Just Warfare: Is a Nuclear Attack an Appropriate Response to a Cyber Attack?

Alexia Fitz and Richard L. Wilson
Towson University, Towson, MD

afitz2@students.towson.edu
wilson@towson.edu

Abstract: It is well known that nuclear weapons pose a grave threat to humanity because of their destructive power and to the lives of innocent civilians potentially affected by them. What might be less known are the grave effects that cyberwarfare can potentially have on a state and its nuclear security. Most nuclear weapons systems were designed decades ago, when manipulations of computer networks, or cyber-attacks, were practically a non-existent threat. In the present international political situation, where threats about the use of strategic nuclear weapons, have been discussed, cyber threats are everywhere, and it may be expected that they will have consequences for the stability of nuclear weapons systems as well. Considering the many unknowns of the continually evolving issues related to cyber threats, it is hard to measure how serious the risks are, but the idea cannot be excluded that, over the long term, they may have "game-changing" effects on the perceived value of nuclear weapons. Potential consequences of this phenomenon include cyber operations targeting nuclear weapons development, nuclear weapons systems, and cyber operations replacing nuclear weapons. It is crucial that nation states, such as for example the United States, work hard to prevent cyber-attacks in a world where we are becoming more reliant on computer systems that if disrupted could destroy the economy, politics, and even military operations. The question, of how far states are willing to go to protect their cyber realm, and the extent to which their nuclear policies might allow for the possibility of a nuclear response to a cyberattack, present significant issues. This analysis will employ distinctions from just war theory, to attempt to address these issues. Just warfare is important to this analysis because developing a sense of right and wrong in a case of unpreventable conflicts could avoid further escalation and even more devastating results. In other words, what occurs when we apply the ethical distinctions of Just War Theory, to Cyber Attacks related to nuclear weapons? Can the distinctions of Just War Theory be employed to create a taboo, so that, the protection of a states cyber security creates an obstacle so that cyber warfare does not lead to a result such as nuclear attack? This analysis also takes into consideration anticipatory research, while developing an argument based on ethical considerations without a nuclear attack having to occur first. Anticipatory research such as this is important as the foundation for developing preventative measures because it can be used to argue for the creation of policies (both domestic and international) that will not allow for a nuclear response to a cyber-attack, therefore eliminating the threat to the international community. This analysis will employ a basic conceptual analysis that will proceed by defining critical terminology and will attempt to address the ethical and anticipated ethical issues related to answering the question, Is a Nuclear Attack ever an appropriate response to a cyberattack?

Keywords: Just Warfare, Cyber Warfare, Nuclear Warfare, Cyber Attack, Nuclear Attack, Appropriate Response.

1. Introduction

The threat of nuclear warfare is not a new concept to the international community. The development of nuclear weapons began taking place in the 1930s when scientists discovered that controlled nuclear fission could be the source of a massive explosion. Since this discovery nuclear weapons have only been detonated twice in times of conflict, both by the United States military in 1945. Currently nuclear weapons have also been developed by ten states, the United States, Russia, China, France, the United Kingdom, Israel, Pakistan, India, North Korea, and South Africa who eventually denuclearized in the 1990s. This means that out of the nearly 194 recognized states in the world only nine states have nuclear weapons. What makes nuclear weapons so unique is their expense and their destructive nature that allows for only a small percentage of states to have access to this technology. These weapons create high levels of international fear due to the possible use of nuclear weapons in the context of warfare. Rapid nuclear weapon expansion took place during the Cold War, well before the creation of modern-day computer systems and cyber threats. However, although nuclear weapons have not been used since World War II the threat of nuclear warfare continues to loom due to inevitable link of nuclear warfare with cyberwarfare.

Cyberwarfare on the other hand is a more recent development that creates fear in the international community as the technology once created for military advantage is now easily accessible to everyone in the political, public and private sectors. Cyber-attacks have continued to increase as cyber technology has continued to develop and pose threats at the individual level all the way up to the government and military. This has led to an increase in security threats within the domain of cyberwarfare which leads to the question, could a nuclear attack ever be an appropriate response to a cyber-attack? This paper will proceed by first exploring the devastating effects

seen with both nuclear and cyber-attacks and will then examine these warfare techniques in the context of just war theory and particularly jus ad bellum criteria. This analysis is focused on applying anticipatory research based on historical nuclear and cyber warfare policies and the current international climate, to suggest preventative measures seeking to protect international security.

