20th International Command and Control Research and Technology Symposium

The Morality of Responses in Cyber Warfare and the Just Warfare Theory

Student Paper: Undergraduate (Junior)
Primary Topic: Topic 1 - Concepts, Theory, and Policy
Alternative Topic 1: Topic 2 – Organizational Concepts and Applications
Alternative Topic 2: Topic 7 – Autonomy
POC Organization: United States Naval Academy
POC Complete Address: 1 Wilson Rd #15150 United States Naval Academy, Annapolis, MD, 21412
POC Telephone: (262) 527-1955
POC Email address: m166912@usna.edu

The Morality of Responses in Cyber Warfare and the Just Warfare Theory

By MIDN Thomas Wester, United States Navy

Abstract

In his 1962 book, *The Structure of Scientific Revolutions*, Thomas Kuhn describes that paradigm shifts in technology transform global dynamics. Cyber-attacks represent such a shift in global warfare; paired with increasing sophistication and greater lethality, cyber warfare will likely dominate the 21st Century and beyond. Mounting morally permissible and appropriate responses to this emerging threat will be crucial to ensuring our security as a nation. However, the lack of clear guidelines outlining moral responses to many cyber threats raises many questions. How are we able to morally respond to an attack that may cripple our infrastructure yet not kill anyone, and how do we respond when a cyber-attack kills American citizens? Furthermore, are we morally justified in having a kinetic response to non-kinetic aggression? Cyber-attacks do not have to destroy anything to be successful; nevertheless, these assaults represent a grave security threat. Appropriately responding requires moral reasoning and justification, yet the lack of clear direction necessitates a broadening of the just war theory as it applies to cyber warfare. The conventional theory must be able to address unconventional warfare. Our policy will likely set the global precedent for responses to cyber-attacks; thus, the morality of responses in cyber warfare must be addressed.

Introduction

Cybersecurity represents a major paradigm shift in global conflict and warfare. In his 1962 book, *The Structure of Scientific Revolutions*, Thomas Kuhn developed the notion that paradigm shifts in technology are, and will continue to transform global dynamics.[1] Cyber-attacks are becoming more common; paired with increasing sophistication and greater lethality, cyber warfare will influence and dominate the war-fighting style of the 21st Century and beyond. In a 2012 article, President Obama warned that the “cyber threat to our nation is one of the most serious economic and national security challenges we face.”[2] Mounting appropriate responses to this emerging threat and future attacks will be crucial to ensuring our security as a nation. However, the response must be morally permissible, and there are no clear guidelines of moral responses to many of the cyber threats we face. As a nation we need to respond to threats in a manner which deters groups from attacking and effectively addresses the threat while still abiding by moral and legal guidelines. Our nation's responses will likely set the global precedent for responses to cyber-attacks. Thus, the morality of responses in cyber warfare is an issue that must be addressed.

The era of conventional warfare is ending and cyber-centric warfare is emerging. Technological developments, which occur at rates much quicker than any previously seen, are forcing this emergence at a rate that is difficult to fathom. For instance, in 1996 the United States (U.S.) Government's Accelerated Strategic Computing Initiative (ASCI) developed the ASCI red. ASCI red cost $55 million and was the size of a tennis court, simulated nuclear tests, and, was the fastest computer in the world. Additionally, it was the "first computer to score above one teraflop – one trillion floating point operations per second - on the standard benchmark test for computer speed."[3] Nine years later, another computer was charted at 1.8 teraflops; this was the Sony PlayStation 3. This example serves to illustrate the pace at which technological advancements are occurring. However, these advancements are doing more than simply providing better gaming systems for teens and young adults; these advancements are changing the battlefield and the way in which we will fight wars in the future.

On top of the rapid evolutions in technology, attacks are becoming more prevalent and span all sectors of business and government. Recent estimates place the number of attempted attacks against the U.S. Department of Defense at over 10 million per day.[4] Additionally, while cyber-attacks vary in nature and consequences, the lethal nature and sophistication of these attacks has steadily increased. Previous attacks have resulted in the loss of highly classified information, such as plans for the F-35 Joint Strike Fighter and similar high-level military projects.[5] In 2007, the U.S. government suffered from an "espionage Pearl Harbor" in which an unknown group gained access to information on military agencies servers and were able to download terabytes of information. Furthermore, private companies are increasingly coming under attack. In September of 2014, Home Depot reported a breach in their systems affecting 56 million debit cards in the U.S. and Canada. Additionally, in November, 2014, Sony Pictures Entertainment was hacked resulting in the release of confidential data. These two cases illustrate the rise in the frequency of cyber-attacks against private companies. However, cyber-attacks maintain the potential to cause previously unheard of amounts of damage to the economy and our national security even beyond stolen information; cyber-attacks can have physical consequences.

