Ethifying Cyberwarfare in modern times

Abstract

There are four things we can ask ourselves to practice better ethical decisions and then apply them to cyberwarfare. First, are we aware of the consequences when we commit this attack? Second, can we meet our objectives and minimize the harm to those we are attacking? Third, will we as a nation accept the consequences? Fourth, was this the right decision to make? This research will aim to analyze these questions by reviewing past attacks and then evaluating the damage caused by these cyberattacks. This research utilizes online tools such as electronic media that focuses on treaties that have been proposed, signed, and recommended as well as whether treaties can be aligned more with our ethical beliefs.

Exploring these aforementioned questions and then looking at the different type of cyberwarfare attacks, we will evaluate if utilizing cyberwarfare to attack other nation states can be performed while minimizing loss of life and causalities, and possibly preventing long-term affects.

Table of Contents

Introduction

Is it possible to engage in cyberwarfare and still perform it in an ethical manner? Defining ethical warfare generally can be quite confusing. A war can be ethical but the means in which the war is being engage can be unethical. If one of the states is utilizing landmines, torture, chemicals and, now during more modern times, drones, this can be considered unethical. The Just War theory outlines principles for a war to be ethical and that means waged by a legitimate authority. Cyberwarfare is defined by engaging in or utilizing digital attacks against an enemy state, resulting in real life consequences. Yet, to date, no cyber actions have been described as a war. Still, “the question remains as to whether war is ever morally justified.” (Moseley, A., n.d.).

Since there has been no indication thus far that a cyberwarfare attack has resulted in human casualties, we don’t have existing data to reflect on. A senior threat intelligence analyst at Jing Xie stated, "I have no doubt it's just a matter of time that someday cyber attacks will definitely cause direct harm to people,” (Palmer, D, 2018). We can speculate what could happen and how we can minimize the damage of future attacks and prevent human casualties.

Literature Review

When researching the definiton of cyber activities, you come across many different meanings. Gernerally, “we define cyber-activities as those that start and have an impact in the cyberworld and may impact the physical world as well.” (Barker, K, 2019).

There are plenty of ethical issues as it relates to cyberwarfare. Let’s say a nation state is aware of a vulnerability on a system which can be utilized to attack another nation. Should that nation state withhold the information from the vendor who has that vulnerability? Is there a moral obligation to notify the vendor so they can develop a patch to mitigate this issue? If the nation state keeps it to themselves, they will have a strategic advantage. However, what happens if that same nation state with the upper hand is also susceptible to the same vulnerability.

There are some guidelines on vulnerability disclosure. Assuming we get past the vulnerability disclosure, there are also guidelines that nations follow that state the attack should be proportional. “The law of proportionality states that the suffering and devastation that one side causes, especially collateral damage to unintended targets, cannot outweigh whatever harm prompted the conflict.” (Stuxnet and its hidden lessons on the ethics of Cyberweapons, n.d.).

Using Stuxnet as an example of a cyber weapon, there are those who felt Stuxnet was indiscriminate. However, “this may be a wrong interpretation, outdated for the cyber age. While Stuxnet lacked discretion under the old way of thinking, its very design prevented harm to anyone and anything beyond the intended target.” (Stuxnet and its hidden lessons on the ethics of Cyberweapons, n.d.). The argument is that the Stuxnet malware infected thousands of machines beyond its original target. Even though those machines were infected, the malware was smart enough to know not to attack the host as this was not the intended target. The malware looked for specific values on the machine before it could activate.

Based on my extensive research, I agree with this author’s findings that the creator of the Stuxnet malware was acting ethically. Another author who also agrees states, “In this paper, I will argue that the developers of Stuxnet were acting morally in creating and releasing Stuxnet because they were acting with support from the authority of the sovereign, because they were acting in line with a just cause, and because they were acting with rightful intention.” (An ethical analysis of the actions of the developers of... , n.d). In my opinion, even though the machines were infected with the Stuxnet malware, since there was no damage to the infected machines, this cyberweapon acted within ethical boundaries. Another author exercised the same opinion, “Jus in bello provides a framework for assessing the moral standing of a war-time action. In the case of Stuxnet and its clear intent to protect civilians, plan for contingencies, avoid damaging anyone other than the enemy, and sustain proportionality, we see jus in bello exemplified.” (University of Pennsylvania, n.d.).