2. Background Effects of Nuclear War

The devastating impact and potential effects of nuclear weapons are well known and are major contributing factors which have led to the creation of many international treaties preventing further proliferation of nuclear weapons while promoting the elimination of existing nuclear arsenals. The destructiveness of nuclear weapons has only continued to increase as nuclear weapons technology has advanced and as nation states have competed to gain military advantage over their adversaries. The first ever atomic bomb was tested by the United States while creating an explosion yielding 20 kilograms of force (ICAN n.d.). Less than one month after the first nuclear test, the United States dropped the first ever nuclear bomb on Hiroshima, Japan, on 6 August 1945. The nuclear bomb known as "Little Boy" produced an explosion with 13 kilotons of force killing directly and indirectly (radiation, burns, cancer) over 200,000 people (Atomic Heritage Foundation 2017, "The Manhattan Project"). Then three days later on 9 August 1945 the United States dropped a second nuclear bomb on Nagasaki, Japan. This bomb was given the name of "fat boy" and produced 21 kilotons of force explosion, killing an estimated 74,000 people both directly and indirectly (Atomic Heritage Foundation 2017, "The Manhattan Project"). Since the first use of nuclear weapons, nation states have increased the amount of force that nuclear explosions yield, which could cause even greater casualties and destruction. The newest nuclear weapons developed by states are thermonuclear weapons, also known as hydrogen bombs, produce explosions a 1000 times more powerful than atomic bombs (Chan 2019, "What is the Difference").

Nuclear weapons create powerful explosions capable of destroying structures and killing millions of people, but they also create a several mile wide radii of radioactive debris. The radioactive fallout from a nuclear explosion will have long lasting effects on the surrounding environment even making some areas affected by the blast uninhabitable. If nuclear weapons were to be deployed all of these factors would have tremendous effects on a state's economy, infrastructure, and military operations. Considerable damage can come from a singular nuclear weapon, however nuclear warfare could potentially lead to the use of multiple nuclear weapons from various states, which could potentially result in even more extreme consequences.

3. Effects of Cyber Warfare

Cyberwarfare has become a growing threat as technological advancements extend the threat of cyberattacks in both the private and public sectors. As technology becomes more accessible so do targets for possible cyber-attacks. These cyber-attacks have the capabilities to reach from individuals all the way up to the government, which could have major effects on a state's stability (Atrews 2020). Cyberattacks can come in many different forms such as information breaches, surveillance, and even gaining control of various devices, including power grids, machines, and nuclear weapon systems and controls. For example, many nuclear weapons systems, including those of the United States, are outdated with outmoded cyber security protective measures and as a result, are at risk for potential hacking. If a cyberattack were to occur on a nation states infrastructure it could lead to massive destruction on infrastructure and effect civilian populations, comparable to nuclear attacks including, crumbling an economy, effecting access to electricity and basic needs, and causing political unrest. These effects could eventually lead to a growing number of causalities over time. Similar to nuclear attacks, cyberwarfare comes with the potential for little to no warning before it is too late to prevent the devastation. Some scholars, such as Benjamin Hatch, would go as far as to say the cyber warfare could be classified as a weapon of mass destruction (WMD), as more states have begun to use cyberattacks as an offensive measure in conflicts. Cyber warfare can create destruction, can disrupt the innerworkings of a state, and can create degradation for those affected, all of which fall within the classifications for WMDs (Hatch 2018).

In 2014 alone, the United States government faced up to 60,000 cybersecurity breaches, potentially effecting the lives of millions of people (Atrews 2020). Cyberwarfare poses threats to U. S. and international security and continues to increase risks as technology continues to advance. Many government officials state that cyberwarfare is more of a threat to US national security than any weapons or physical attacks because of how easily accessible technology has become and how reliant people are on that technology (Dever 2013). Unlike nuclear weapons, cyberwarfare involves military strategy and tactics available to a much wider variety of members of the international community and many states have adapted to the threat by establishing their own

departments of cybersecurity within their government systems. In addition, Cyber-attacks are more threatening because they do not necessarily come from enemy nation states, they can also come from civilian attackers with their own individual motivations, while in comparison nuclear attacks involve large scale military operations. According to the Center for Strategic and International Studies, in October 2022 there were eight significant cyber incidents directed against government agencies. For example, Russia in October 2022 accused the United States of cyberattacks against Russia in the U. S. effort to support Ukraine (CSIS 2022). This is a very clear example of how nation state alliances can also be at play in the use of cyberwarfare similar to how members of alliances can support one another related to nuclear warfare strategy. In Ukraine's current conflict with Russia, Ukraine is focusing on traditional warfare strategies but good relations with the US allows the US to get involved in the war, without even setting foot in the warzone. This example also demonstrates the potential consequences of cyberwarfare, which can create increased tensions between nation states with nuclear capabilities. These developments can in addition potentially spark more aggressive military actions, including cyber-attacks that can lead to the threat of the use of strategic nuclear weapons (and in the current situation, the threat of nuclear weapons and retaliation by Russia) (NTI 2022).