A cyber-attack can now be used as a method of destroying critical infrastructure, instigating mass panic, or even targeted assassinations. The capability to destroy electric power generators has been demonstrated several times and the U.S. military successfully simulated a cyber-attack that could decimate the entire U.S. power grid.[6] This scenario is commonly referred to as the "repeat smack down scenario" in which cyber-attacks would take down the power grid by targeting electric generators at power stations, possibly even destroying the generators in the attack. Destroyed generators take months to replace, and as a result the grid would be down for a significant amount of time. All of our systems are dependent upon the electric power grid for operation. Such an attack would have widespread disastrous effects. Our ability to distribute and produce food and other consumer goods would be eliminated, factories would have to be shut down, and the financial markets would close. This attack on critical infrastructure would serve as a crippling blow to the economy, result in mass chaos, and possibly kill thousands. However, in addition to a threatening critical infrastructure, cyber provides the capability and precision to target individuals in "assassination" like attacks. For instance, former Vice President Cheney's heart monitor was recently modified in order to prevent the possibility of a cyber-attack when it was found to be vulnerable to attack.[7] As we become ever more connected in cyberspace, this new form of warfare has the potential to exploit even previously unheard of means of targeting individuals. In addition, cyber-attacks can cause mass panic. Consider when Israel's traffic system was attacked in 2013 resulting in the shut-off of the system which controls and monitors the nation's traffic grid and traffic lights.[8] This attack instigated mass panic and chaos on the roads. Yet, while these examples only scratch the surface, they illustrate that with a simple key-stroke far from the battlefield, a single human has the potential to completely cripple even the most technologically advanced world powers.

Furthermore, as nations and organizations seek effective ways to attack much more powerful entities, cyber warfare becomes significantly more appealing. An attack does not necessarily require the purchase of millions of dollars' worth of technology as in conventional warfare. Thus, cyber is relatively inexpensive for the aggressor when compared to conventional warfare. In addition, there is no need to incur the risk of "transporting equipment and deploying troops across borders into enemy territory, not to mention the political risk of casualties."[9] Also, cyber-attacks can be difficult or impossible to trace offering the potential for non-attributable attacks. Furthermore, anyone with a computer and access to a network has the potential to attack even the most sophisticated and critical systems of powerful nations, causing irreparable financial damage and threatening human lives.[10]

Just Cyberwar?

Today, many nations maintain the ability to carry out a cyber-attack. Yet, International laws as well as the laws of war were clearly not written with this capability in mind. Thus, there is a large gap in policy which many organizations have tried to address in recent years. However, the gaps in policy regarding cyber space are coupled with gaps in morality and ethics, including the ethics regarding responses to cyber-attacks. Furthermore, there is little direction provided by current or historical moral theories. This lack of clear direction with regard to potential responses to cyber-attacks raises many questions. How are we able to morally respond to an attack that may cripple our infrastructure yet not kill anyone, and how do we respond when a cyber-attack kills American citizens? In addition, are we morally justified in having a kinetic response to non-kinetic aggression? By their nature, cyber-attacks do not have to destroy anything to be successful; an enemy can steal important information, or simply plant a virus in a system for future exploitation or attack. These types of assaults represent a grave threat to our security as a nation; yet responding requires moral reasoning and justification.

There are several suppositions that must be addressed prior to a discussion of morality and cyber. For sake of this paper, one must assume that we have the technology available to identify to a high level of certainty where the attack originated, and by whom the aggression was committed. While we are currently not fully able to predict the derivation of attacks, our capability to do so is increasing. For the purposes of our discussion, we will assume that this capability has been significantly developed. This assumption addresses the challenge of attribution of a cyber-attack. Yet, additionally, one must assume that we have the technical ability to carry out any proposed response or pre-emptive actions.

Current theories, including the just warfare theory, fail to fully address the moral conflicts in dealing with cyber warfare. The just war theory addresses the conditions in which attacking another country and waging war are permissible. The theory requires war to be declared by a legitimate authority and have a just cause. Additionally, war is only permissible "as a response to some egregious fault, such as a violation of human rights."[11] Furthermore, war must be declared and conducted with the right intention: war should secure peace and protect the common good. Furthermore, war must be a last resort, and it should be avoided at all costs.[12] Finally, war must be both proportionate and provide the opportunity for the just to be victorious.

