What Do Social Scientists Know About Cyber Defense?

Cameron Stegura

26 October 2021

Distinctions between Cybersecurity and Cyber Defense

As we dive deeper into the technological era of society, not only must we take preventive measures to secure our sensitive information, but we must also implement defensive operations when we are attacked. Referring to Mike Tyson's famous 1987 quote: "Everybody has a plan until they get punched in the face." Tyson's words aptly demonstrate the difference between cybersecurity and cyber defense. Cybersecurity applies and plans the correct preventive software and measures required to prevent an attack from happening. Preventive measures are indeed essential. However, if a security breach still occurs, only defensive mechanisms will prove to be effective. Little is known about how effectively defensive strategies are conducted. This essay will not only discuss articles relating to cyber defense, but will also examine topics such as cyber-deterrence, cyberattacks, and the measures currently taking place to ensure the safety of private information.

What is Cyber Defense?

Unlike cybersecurity, which focuses on taking preventive measures, cyber defense focuses on counteracting and actively defending against cyberattacks Chuck White (2017). For example, in the United States government, there currently exists a response plan called the NCIRP (National Cyber Incident Response Plan) which provides a national approach for dealing with cyber incidents involving both government and civilian agencies.

There are also multiple procedures that could be considered cyber defense. One of the most common procedures used applies the most appropriate and effective counteractions to neutralize the opposing force. This method is the swiftest and most appropriate for dealing with cyberattacks. Another procedure commonly used involves resisting the attack. It may not be the most effective, but depending on the situation, it could be the most appropriate in stopping the attack from going any further.

What do we know about Cyber Defense?

In Dorothy Denning's (2016) *Cybersecurity's next phase: Cyber-deterrence*, she discusses the recent topic of cyber-deterrence and how it can be used to address certain cyber threats. Denning found that there was a 1,300% increase in cyber incidents against the federal government from 2005 to 2015. This inspired her idea of deterring attacks before they occur. Denning proposes two main principles of deterring cyberattacks. The first is classified as denial, which consists of persuading the attacker of the futility of their efforts. Denial involves reasoning that the attack requires more resources than the attacker is willing to give up. The second principle punishes the opposing force by informing them of the severity of a potential response. This deters the attacker from making rash decisions that could lead to consequences that they are not prepared to handle. Cyber-deterrence is its own cyber defense system, it not only creates a response towards the enemy, but it also lets the enemy know, bluff or not, that there exists the possibility of retaliation which could result in the termination of their attack.

In *The FBI is breaking into corporate computers to remove malicious code – smart cyber defense or government overreach?* by Scott Shackelford (2021), there is discussion of how the government, in spite of potential cyberattacks, is able to search through privately owned computers and delete malicious software designed to take over the victim's computer. Due to the rise in malicious software being delivered and downloaded through email, on April 9, 2021, the United States District Court for the Southern District of Texas approved a search warrant for the layered defenses. The second part of Shackelford's article demonstrates a proactive approach that retaliates against the hack and counterattack through the exploitation of information on the adversary. An example of this is the supply chain hack on Solarwinds, which allowed us to demonstrate the government's ability to pinpoint the location of hackers from Russian intelligence services.

Johns Hopkins University's Terry Thompson (2021) is a cybersecurity professor as well as the author of *The SolarWinds hack was all but inevitable – why national cyber defense is a 'wicked' problem and what can be done about it*. Thompson's article describes one of the most disastrous cyber breaches in national security history. To summarize, the Solarwinds hack was a supply chain/trojan horse hack in which customers of Solarwinds downloaded an update containing malicious software, giving the hackers access to customer IT systems. Thompson also describes the problematic nature of the current cyber defense situation in the United States. He describes the flaws of the cyber defense situation by analyzing the lack of clear motivation and unity in effort regarding the defense of cyberspace from enemies. By focusing more on the driving force behind and the U.S. cyber defense branch's ability to react to situations, attacks similar to the Solarwinds hack can be prevented in the future.