It's fair to say if you're following the points mentioned below, you are working within ethical boundaries when utilizing a cyberweapon:

• The attack must be proportionate to the attack, known as "jus in bello.."

• Acting ethically means acting with rightful intention. In this case, the malware qualified its targets.

During my research, I was unable to find any analysis in which someone thought Stuxnet was unethical nor was I able to find conflicting statements about the use of cyberweapons being unethical as long as they followed similar treaties involving conventional weapons.

Background

A cyberwarfare attack is an attack where computers have become weaponized. Cyberwarfare is usually associated with a nation state performing the attack. Research shows the first cyberwarfare attack was the Stuxnet attack, which was the first attack reported to cause real world physical damage. The Stuxnet attack was an attack that destroyed numerous centrifuges at Iran's Natanz uranium enrichment facility. The code on the centrifuges was modified which caused the centrifuges to spin faster than they should as well as slower than they should, causing the centrifuges to burn themselves out.

Those in the military have been debating quite a while as to whether cyberwarfare is considered to be on the same level as a kinetic attack and would require a kinetic response. This paper brings to question whether a nation state's response to a cyberwarfare attack can and should be with conventional weapons. "The current legal system which exists around war isn't necessary up to date with this type of problem. The borders of cyberspace are much more malleable and unclear, so it's not entirely clear when a nation-state has a moral or ethical right to react in a forceful way." (Palmer, D, 2018)

Significance

Engaging in this discussion is needed in the early days of cyberwarfare considering cyberwarfare is a newer aspect of war. As technology improves, the question that becomes more evident is if automated warfare separates humans from the consequences of their actions. This become evident with drones. "Evidence points to them as being wildly unsafe towards noncombatants." (Huang, T, 2019). This, in my opinion, sets a parallel with cyberwarfare. You are sitting behind a computer or a console with very little or no fear of harm to yourself pulling a trigger where there can be real life consequences. With drones, this type of warfare has resulted in loss of human life. The next step is the loss of human life from cyberwarfare. We need to understand how to make ethical decisions and then, more specifically, ethical decisions towards cyberwarfare.

As we continue to study boundaries, morally acceptable actions, and how a cyberwarfare can result in the loss of human life, we need to bring to light how these actions can significantly cause a chain reaction that can result in escalated actions and possibly resulting in a kinetic war. Nation states need to engage in treaties and understanding in order to know where that “red line” sits. “There is no universal, formal, definition for how a cyber attack may constitute an act of war.” (What is cyber warfare: Types, examples & mitigation: Imperva. Learning Center, 2021)

Discussion

There is no doubt cyberwarfare attacks will continue as well as escalate in their level of sophistication. The reasons behind cyberwarfare attacks vary and this paper will present some of the reasons behind cyberwarfare attacks. Carl von Calusewitz brought up a good point “War is not an independent phenomenon, but the continuation of politics by different means.”

One of the reasons a nation state will engage in a cyberwarfare attack is because of espionage. A nation state will launch botnets or engage in spear phishing attacks in order to gain access to infrastructures that house sensitive data. Once access is gained, sensitive data will be exfiltrated and brought back to the nation who launched the attack. Nations look for sensitive data such as military deployments or blueprints for military equipment. They will even attack companies to get data on certain products that can give that nation an unfair advantage for economic benefits. Some nations have attacked

law firms to get merger and acquisition data that allow them to make unfair advances in the market. “The three allegedly conspired to ‘infiltrate’ the networks and servers of two unnamed New York-based law firms to steal inside information about pending M&A deals that the firms were handling.” (Cheng, R, 2017). The aforementioned case has been rumored to be sanctioned by China but no evidence can connect the two.