However, morally justifying a response to a cyber-attack is difficult under the just war theory because "cyber-attacks range from morally trivial to absolutely devastating."[13] An enemy may shut down or take control of a power grid, missile defense system, or unmanned aerial vehicle. Yet, they may also deny access to websites or steal critical information. Since none of these attacks are a direct violation of human rights, a response (especially one that is kinetic in nature) under the just war theory is considered morally impermissible because any kinetic response would not necessarily be considered proportional. However, not responding to these threats in some manner is unreasonable. Stifling the United States' moral responses to a cyber-attack leaves us vulnerable as a nation against an ever emerging and lethal threat. We need to respond to these attacks in a manner that ensures our national security, yet abides by moral guidelines. Our response should set an example for the rest of the world in this new era of warfare. Thus, there is a need for a broadening of the just war theory as it applies to cyber warfare. In this respect, the conventional theory of just war must be able to address the aspects of unconventional warfare.

Framework for Moral Responses to a Cyber Attack

An expansion of the just war theory needs to include kinetic and non-kinetic responses in the event of a cyber-attack, even in the event that human rights are not directly violated. In addition, the theory should also account for cyber responses to non-cyber aggression, both symmetric and asymmetric. The broadened theory should institute new precepts that allow for a reasonable response, yet necessitate a detailed analysis of each case to ensure that responses are morally justifiable. Furthermore, the broadening must maintain the spirit of the original theory and international case law. Therefore, it needs to require that the attack is a direct act of aggression and has lasting effects. For example, much like in conventional warfare, if damage by an attack is done to an offensive ability, the damage is to be considered insubstantial. Yet, if damage limits defensive capabilities, or destroys civilian infrastructure or lives, the damage is to be considered substantial and warrants a more aggressive response. Both kinetic and non-kinetic responses must secure peace and protect the common good. Furthermore, they should be proportional, in the case of kinetic, and for non-kinetic, the minimum response necessary to stop continuing or impending attacks. These qualifications thereby attempt to ensure that conflict is not escalated, and are based on the premise that the responses have successfully deterrent affects.

Kinetic responses should remain only allowable in the case that the attack has intended lethal effects or human rights are directly violated. First, if a cyber-attack directly causes human suffering or loss of life, a kinetic response is warranted. This is much the same as if we were attacked in a physical manner. For example, if cyber is used as a weapon to assassinate an individual, that attack warrants a kinetic military response. Additionally, if a cyber-attack directly results in our susceptibility to a kinetic attack by eliminating our defensive capability, and therefore have reason to believe that a kinetic attack is impending, then we are morally justified in taking kinetic military action even if there is no physical damage. For instance, if a hacker penetrates our missile defense systems and attempts to disable them, a kinetic response is justified. Furthermore, as is the case with many segments of our critical infrastructure, if a cyber-attack has any order effects (2nd, 3rd, 4th, etc.) that result in human harm or death, a kinetic response is justifiable. For example, if a cyber-attack were to take down Chicago's power grid in the middle of winter, many people would freeze to death, and thus a kinetic response is justifiable since the attack results in human suffering. Thus, we are able to morally respond in a kinetic manner to a non-kinetic attack. Yet, kinetic responses should be a last resort; should cause a proportional amount of damage; and, should attempt to be avoided at all costs while abiding by the *just in bello* (justice in war) guidelines of warfare. By utilizing kinetic responses only as a last resort, we will discourage an escalation of attacks and limit the potential spread of warfare.

Non-kinetic responses are justified in the event that a cyber-attack directly targets our systems or information in an offensive manner, yet the attack does not meet the above criteria for a kinetic response. Thus, we are justified to respond in a non-kinetic manner if a cyber-attack directly targets our offensive capabilities or directly targets our systems. However, our response must be limited in the manner that the counter must be the minimum necessary to stop continuing cyber-attacks. This represents a broadening of the just warfare theory. Even though there is no "egregious fault," we maintain the ability to limit enemy systems from attacking. However, in broadening we must ensure that we maintain the spirit of the original theory and international law. In the event of an attack on a system, we are justified in responding to the cyber-attack with a non-kinetic counter-attack that invokes the minimum damage necessary to stop continuing cyber-attacks; however, the damage can not result in any human suffering or elimination of defensive capabilities, as that would violate and criteria and serve as grounds for escalation. Thus, the counter-attack must be defensive in spirit. Therefore, non-kinetic responses apply in the event that critical information is stolen. This broadening constitutes a self-defense of networks and information, and thus allows us to ensure the security of our nation, as well as, set an example for the rest of the world to follow.

The broadening of the just war theory can be analyzed using the Stuxnet virus as a case study. This case is known as the turning point of cyber-attacks; the first instance in which a cyber-attack proved its ability to physically damage systems.[14] In this case, a kinetic response would not be justifiable; neither the attack itself nor the residual effects killed or harmed anyone. Additionally, the attack did not obviously precede a kinetic offensive, nor make the nation vulnerable to a kinetic attack. Therefore, a kinetic response would be unjust. However, a non-kinetic cyber-attack in response would be morally justifiable, under the condition that the response follows the guidelines above. For example, Iran could attack the enemy's servers or network and shut down their ability to impart future attacks. If we modify the case to where an individual working at the plant was harmed, then the response changes dramatically. Rather than being limited to a counter-attack in the cyber domain, a kinetic attack would now be justifiable. In this case, Iran could respond through the use of military force against the attacker.