4. Just War Theory

The previous section of this paper explored both the similarities and the uniqueness of the destructive capabilities when nuclear warfare and cyber warfare are compared and when they are combined. Next, we introduce Just War Theory, which aims at establishing legitimate criteria for engaging in war according ethical criteria. The criteria in Just War Theory have changed throughout the course of history. Since ancient times scholars have studied the morality of appropriate and inappropriate actions in warfare, discussing the use of force as justifiable if an enemy has engaged in inappropriate behaviour in war? just war theory falls into 4 categories (Internet Encyclopaedia of Philosophy):

> **Jus ad Bellum:** "conditions under which States may resort to war or the use of armed force in general" (ICRC 2015).
>
> **Jus in Bello:** "regulates the conduct of parties engaged in an armed conflict" (ICRC 2015).
>
> **Jus post bellum:** deals with the conditions of states following war including compensation, punishment, and possible rehabilitation (Internet Encyclopaedia of Philosophy n.d.).
>
> **Jus ad vim:** similar to jus ad bellum but it specific to use of force against state and non-state actors, with lesser outcomes compared to traditional [kinetic] warfare (Brunstetter and Braun 2013).

In other words, war is appropriate if used for means of retaliation against acts of aggression by other nation states (Schmitt 2003). The Treaty of Westphalia in 1648 deemed war justifiable if it was in the best interest of the state, essentially arguing that because of sovereignty there was no limit to conflicts. The Hague Conventions also explored the morality of war, justifying war if conflicts were too large to be resolved through mediation. However, the effects of World War I led to stricter limitations of war and the creation of an international judicial system by the League of Nations, which was later replaced by the United Nations and the International Court of Justice, trying to provide states with methods to resolve conflicts other than by war (Schmitt 2003).

Some scholars explore just war theory from a legal perspective where the international system has made the threat of force and use of force illegal (Nussbaum 1943), including modern day developments in the use of nuclear weapons and the use of cyber weapons to wage cyberwarfare. We can conclude that nuclear and cyber warfare are not justified since they are illegal, yet there is a continuation of conflict in today's world. This paper is focusing on just warfare from the perspective of nation states and how they use moral justifications to argue for their continued use of force in war. Jus ad bellum provides the criteria that theorists established to justify when war is permissible by nation states based on ethical considerations. The criteria that make up jus ad bellum analysis include,

just cause: responding to aggressions by an actor, not initiating conflict. In other words, just cause is an act of self-defence. However, "aggression" is nor narrowly defined and does not only have to include physical

violence. Theorists could argue an act of aggression takes form as interfering with a states economy (sanctions), disrespecting a state's culture or practices, or violating a treaty (Internet Encyclopaedia of Philosophy n.d.).

chance of success: a state must weigh the cost and benefits of waging war to determine if reasonable success is possible. There are moral considerations that must go into the calculations, so that monetary and possible casualties are factored in even in the war is won (Internet Encyclopaedia of Philosophy n.d.).

last resort: war should be a final solution only after all other forms of diplomacy and mediation have failed. In all scenarios, war should be a last resort because of the devastating effects it causes to a state's economy and society as a whole (Internet Encyclopaedia of Philosophy n.d.).

proper authority: a government has proper authority because of state sovereignty. The concept of state sovereignty can be a grey area, but theorists have agreed as long as a government has a legitimate ruling over its citizens (therefore making it a proper state) then it has the authority to declare war (Internet Encyclopaedia of Philosophy n.d.).

proper intention: a state engaging in a just war must be doing so with the intentions of seeking peace and justice. A state cannot justify wars for their own national interests or to assert dominance over another state (taking territory, etc.) when there is no longer just cause and it becomes acts of aggression (Internet Encyclopaedia of Philosophy n.d.).

proportionality: is an overlapping concept with jus in bello in the sense that a war must be fought with an end goal. The end goal, however, should not surpass the aggressions that initiated the war in the first place. For example, a state cannot start a just war, but then continue to act aggressively takeover other states land in the process. (Internet Encyclopaedia of Philosophy n.d.).