Benjamin Jensen and Chris Inglis (2020), co-authors of *Government cybersecurity commission calls for international cooperation, resilience and retaliation*, address the international cooperation necessary to bring cyberattacks to an end. Jensen and Inglis conducted extensive research on a new comprehensive plan of action that utilizes a cyber deterrence strategy consisting of three layers. The first layer focuses on the rules of society and the shaping of behavior in cyberspace through the promotion of responsible behavior in addition to the assignment of different expectations based on the roles of the government in addition to the private sector. The second layer prioritizes decreasing the effectiveness of cyberattacks through the encouragement of national resilience throughout the United States. This would call for collaboration between all sectors of the cybersecurity community to continue the operation of economic markets online, even if faced with a cyberattack. The third layer suggests a cyber geneva convention of sorts. This entails holding perpetrators accountable and imposing appropriate fines for malicious actions in cyberspace. As technology rapidly evolves, the United

States must constantly update its technology to maintain the capability to respond to any nation's attack. Lastly, the implementation of an "early action with diverse responses" emphasizes the importance of early detection and rapid action upon the perpetrator.

Although the government is primarily responsible for defending our country from all threats, private companies that are critical to the country's economy and infrastructure must also take on this burden. Bryan Cunningham (2020), the author of *Cyberspace is the next front in Iran-US conflict - and private companies may bear the brunt*, explains how Iran and other countries have been targeting U.S. private sector companies rather than the government. With the lack of government protection throughout the private sector in addition to the absence of rules in cyberwar, U.S. infrastructure is at a high risk of being attacked. By attacking the economy, enemies are able to cause significant damage to homes, businesses, and people. Iran's history of conducting cyberattacks on the United States includes the illegal access and control of the New York Dam, stealing personal information from the Sands Las Vegas Corporation, and targeting private information from universities and federal agencies. This only highlights several instances of what the Iranian government has done from 2011 to 2017. With this recent history, more cyberattacks can be expected and the private sector must find a way to protect itself. Cunningham advocates for vigilance and communication. Not only should these critical infrastructure companies communicate diligently with each other, but also with government entities such as the DHS and FBI to provide further protection. Being vigilant calls for the constant monitoring for cyberattacks and the ability to immediately act upon them to stop any potential damage. By adding vigilance and communication to our cyber defenses, there is potential to halt cyberattacks from Iran and possibly stop a cyberwar from happening.

Potential Strategies and Future Implementation

Shifting U.S. focus to the improvement of the nation's cyber defenses permits the avoidance of significant damage and appropriate responses to attack. Some scholars suggest that cyber-deterrence be implemented through reasoning with the attacker before anything occurs, resulting in less financial strife and the preservation of infrastructure. However, it is important to note that risk is involved with these methods. Negotiation should be done with confidence and preparation with essential equipment on standby to avoid disaster born from negligence. Whether the FBI performs malware checks on private computers or individuals perform self-checks, methods of communication and vigilance are key to cyber defense. Scholars believe this would allow the U.S. to maintain risk awareness and minimize damage dealt. Other professionals suggest direct reactions to the opposing force by investigating, retaliating, and engaging in counterattacks. This would not only aid in identifying perpetrators, but also in the maintenance of proficiency and credibility across cyberspace. This research establishes the importance of cyber defense and how the United States must stray from reliance on preparation and practice a proactive approach when encountering cyberattacks.

References

Cunningham, B. (2021, February 1). *Cyberspace is the next front in Iran-US conflict – and private companies may bear the brunt*. The Conversation. Retrieved November 1, 2021, from https://theconversation.com/cyberspace-is-the-next-front-in-iran-us-conflict-and-private-companies-may-bear-the-brunt-129487.

Denning, D. (2021, February 1). *Cybersecurity's next phase: Cyber-deterrence*. The Conversation. Retrieved November 1, 2021, from https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090.

Jensen, B., & Inglis, C. (2021, September 1). *Government Cybersecurity Commission calls for International Cooperation, resilience and retaliation*. The Conversation. Retrieved November 1, 2021, from https://theconversation.com/government-cybersecurity-commission-calls-for-international-cooperation-resilience-and-retaliation-133610.

Shackelford, S. (2021, July 29). *The FBI is breaking into corporate computers to remove malicious code – smart cyber defense or government overreach?* The Conversation. Retrieved November 1, 2021, from https://theconversation.com/the-fbi-is-breaking-into-corporate-computers-to-remove-malicious-code-smart-cyber-defense-or-government-overreach-159185.

Thompson, T. (2021, July 29). *The SolarWinds hack was all but inevitable – why National Cyber Defense is a 'wicked' problem and what can be done about it*. The Conversation. Retrieved November 1, 2021, from https://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084.

White, C. (2017, July 5). *What is cyber defense? cyber security vs cyber defense*. Fornetix. Retrieved November 1, 2021, from https://blog.fornetix.com/pivoting-from-cyber-security-to-cyber-defense.