Objections to Just Cyberwar

A reasonable person may conclude that my expansion of the just war theory is against the very purpose of the theory itself. My broader definition makes counterattacks very easy; the whole purpose of the just war theory is to make war a necessary evil and to stem conflict. Thus it seems as though my expansion of the theory furthers conflict. One major problem is that every cyber-attack warrants some sort of response, in essence creating a sort of limited warfare. In the case of a cyber-attack that steals information, we are able, under my expanded theory, to destroy their ability to carry out that action in the future. Thus, even though they impart no direct damage on us, we are able to pre-empt future activities/attacks with a counter-attack and destroy potentially threatening systems. Some may see this as going against the proportionality contained in the just war theory, since we are destroying in response to a non-destructive attack. Additionally, some may argue that my theory allows for a kinetic response to a non-kinetic attack in the instance where a cyber-attack may stifle our ability to defend ourselves. In many ways this goes against the just war theory, since human life is sacred. Furthermore, it can be very hard to distinguish, especially with computing or command and control systems, the difference between defensive and offensive capabilities. This would prove a challenge when contemplating how to respond to an attack.

Conclusions

Moral responses to a cyber-attack are dictated by the nature of the attack. These are outlined by an expansion of the just war theory. If the attack results in the harm or loss of human lives, a kinetic response can be justified. Additionally, if the cyber-attack is a preemptive strike in order to make a kinetic attack more effective, a kinetic response is morally justifiable.

However, if the cyber-attack does not inflict any suffering upon humans, a kinetic response is unwarranted. In this scenario, responses are limited to a proportional cyber counter-attack. Thus, the expanded just war theory allows room for engagement in cyber warfare, however, still ensures responses are within the bounds of moral reason.

Cyber will be an ongoing threat we will face as a nation now and for the foreseeable future. The threats we face from enemies using cyber are constantly evolving and cannot be analyzed solely by using current moral reasoning. This leaves us vulnerable to attack and limits our ability to respond to many of the grave threats we will face. Thus, it is necessary to expand the breadth of current moral reasoning. If we abide by the moral reasoning outlined in this paper, we will be able to limit the escalation of warfare and maintain the security and integrity of our nation. Without these limits, conflict may spread from the cyber domain and escalate into total war; however, without the expansion of the just war theory, our ability to respond to many of the threats we face is thwarted, leaving us vulnerable and weakening our great nation.

[1] Hagerott, Mark. "What to Expect as Cyber Disrupts the Navy: Insights from Past Technological Revolutions at Annapolis and During Wartime." Lecture, United States Naval Academy, Annapolis, MD, November 8, 2013.

[2] Obama, Barack. "Taking the Cyberattack Threat Seriously." Wall Street Journal. Last modified July 19, 2012. http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

[3] Brynjolfsson, Erik, and Andrew Mcafee. *The Second Machine Age*. New York, NY: W.W. Norton and Company, 2014.

[4] Fung, Brian. "How many Cyber-attacks Hit the United States Last Year." Nextgov. Last modified March 8, 2013. Accessed November 14, 2013. http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

[5] Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal* (New York, NY), April 21, 2009.

[6] Berst, Jesse. "Why NERC Will Attack the Grid November 13 (and What it Could Mean for Utilities)." Smart Grid News.com. Last modified November 7, 2013. Accessed November 14, 2013. http://www.smartgridnews.com/artman/publish/Technologies_Security/Why-NERC-will-attack-the-grid-November-13-and-what-it-could-mean-for-utilities-6152.html/#.UoQuGfkqiSq.

[7] Walker, Danielle. "Dick Cheney's wireless heart monitor was modified to curb hacking threat." SC Magazine. Last modified October 21, 2013. http://www.scmagazine.com/dick-cheneys-wireless-heart-monitor-was-modified-to-curb-hacking-threat/article/317205/.

[8] Estrin, Daniel. "In Israel, Cyberattack on Haifa Road Network Work of Unknown, Sophisticated Hackers." Huffington Post. Last modified October 27, 2013. Accessed November 14, 2013. http://www.huffingtonpost.com/2013/10/28/israel-cyperattack-haifa_n_4169813.html.

[9] Lin, Patrick, Fritz Allhof, and Neil Rowe. "Is it Possible to Wage a Just Cyberwar?" *The Atlantic*, June 25, 2012.

[10] Eberle, Christopher J. "Just War and Cyberwar." *Journal of Military Ethics* 12 (2013): 54-67.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. "Stuxnet Under the Microscope." *White Paper*.