Each of these criteria provide potential justification for use of force by one nation state against another. Proportionality is an important distinction for addressing the question, "is nuclear warfare an acceptable response to a cyber-attack?" At first the use of nuclear weapons might seem an extreme response to a cyber-attack that involves no direct physical conflict, however the devastating effects of each type of warfare must be considered before answering the question. A difficulty that is immediately present involves responding to a simple issue, whether when a nation state uses cyber-attacks and cyber warfare to attack another nation states nuclear weapon infrastructure, the attacked nation can respond with a nuclear attack. Proportionality refers to the use of violence by one actor which must be comparable to the violence inflicted on them by another actor. Nuclear warfare and cyber warfare can both possibly target millions of military personnel and civilians. Additionally, they both have the ability to inflict extreme damage to a state's economy, political system, and can cause extreme suffering for a nation's population. So, although both cyber warfare and nuclear warfare are illegal in the context of armed conflict, especially when targeting civilians (ICRC 2021), the use of a nuclear weapons as a response to a cyber-attack is a creditable fear depending on the level of destruction that a state sees as a threat.

A brief discussion of the other criteria of jus ad bellum, as they relate to a nuclear response to a cyber-attack, is also useful in determining if this satisfies the criteria of just warfare. Just cause is applicable in the sense that a nuclear attack could be an appropriate response to initial aggressions in the form of a cyber-attack. Chance of success is also plausible for a state choosing to utilize a nuclear response because a state could justify that it saves money and risks high number of casualties by using a nuclear weapon rather than other tradition means of war that can be extremely costly if the conflict is drawn out. The idea of reasonable success is arguably one of the main reasons for the United States' use of nuclear weapons in World War II, which is explained in the next section, "Just Warfare in Practice." Last resort can be argued on a more conditional basis. Depending on the individual situation, a state could argue that other means of diplomacy were utilized, and that a cyber-attack was the final straw in making its decision to use nuclear weapons. Additionally, proper authority is a criteria that currently applies to all international actors that maintain nuclear arsenals because they are all states with sovereignty and legitimate governments. Finally, It could be argued that proper intent is legitimate, on a situational basis, if states retaliate in order to bring peace and not to use nuclear weapons for additional political gains.

A further distinction that needs to be taken into consideration given the current circumstances is Jus ad Vim. In the 2006 edition of *Just and Unjust Wars*, Michael Walzer introduces an important distinction between, "measures short of war," such as imposing no-fly zones, pinpoint air/missile strikes, and CIA operations, and on the other, "actual warfare," typified by a ground invasion or a large-scale bombing campaign. Even if the former are, technically speaking, acts of war according to international law, he argues that "it is common sense to

recognize that they are very different from war." While they all involve "the use of force," Walzer distinguishes between the level of force used: the former, being more limited in scope, lack the "unpredictable and often catastrophic consequences" of a "full-scale attack." (Brunstetter and Braun, 2013)

In terms of state to state conflicts Jus ad Vim distinctions are related to measures that fall short of kinetic acts in traditional conflicts. Cyberattacks that do not cause immediate physical causalities as opposed to nuclear attacks that immediate physical casualties, fall within the criteria that do not legitimate a physical response. The issue that is focused on in this analysis, Is a Nuclear Attack an appropriate Response to a Cyber Attack? needs to address *jus ad vim* acts that are military actions. The moral issues related to *jus ad vim* acts and cyber-attacks and whether they can rise to the level of justifying a nuclear response can be directly related to the proportionality principle in jus ad bellum criteria. it is important to recognize the degree to which non-violent actions such as cyberattacks, align with and adhere to the proportionality criteria in jus ad bellum, while moving beyond *jus ad vim* principles as introduced by Walzer. The important issue that needs be addressed is, could a cyberattack move beyond jus ad vim distinctions to a degree that would trigger a nuclear response in the context that would satisfy the criteria necessary to engaging in just warfare?

