**The Present Strengths of Offensive Actions Over Defense in Cybersecurity**

Mandeep Parihar

ITSC 201 – Military and Strategic Studies

Dr. Stuart White

December 14, 2020

In cybersecurity, there is a perpetual struggle between the offensive and defensive sides. Through the use of obfuscation to disguise attacks, the shortcomings of defense not being limitations for offense, and using the initiative of an attack to circumvent defenses, offense is the leading side of the two. For defense to close the lead that offense has taken, it will need to adapt the ideas and strengths of the offense and blend them together with their defense.

Cyber-attacks hold an advantage by using obfuscation to disguise the workings and intent to achieve their goal. The core idea of obfuscation in warfare “is the art *(tao)* of deceit” (Sun-Tzu, 1993, p. 104). Because deceit needs to be maintained and this slows down the process of attack, this runs contrary to Sun-Tzu’s (1993) idea that warfare should “seek the quick victory” (p. 107). “Attack where he is not prepared; go by way of places where it would never occur to him you would go” (Sun-Tzu, 1993, p. 105). While these slow working, back-channel types of attack take more time to get through a network, they, in turn, makes the attacks more difficult to detect, and, once detected, difficult still to stop. Sun-Tzu (1993) said “generally in battle, use the “straightforward” to engage the enemy and the “surprise” to win the victory” (p. 119). The “straightforward” is the disguised appearance and innerworkings of the attack, and the “surprise” is the real intent of the offensive action. In cybersecurity, obfuscation of offense runs parallel to areas of Sun-Tzu’s The Art of Warfare, such that they are both centrally concerned about whether or not to engage in war, and if one does engage then they need to be very aware of it, focusing on the logic and calculations necessary to make careful choices. This distinction puts offensive cybersecurity actions ahead of defensive because there isn’t a fearful waiting of when something will happen. The attackers are able to decide when and how their attacks are deployed and when their goals are considered met by hiding behind an inconspicuous mask.

Offense are not restrained in the same ways that defense is in cybersecurity, nor does it have to make the same considerations. Clausewitz (2008) said that “one cannot think of the defense without that necessary component of the concept, the counterattack” (p. 194), something echoed by Corbett (2004) when he said “counter-attack is the soul of defense” (p. 29). This limitation does not exist for the attack because it “is complete in itself” (Clausewitz, 2008 p. 194), meaning that an offensive action can be made without the need for an accompanying defensive action, whereas the inverse is not capable. Combining this with the “straightforward” and “surprise” elements mentioned earlier, this provides cyberattacks with additional layers of complexity. These complexities make the attack harder to trace back and fully remove from a system that uses defense in depth as the attackers have more areas where they can obfuscate and focus on just the attack. Additionally, whereas a defense needs upkeep and maintenance to ensure functionality even after being established, the offense does not. Clausewitz (2008) wrote an “attack cannot be completed in a single steady movement: periods of rest are needed, during which the attack is neutralized” (p. 194); however, once the attackers successfully infiltrate a network and establish themselves, the attack can continue with limited interactions. Many defensive systems are difficult and/or expensive to update and upgrade, so an autonomous attack can be made for headless operations that, for example, actively copies the information and changes made to a database composed of private information. Where defense is put in the position of having to incorporate offensive ideas into itself to be complete, offense is complete on its own. This positions offense to have less overheads to plan for, and can be strengthened with defensive ideas.

By utilizing the initiative, offense is able to exploit the advantage it holds to bypass defenses unnoticed. The most substantial element of the initiative is the first move, which combines with the element of surprise, to attain victory through “speed, concealment, accuracy of fire” (Freedman, 2013, p. 182). The speed comes in the form of how sudden cyber-attacks often occur, concealment comes in the form of the aforementioned obfuscation, and accuracy of fire is expressed through the targets of the attack and the exploitations needed to get to them. These three ideas come together by “surprising the enemy by concentrating superior strength at certain points” (Clausewitz, 2008, p. 163). “It is that where attack is most to be feared, there defense is weakest” (Corbett, 2004, p. 264). Attackers can map a network before initiating their attack, identifying the vulnerabilities in their defense and what those defenses are attempting to protect, and then establish themselves behind them. As the offensive side are against “the expert in the attack, the enemy does not know where to defend” (Sun-Tzu, 1993, p. 123), thus permitting them to reveal themselves with a concentrated attack at specific targets of the network that will coerce their victims into compliance and submission. Sun-Tzu (1993) stated “if we can make the enemy show his position *(hsing)* while concealing ours from him, we will be at full force where he is divided” (p. 125). The initiative of the attack grants the attackers the advantage to understand the innerworkings of the target before they commit to an attack method. This understanding positions the attackers to circumvent the defenses that stand in their way, and see to it that their attacks are successful.

A familiar expression is that the best defense is a good offense, something that needs to be taken more seriously if the gap between offense and defense is to be reduced. As it stands now, offense holds the upper hand in cybersecurity by utilizing its strengths. The attackers are able to use their initiative to understand their target network, traverse around the defenses in place to stop them, and use obfuscation to conceal themselves to make their detection difficult, and, even if detected, difficult still to remove. Both of which are attributes that only attackers can wield against defenders. Sanger (2018) wrote “the sheer acceleration in the number of attacks, and their rapidly changing goals, is one of several warning signs that we are all living through a revolution, playing out at digital speed.” (p. 319 – 320). Presently, there is a growing threat being posed by attackers, revealing that cyber-attacks are currently stronger in cybersecurity than defense can hope to compete with unless they integrate ideas offensive cybersecurity. Until new measures are taken to improve security, the lead the attackers hold will only grow.

# REFERENCES

Clausewitz, C. (2006). *On war*. (M. Howard & P. Paret, Trans., B. Heuser, Ed). New York:

Oxford University Press.

Corbett, J. S. (2004). *Principles of maritime strategy.* Dover Publications.

Freedman, L. (2013). *Strategy: A history*. Oxford: Oxford University Press.

Sanger, D. (2018). *The perfect weapon*. New York: Crown.

Sun-Tzu (1993). *The art of warfare*. (R. Ames, Trans.). New York: Random House.