Let’s start with the first question, are we aware of the consequences when we commit this attack? We can be assured, whatever the attack is, the results can be disastrous. The goal of a cyber attack is to disrupt computer systems and the majority of cyber attacks have resulted in the loss of sensitive information from military sites and private corporations. To provide an interesting comparison here, in May 2006, The Department of State’s networks were hacked and an unknown threat actor downloaded terabytes of sensitive data. So, what if this occurred outside of cyberspace and a nation state backed up a truck to a United States government building, broke through the front door, disabled our security guards, and removed cabinets of secret information? This would absolutely constitute an act of war. However, since it is in cyberspace, nothing happened. Let’s fast forward to January 2008 where four incidents overseas either threatened or were able to disrupt the power supply to four foreign cities, which could result in human causalities. Specifically, those who are receiving medical treatment and surgery requiring electricity for successful procedures and operations.

Second, can we obtain our objectives and minimize the harm to those we are attacking? Utilizing a publication “Minimizing casualties in biological and chemical threats (war and

terrorism)" (S;, N, n.d.), I was able to extract information on how to prevent harm to an enemy state's population that originally had not come to mind. We can minimize human casualties by educating them; the main goal of educating allows us to reduce human loss by allowing them to defend themselves. They would be provided with what the threat can do and how they can cope with it.

In regards to a cyberwarfare attack, let's consider this as the example. The nation state who is going to attack would provide the state being attacked with information on the nature of the attack and how to prepare. If their electrical grid is going to be attacked, they would be given a notice that in 48 hours, they will take down their electricity. They would be told to bottle water, and obtain foods that won't spoil. Of course there will be citizens unable to implement all of this with short notice, but there will be those who can, which would minimize the human casualties as compared to not knowing. Israel is one nation that exercised a warning before attacking. "A text message, a phone call, or an initial strike on the roof. Israel says it gives Gaza civilians warnings to evacuate before bombardment, but activists say it is not nearly enough." (Hermesauto,2021)

Third, will we as a nation accept the consequences? Innocent people are undoubtedly harmed during a war. Part of a nation accepting the consequences is being conscience of who is innocent and who is not. Michael Walzer who wrote "Just War Theory" states, "those who do not pose a threat to anyone else have a basic and inalienable right to life that should not be violated." (Nicholas Wheeler, 2002). Is it fair to accept the

consequences of a soldier's death since they put themselves in a position to impose death?

Fourth, was this the right decision to make? When the United States engaged in war with Afghanistan in 2001, it was in retaliation for the September 11th attacks. I believe this is an excellent example evaluating the consequences of the aftermath and if this the right decision to make. Since no war has been waged via cyberwarfare, we will have to evaluate kinetic wars.

Afghanistan is interesting because there were actors that attacked America on behalf of a group that was located in many different countries. When we evaluate whether or not this was the right decision to make, we need to weigh our objectives versus the effects on the enemy state and whether this puts our country and citizens in a safer position. As a result of Operation Enduring Freedom and Operation Freedom's Sentinel, a total of 2,455 service members were killed along with 10 CIA operatives. (Wikimedia Foundation, 2021). This is just the death total on the American side. From 2001 to 2021, 46,319 Afghan citizens, 69,095 Afghan military and police and at least 52,893 opposition fighters have died. These are staggering numbers. The cost of the project was 176,000 people in Afghanistan. (Wikimedia Foundation, 2021). We have to ask ourselves again, was this the right decision? Did the end justify the means?

Though Stuxnet was not cyberwarfare, it was a sophisticated cyber attack with at least one nation state attacking another nation state. What if the attack was not as

sophisticated and somehow that malware ultimately resulted in a nuclear meltdown of the nuclear reactor? We ask these questions because it brings us back as to whether this was the right decision to make. Thankfully, the result of the attack appears to be what was expected. Assuming Iran's intention was to create a nuclear weapon program, then perhaps the attacking nation state felt it was the right decision to make. There was no direct human loss as a result of this attack and it accomplished its goal.