5. Just Warfare in Practice

To better understand the argument that nation states could justify a nuclear response to a cyber attack we must look at past uses of just warfare from both a nuclear and a cyber perspective. Anticipatory research must involve examining past and present examples of situations in order to use this material to make projections about potential future outcomes. In the case of nuclear warfare there is only two examples of the use of nuclear weapons in war, the bombings of Hiroshima and Nagasaki. In these cases what prompted the United States' use of nuclear weapons? The decision to drop the atomic bombs on Japan was made by President Truman and his committee of advisers including, Secretary of War, Henry Stimson (Burr 2020). The decision came due to the unwillingness of Japan to surrender, which would lead to the continuation of the war and cause further devastation and human causalities. World War II was one of the most costly and deadly wars and ending it would be beneficial for the United States and the international community. Additionally, Japan had directly attacked the United States territory in it's surprize attack upon Pearl Harbour, killing both civilians and soldiers, which was one of the driving factors for the US to get involved in WWII in the first place. Stimson advocated for not letting the war drag on when the US had the nuclear technology to end it (Burr 2020). President Truman's committee also considered an invasion of Japan or a demonstration of nuclear weapons near Japan, but all other options were considered to be costly and not forceful enough to motivate the Japanese to surrender. The US military believed they had no other choice and decided to bomb Hiroshima because of its importance to the Japanese military (NPR 2015). On August 6, 1945, the US dropped a nuclear weapon on Hiroshima which was followed by another one on Nagasaki on August 9, five days later Japan surrendered. Because the US was the first state to use nuclear weapons in war, they did not break any international laws. Based upon the criteria of just warfare from an ethical perspective the United States' decision to use nuclear weapons came according to the criteria of last resort, proper intention and just cause in order to attempt to end a very costly war. At a fundamental level it can be argued that proportionality was met because the Japanese had targeted US civilians and military bases first, however, it can also be argued that proportionality was violated due to the total destruction and radiation caused by nuclear weapons that was unlike any other weapon used previously in wars.

The destruction caused by the first and only use of nuclear weapons led to the establishment of many international treaties to prevent future nuclear warfare. Treaties like the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which was open for signature in 1968, was created to prevent an increase of nuclear weapons. NPT only recognized five nuclear weapon states including, China, the United States, Russia, France, and the United Kingdom (United Nations Office for Disarmament Affairs, n.d.). Even with international treaties like NPT in place there is now nine operating nuclear weapons states, Russia, the United States, the United Kingdom, France, China, Israel, North Korea, India, and Pakistan; each with varying policies regarding the use of nuclear weapons. A very common nuclear policy is a "no first use" policy, which ensures that a state will not use its nuclear weapons unless in an act of retaliation against an enemy state that strikes them first (Center for Arms Control n.d.). Currently, India and China are the only countries that have agreed to a no first use policy regarding the use of their nuclear weapons (Global Zero n.d.). India claims to only maintain its nuclear arsenal as a nuclear deterrent against Pakistan, therefore it also agrees to only use its weapons if Pakistan were to initiate nuclear warfare with a nuclear attack. China also has claimed to have a no first use policy, but its creditability has been challenged in recently due to the rapid increase of nuclear weapons in its stockpile and the lack of restraint shown by the Chinese government (Zhao 2021). This leaves a number of key international actors with nuclear

weapons that do not have no first use policies, including the United States, Russia, and North Korea. In theory these states seem to appear to be willing to use their nuclear weapons, if there is a creditable threat to their security due to a cyberattack upon their nuclear weapons system, which goes beyond being a target of a nuclear 1st strike attack. In this case, the destruction could be caused by cyber-attacks could be within the realm of possibilities that could inspire these states to use nuclear warfare in response to a destructive cyber-attack targeting their nuclear arsenal.

6. Current International Climate

Additionally, it is important to examine the current political climate in the international community to understand the use of cyber warfare and the potential for nuclear attacks as well. One of the most notable conflicts as of 2022, is the war between Russia and Ukraine. Russia's invasion of Ukraine that took place on February 24, 2022 and can be seen as a prime example of an unjustifiable starting of conflict by a majority of the international community. Russia's interest in the territory of Ukraine that it claims to be its own, is being used to justify the war and ignore the fact that Ukraine is a recognized sovereign state, which was illegal to invade. In response to Russia's invasion, many states including the United States and its European allies condemned Russia's actions. Ukraine is not a member of NATO; therefore, it is not protected by NATOs nuclear capabilities. However, Ukraine has received aid including conventional weapons and tanks in order to counter Russian attacks. The United States is among many of the countries involved in enforcing sanctions against Russia as a means of punishment for their unlawful war with its neighbouring state. The US and NATOs involvement has led President Vladimir Putin to threaten the use of a first strike and the use of strategic nuclear weapons.

