Active Cyber Defense Certainty Act but also preventing any mistaken or unexpected damages causing by unqualified cyber defenders. This policy also has sanctioned for violating the policy and damaging other's computer as the result causing any loss or creating more advances for the attackers in the future. For any involvement, the consequences will bring more effects on financial solvency in private sectors (Martinez, 2020). Back to why the policy is costly to implement, the DOD reported US had spent $8.5 billion in FY 2019 funding on the cyber attacks, which increasing 4.2 percent above the fiscal year (FY) 2018 (AP 21, 2018). This also explains how this policy will be costly in the case it is subsidized by the federal budget.

In conclusion, there are more efforts to keep running and implement the policy, especially during the effects of the Covid-19 pandemic. Though the improvement of advanced technology growth worldwide, there also other cybersecurity issues still existing and the growth of cybercrime in the AI's world. By knowing the victim's behavior of hacking, the Active Cyber Defense Certainty Act specifies reasons on which allowing the cyber defenders to performing cyber defense techniques. There are also other ways to protect oneself from hackers as the following: using the secured Internet connection, limiting access to all personal accounts through public laptops or computers, and preventing fighting back the hackers or attackers if you cannot able. However, these ways may not apply if the devices have been compromised and already hack. Following this policy sides with the Active Cyber Defense Certainty Act, it may help.

References

AP 21. (Feb 2018). Cybersecurity Funding. White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf

Bocetta, S. (2020, March 10). *Has an AI cyber attack happened yet?* InfoQ. https://www.infoq.com/articles/ai-cyber-attacks/

Cook, C. (2018). Cross-border data access and active cyber defense: Assessing legislative options for a new international cybersecurity rulebook. *Standford Law & Policy Review*, 29(2), 205-236. https://law.stanford.edu/wp-content/uploads/2018/08/SLPR_Cook.pdf

Gandhi, H. (2019). Active cyber defense certainty: Digital self-defense in the modern age. *Oklahoma City University Law Review,43*(2), 279-310. https://heinonline-org.proxy.lib.odu.edu/HOL/Page?collection=journals&handle=hein.journals/okcu43&id=292&men_tab=srchresults

Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sensing*, *11*(10), 1168. https://doi.org/10.3390/rs11101168

Martinez, G. (2020). Hacking back: Self-defense, self-preservation, or vigilantism. (Publication No. 28089093) [master's thesis, Utica College]. ProQuest Dissertations and Theses Global.

McGuigan, A. (2019). Hacking back: Justifiable or vigilantism? (Publication No. 22618512) [master's thesis, Utica College]. ProQuest Dissertations and Theses Global.

McKenna, A. T. (2019, July 21). The ACDC Act opens the door to a hack-back highway to hell. Brinknews. https://www.brinknews.com/the-acdc-act-opens-the-door-to-a-hack-back-highway-to-hell/

Sussman, B. (2019, October 9). *The ransomware victim that hacked back*. Secureworld. https://www.secureworldexpo.com/industry-news/the-ransomware-victim-that-hacked-back

Text - H.R.3270 - 116th Congress (2019-2020): Active Cyber Defense Certainty Act. (2019). Congress.Gov. https://www.congress.gov/bill/116th-congress/house-bill/3270/text?r=1&s=1