Implications

As a result, it is important to continue to perform this research—a way of keeping us in check and reminding us that the consequences of a cyberwar can be devastating. As we live, or some might say hide, behind our keyboards, we lose the human element of the attack and might not feel the emotional effects of the attack. We need to keep the practice of ethics constantly in the forefront. If a cyberwarfare attack needs to be initiated, we must only perform the necessary force and attack to accomplish our goal. Injecting my personal opinion here, we should weigh in as to whether the attack justifies the means. Will people be unnecessarily harmed during this attack? Is this attack, overall, preventing future wars and loss of human causalities? Will this preserve democracy? And, as a US citizen, will this protect our country and allow us to continue our way of life that we cherish. If this can help preserve our liberties, then the attack should be considered (if our liberties are truly in jeopardy). To me, it is clear in my

research that not every war or every attack does this. Some have hidden and political agendas.

Recommendations

Technology will continue to advance as we continue down the path of cyberwarfare. It is clear that devastation and destruction you can deliver while sitting behind a keyboard thousands of miles away while sipping on warm coffee will get easier and easier. Being able to see the target with your eyes will be far removed. So, what do we do? I make the following recommendations:

1) Diplomacy, diplomacy and diplomacy – We should engage in diplomacy with enemy states. However, there is a point where diplomacy no longer works, which then leads to the next point.

2) Proportional force – If diplomacy no longer works, proportional force should be utilized. Only use necessary force to send the enemy state a warning to show that force shall be used when needed. This might be a light cyber attack that demonstrates we have the capability to do so and serves as a sample of what we will use if we don't achieve our objective.

3) Awareness – The attacks we launch across other nation states can be launched towards us. We need to protect ourselves from similar types of attacks.

4) Treaties/Rules of Engagements – Treaties with other countries, especially with those who have similar capabilities, can help. These treaties, hopefully, will prevent unneeded escalations and provide an understanding in advance, preventing future attacks. Overall, promoting peace and working with opposing nations through diplomacy should always be the initial effort before escalating and advocating war.

References

4 tips to help you make better, more ethical decisions. Big Think. (2021, September 30). Retrieved November 6, 2021, from https://bigthink.com/thinking/4-tips-to-help-you-make-better-more-ethical-decisions/.

A., T. (2019, October 10). What is cyber warfare? LinkedIn. Retrieved November 6, 2021, from https://www.linkedin.com/pulse/what-cyber-warfare-tejaswini-anand-h/.

Barker, K. (2019). Cyberattack: What Goes Around, Comes Around: Risks of a Cyberattack Strategy. School of Public Policy Publications, 12(17), 1–22. https://doi.org/10.11575/sppp.v12i0.56877

Bellaby, R. W. (2016). Justifying Cyber-intelligence? Journal of Military Ethics, 15(4), 299–319. https://doi.org/10.1080/15027570.2017.1284463

Business home. McAfee. (n.d.). Retrieved December 4, 2021, from https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.

Center for Strategic and International Studies (CSIS) | Washington, D.C. (n.d.). *Significant Cyber Incidents Since 2006*. Retrieved December 11, 2021, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cheng, R. (2017, January 11). *China-based hacking case against U.S. M&A firms illustrates cyber security and enforcement issues*. Forbes. Retrieved December 5, 2021, from https://www.forbes.com/sites/roncheng/2017/01/11/china-based-

hacking-case-against-u-s-ma-firms-illustrates-cyber-security-and-enforcement-issues/?sh=27ba40263c58.

Encyclopædia Britannica, inc. (n.d.). *Afghanistan War*. Encyclopædia Britannica. Retrieved December 12, 2021, from https://www.britannica.com/event/Afghanistan-War.

Ethify: Meaning, origin, Definition - WordSense dictionary. (n.d.). Retrieved November 6, 2021, from https://www.wordsense.eu/ethify/.

Hermesauto. (2021, May 20). *'roof knocking': Israel bombardment warning system under scrutiny in Gaza conflict*. The Straits Times. Retrieved December 11, 2021, from https://www.straitstimes.com/world/middle-east/roof-knocking-israel-warning-system-under-scrutiny-in-gaza-conflict.