Another rouge state actor contributing to today's highly charged political climate is North Korea under the leadership of Kim Jong Un. North Korea is the latest state to obtain nuclear weapons and has gone against international taboos with the creation of its program and continued nuclear, and ballistic missile testing. The nuclear demonstrations practiced by North Korea has become a form of nuclear terrorism which flaunts their access to deadly weapons in order to deter any potential threats to their sovereignty and security. North Korea continues to be motivated to maintain its nuclear arsenal because of the power all nuclear states hold. For example, a state with nuclear weapons has never been invaded (Ong 2016). Although, this statement is true, the use of cyberwarfare creates a new means of invasion without troops stepping foot onto foreign soil. Any country no matter its military strength, can be affected by cyberwarfare and how they choose to respond to this threat can vary depending on regime type. Any rouge actor, like North Korea, might be quick to respond to a cyberattack with nuclear warfare in order to not appear weak to the international community.

China is another current international actor that should be monitored for both its cyber and nuclear attack capabilities. On one hand, China is extremely well-versed in terms of cyber activities as it has conducted many cyber-attacks for its own national interests. For example, these attacks have targeted the United States government and many other industries including, healthcare, education, energy, and trade, and as a result continues to be a creditable threat to international security (CISA 2022). In addition, the US Defence Department reports that China is rapidly increasing its nuclear weapons arsenal. The report suggests that by 2030 China will have roughly 1,000 nuclear warheads, which is a nearly 300 percent increase of its current stockpile (Bugos 2021). Although China has not openly threatened the use of its nuclear weapons, officials are concerned about China's possible plans of expansion, which seem to include invading Taiwan (Bugos 2021). An invasion of Taiwan would likely result in a similar reaction by the international community to Russia's invasion of Ukraine, This would mean we could see sanctions or cyber-attacks directed at China. Then, depending on how threatened China is by the international response, they could decide to use strategic nuclear weapons.

7. Conclusion

Today's international political climate shows that there is a rise in international tensions from various threats, both from state and non-state actors. The institutions that have been put in place to try to further mitigate deadly conflicts and prevent states from being able to justify wars are arguably becoming less effective. From a realist perspective, just warfare is no longer being considered in conflicts because a state's own interest takes precedence. Technological advances mixed with complicated international relations continue to cause tensions between states and between state and no state actors which increases the possibility of the use of cyberwarfare. Although cyberwarfare is not a conflict in the traditional sense of a physical conflict, it can be perpetuated by both state and non-state actors. To date although there have been a number of incidents that show the potential for inflicting kinetic damage through cyber means (i. e. Stuxnet) no cyber actions have caused physical death. Cyber warfare has the potential when the proper targets are identified, to cause just as much damage to a society as combat warfare. Additionally, states have been more reluctant to implement nuclear policies, such as no first use, and hesitant to adopts treaties that prevent the use of nuclear weapons, like the Treaty on the Prohibition of nuclear weapons (TPNW). Access to nuclear weapons, whether through a state's own arsenal or an ally's, has become a symbol of ultimate security. However, due to the emergence of cyber threats there can no longer be a guarantee of a state's security because even nuclear systems could be a potential target of an adversary's cyberattacks. All of these factors combined could lead to a variety of dangerous outcomes that could potentially include the use of nuclear warfare as a response to a cyber-attack.

It is important to look at this anticipatory research now to better understand the various factors that states might consider amidst a cyber-attack and how to prevent the use of nuclear weapons. Nuclear threats will continue to remain as long as nuclear weapons exist. Therefore, policies must be examined to implement international taboos that make states feel secure and eventually promote nuclear disarmament. For example, the creation of a universal "no-first use" policy would ensure that states will never use their nuclear weapons as a first strike offensive thus reducing the possibility of a nuclear response to a cyber-attack. Perhaps an analogue to this nuclear no first use policy for nuclear weapons needs to be extended and applied to cyberattacks upon adversary's nuclear systems. The no first use policy for nuclear weapons needs to be applied to cyberattacks in order to develop a no first use policy related to cyber- attacks upon an adversary's nuclear systems.

References

Atomic Heritage Foundation. 2017. "The Manhattan Project." *Atomic Heritage Foundation.* https://www.atomicheritage.org/history/manhattan-project (November 15, 2022).

