Alexei Hooks

SRA 450

Professor Hodgson

November 18, 2022

Individual Assignment One

The policy maker's perceptions need education on the difference between modern day cyber-attacks and cyber warfare. The two are often confused, but one is a subcategory of the other. Cyber warfare is the general concept of modern-day digital war, while cyber-attacks can be compared to weapons used on the battlefield.

As each generation has conflict, new weapons come to fruition to serve a purpose on the battlefront. Cyber warfare has been used at an increasing rate to attack enemies in various ways, however the media has misconstrued why cyber-attacks are used. The journal article "Cyber Warfare: A Misrepresentation of the True Cyber Threat" by author Troy E. Smith, points out how the media presents a negative connotation on the understanding of what cyber war is, and what it may become in the future. As technology continues to become the dominant force within the world of warfare and battle strategy, it is very important to understand the policy around actionable war tactics as it can help in knowing when an acceptable retaliation should occur. As the world has developed an understanding of what just war should resemble (bellum iustum), advancements in cyber capabilities have forever changed the way that countries attack each other, and therefore should adjust the correct response to never-before-seen circumstances. Smith illustrates the current landscape for cyber warfare in a masterfully written article about how change needs to occur within policy to adapt to how cyber warfare has recently been experienced.

As the journal article attempts to explain what the current state of cyber tactics entails, use of previously established war strategy allows for a comparison to see how distinct cyber warfare is to traditional war. The use of the term cyber-attack, as it increases in popularity, has allowed the media to confuse its definition with cyber warfare. Smith argues that instead of trying to constitute cyber-attacks into a category of warfare, policy makers should instead lean towards cyber-attacks being more of a weapon. Now that there is the ability to wage war with unmanned fighters and through digital means, cyber-attacks should be considered the new era's machine gun. Smith says "Cyber-weapons are different from classical ones, in that they are not directly lethal; however, if used correctly they can lead to potentially lethal situations and devastate economies" (Smith 84). As cyber warfare should be aimed at how the actions of attackers are taking place, it allows for a more precise definition, giving policy makers a more distinct understanding about how to arrange cyber tactics into the just war theory.

Smith uses teachings from the ancient Chinese military strategist Sun Tzu, who is credited with the famous writing "The Art of War," which has been used throughout war history by some of the most prolific strategists. The teaching Smith references states "the clever combatant imposes his will on the enemy, but does not allow the enemy's will to be imposed on

him" (Smith 82). Within the context of cyber warfare, the article lays the foundation as to why it is critical that cyber-attacks are meant to be used without the enemy knowing it is occurring. As cyber warfare has been used for mostly indirect attacks, because enemies learn to add defenses quickly, this leads to a lack of ability to repeat over a short amount of time. The continued popularity of the term cyberwar is creating a change in perception in how attacks and defenses should be used. As the true nature of cyber-attacks should be to stay anonymous from the enemy, Smith explains that cyber-attacks are comparable to the prolonged use of espionage in war, whereas both are war strategies that are used in warfare. As the media has transformed cyber warfare to mean a more direct and instant threat, policy makers can get caught thinking that cyber-attacks are more than just a means of war. This can lead to a litany of issues including wrongful calls to action, and regulations that escalate the need for more devastating offensive cyber tactics.

A stem that comes from nation-states not wanting to be known as aggressors through cyber-attacks is what Smith calls "the problem of attribution" (Smith 83). In most modern cyber-attacks, it is known that identifying the perpetrator is one of the most difficult tasks. Continuing from Sun Tzu's teaching, cyber attackers mask their presence, but also can fully denounce that they had involvement, creating an issue when attributing the attack to an enemy. This can cause chaos when an attacked nation is trying to know their enemy, as their defenses will be shielding from any combination of enemies. This leads to an overall weakness from the true attacker, who can continue to attack undefended against in the future. As policy makers should understand the nature of cyber-attacks, they should also need to understand that there should be separate processes in case of unknown or known attackers. This would allow for more specific procedures, which could translate in better wartime decision making and execution of cyber defenses.

Being that policy making is reactive in nature, tensions for victim nations run very high when new rules are enacted. A weakness found in this article is that Smith does not try to quantify emotional value in policy making. It would have added an additional layer of understanding as to why policy makers need to have the best education on these issues. Cyber warfare is an ever-evolving arena, and policy makers can act as referees to allow for a just war to be fought. Having an extra element of emotional value could have enhanced the overall study as it would have increased reader connection to the issue.

When looking into what types of subsequent studies could be done to further Smith's points of cyber warfare, it would be advantageous to pursue another scope into the issue. As cyber is based in espionage and sabotage, looking into the economic factors that go into this type of war would help researchers understand the difference from traditional war. Using the results of this article, analyzing the costs of defense, offense, and overall economic factors of known attacks. Cost breakdowns from these known attacks can show another angle to an already devastating situation and allow researchers to see other layers of cyber-attacks. Cyber warfare is not unlike financial warfare as both see catastrophic economic impacts to victims involved.

Overall, the argument that the journal article Troy E. Smith creates is backed by evidence-based analysis. With increased confusion around the term cyberwar, policy makers will

be making uninformed decisions about how to handle these situations. As cyber-attacks are constantly being attempted, overreaction from governments can create issues and tensions that could possibly be avoided. Being able to put into practice the use of teaching around how cyber should be used in war, and what its capabilities are, can allow for an increase in educated policy makers, resulting in better overall decision making.

References

Smith, Troy E. *Cyber Warfare: A Misrepresentation of the True Cyber Threat*, Vol 31, no. No. 1, 2015, pp. 82–85.