Huang, T. (2019, January 28). *The ethical concerns of drone and Automated Warfare*. SIR Journal. Retrieved December 11, 2021, from http://www.sirjournal.org/op-ed/2019/1/28/the-ethical-concerns-of-drone-and-automated-warfare.

M. Taddeo, "An analysis for a just cyber warfare," *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 2012, pp. 1-10.

Moseley, A. (n.d.). The Philosophy of War. Internet encyclopedia of philosophy. Retrieved December 4, 2021, from https://iep.utm.edu/war/.

Nicholas Wheeler. (2002). Dying for “Enduring Freedom”: Accepting Responsibility for Civilian Casualties in the War against Terrorism. International Relations, 16(2), 205–225.

Palmer, D. (2018, July 24). Cyberwar: What happens when a nation-state cyber attack kills? ZDNet. Retrieved December 4, 2021, from https://www.zdnet.com/article/cyberwar-what-happens-when-a-nation-state-issued-cyber-attack-kills/.

Randall R. Dipert (2010) The Ethics of Cyberwarfare, Journal of Military Ethics, 9:4, 384-410, DOI: 10.1080/15027570.2010.536404

Randall R. Dipert (2013) OTHER-THAN-INTERNET (OTI) CYBERWARFARE: CHALLENGES FOR ETHICS, LAW, AND POLICY, Journal of Military Ethics, 12:1, 34-53, DOI: 10.1080/15027570.2013.785126.

S;, N. (n.d.). Minimizing casualties in biological and Chemical Threats (war and terrorism): The importance of information to the public in a prevention program. Prehospital and disaster medicine. Retrieved December 11, 2021, from https://pubmed.ncbi.nlm.nih.gov/15453157/.

Top 25 quotes by Carl von Clausewitz (of 161): A-Z quotes. A. (n.d.). Retrieved December 11, 2021, from https://www.azquotes.com/author/2957-Carl_von_Clausewitz.

Top 5 most notorious attacks in the history of Cyber Warfare. Fortinet. (n.d.). Retrieved December 4, 2021, from https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare

What are cyber threats and what to do about them. The Missing Report. (2021, September 9). Retrieved December 11, 2021,

from https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

What is cyber warfare: Types, examples & mitigation: Imperva. Learning Center. (2021, November 9). Retrieved December 5, 2021, from https://www.imperva.com/learn/application-security/cyber-warfare/.

Wheeler, N. J. (n.d.). *Dying for `enduring freedom': Accepting responsibility for civilian casualties in the war against terrorism - Nicholas J. Wheeler, 2002*. SAGE Journals. Retrieved December 11, 2021, from https://journals.sagepub.com/doi/abs/10.1177/004711780201600203?journalCode=ireb.

Wikimedia Foundation. (2021, November 17). *Civilian casualties in the war in Afghanistan (2001–2021)*. Wikipedia. Retrieved December 12, 2021, from https://en.wikipedia.org/wiki/Civilian_casualties_in_the_war_in_Afghanistan_(2001%E2%80%932021)#:~:text=During%20the%20War%20in%20Afghanistan,at%20least%2052%2C893%20opposition%20fighters.

Wikimedia Foundation. (2021, November 26). *United States military casualties in the war in Afghanistan*. Wikipedia. Retrieved December 12, 2021, from https://en.wikipedia.org/wiki/United_States_military_casualties_in_the_War_in_Afghanistan.

Wikimedia Foundation. (2021, November 28). *Cyberwarfare*. Wikipedia. Retrieved December 11, 2021, from https://en.wikipedia.org/wiki/Cyberwarfare.

Wikimedia Foundation. (2021, November 5). Stuxnet. Wikipedia. Retrieved November 6, 2021,

from https://en.wikipedia.org/wiki/Stuxnet#:~:text=Stuxnet%20reportedly%20ruined%20almost%20one,1%2C000%20machines%20to%20physically%20degrade.&text=The%20worm%20then%20propagates%20across,on%20computers%20controlling%20a%20PLC