Atrews, RA. 2020. "Cyberwarfare: Threats, Security, Attacks, and Impact." *Journal of Information Warfare* 19. no. 4. 17-28. JSTOR. (November 15, 2022).

Brunstetter, Daniel, and Megan Braun. 2013. *Ethics and International Affairs* 27. no.1. 87-106. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/38F9679507EBFD40E883CFADCC271F27/S0892679412000792a.pdf/from_jus_ad_bellum_to_jus_ad_vim_recalibrating_our_understanding_of_the_moral_use_of_force.pdf (December 7, 2022).

Burr, William. 2020. "The Atomic Bomb and the End of World War II." *National Security Archive.* https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2020-08-04/atomic-bomb-end-world-war-ii (November 15, 2022).

Center for Arms Control and Non-Proliferation. n.d. "No First Use." *Center for Arms Control and Non-Proliferation.* https://armscontrolcenter.org/issues/no-first-use/ (November 12, 2022).

Center for Strategic and International Studies. 2022. "Significant Cyber Incidents." *Center for Strategic and International Studies*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (November 15, 2022).

Chan, Melissa. 2019. "What is the Difference Between a Hydrogen Bomb and an Atomic Bomb?" *Truman Library.* https://www.trumanlibrary.gov/public/2019-10/Development%20of%20the%20Hydrogen%20Bomb-%20Document%20Set.pdf?VersionId=TIums5XoxSxXDVHA.MGW8aqOO6IZItZ2 (November 15, 2022).

Cybersecurity and Infrastructure Security Agency. 2022. "China Cyber Threat Overview and Advisories." *Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/uscert/china (December 7, 2022).

Dever, John, and James Dever. 2013. "Cyberwarfare: Attribution, Preemption, and National Self Defense." *Journal of Law and Cyber Warfare* 2. no. 1. 25-63. JSTOR. (November 15, 2022).

Global Zero. n.d. "No First Use FAQs." *Global Zero.* https://www.globalzero.org/no-first-use-faqs/ (November 15, 2022).

Hatch, Benjamin B. 2018. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." *Journal of Strategic Security* 11. no.1. 43-61. JSTOR. (December 7, 2022).

International Campaign to Abolish Nuclear Weapons. n.d. "The Road to a World Free of Nuclear Weapons." *International Campaign to Abolish Nuclear Weapons.* https://www.icanw.org/nuclear_weapons_history (November 15, 2022).

International Committee of the Red Cross. 2015. "What are jus ad bellum and jus in bello?" *International Committee of the Red Cross.* https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 (December 7, 2022).

International Committee of the Red Cross. 2021. "Cyber Warfare: Does International Humanitarian Law Apply?" *International Committee of the Red Cross.* https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law (December 7, 2022).

Internet Encyclopedia of Philosophy. n.d. "Just War Theory." *Internet Encyclopedia of Philosophy.* https://iep.utm.edu/justwar/#H3 (December 7, 2022).

National Public Radio. 2015. "Why Did the U.S. Choose Hiroshima?" *National Public Radio.* https://www.npr.org/2015/08/06/429433621/why-did-the-u-s-choose-hiroshima (November15,2022).

Nuclear Threat Initiative.2020."The Cyber-Nuclear Threat." *Nuclear Threat Initiative.* https://www.nti.org/analysis/articles/cyber/ (December 7, 2022).

Nussbaum, Arthur. 1943. "Just War: A Legal Concept?" *Michigan Law Review* 42. no. 3. 453-479. JSTOR. (December 7, 2022).

Schmitt, Michael N. 2003. "International Law and the Use of Force: The *Jus Ad Bellum." Connections* 2. no. 3. 89-97. JSTOR. (November 15, 2022).

United Nations Office for Disarmament Affairs. n.d. "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)." *United Nations Office for Disarmament Affairs.* https://www.un.org/disarmament/wmd/nuclear/npt/ (December 7, 2022).

Zhao, Tong. 2021. "China and the International Debate on No First Use of Nuclear Weapons." *Asian Security* 18. no.3. 205-213. https://www.tandfonline.com/doi/abs/10.1080/14799855.2021.2015654?src=&journalCode=fasi20 (November 15, 2022).

Walzer, Michael, Just and Unjust Wars: A Moral Argument with Historical Illustrations (New York: Basic Books, 2006 [1977]), pp. xv–xvi Google Scholar.