INSTABILITY IN SECURITY:

A COMPARATIVE ANALYSIS OF COOPERATION IN INTERNATIONAL SECURITY

Sydney Box

A THESIS

Submitted to The University of Michigan

In partial fulfillment of the requirements for the degree of

Honors Bachelor of Arts

Department of Political Science

11 May 2020

Table of Contents

Abstract

Countries across the globe have outwardly called for solutions to the destabilizing threat of cyberwarfare, noting how damning it can be to governments and citizens alike. Throughout history, states have come together after new international threats arise to negotiate some type of agreement or form an international institution to make sure that threat is mitigated. With the new-age peril of cyberwarfare, this has not been the case. If an issue poses such a pervasive threat to every person who has access to technology, arguably more far reaching than any physical war could ever be, why have states not cooperated to regulate cyberweapons in the way we would assume? In particular, my research tackles the following question: why are states willing to cooperate on some security issues and not others? This paper employs a comparative analysis of traditional weapons of mass destruction to better understand what characteristics of certain weapons inhibit international cooperation. I find two situations that affect a state's willingness to cooperate: an understanding of a weapon's consequences, and the strategic value of the weapon. I posit that a state is more willing to cooperate when it understands the weapon's consequences, and the strategic value of the weapon is lower than the value of disarmament. Each of these situations create incentives for states to choose non-cooperation over cooperation. I recommend two steps that international decision makers can take to increase the probability of cooperation: the promotion of an international norm against the use of unregulated cyberspace, and fixing the hacker attribution problem in an effort to lower the non-cooperative payoff.

Acknowledgments

I started thinking about this project in the fall of 2017. I learned about cybersecurity in my Polsci 464 class, taught by my advisor Barbara Koremenos. It sparked such a deep-seeded enthusiasm within me that I decided to spend the next two and a half years writing an 80-page thesis on it. To Professor Koremenos, thank you for being my guide and my mentor since freshman year. There are so many things beyond this project that I could not have achieved without your trust and support.

Thank you to Brian Min, leader of our cohort, for being such a stable force and for helping me stay on track when I felt like I was falling off. Thank you to my GSI Michael Lerner for responding to every one of my late-night, panic filled emails with such in-depth and sincere help. I also owe a huge thank you to Iain Osgood for not only being an amazing professor, but also a constant source of encouragement over the past two years. Also, thank you for employing me! Lastly, thank you to the Gerstein Family Research Stipend for giving me the resources I needed to complete this project.

I want to thank my friends from home and from school for cheering me on and being there for me, even when I went off the grid to write – especially the second time around.

To my family - not only while I was working on this thesis, but for the entirety of my time in school, you have been the biggest source of support, love, and encouragement. This thesis is the culmination of four years of hard work, but I could not have even gotten there without you all. This project is as much yours as it is mine. Thank you.

This thesis marks the end of my undergraduate career at the University of Michigan. But, it also has unlocked an academic curiosity in me that I hope to keep chasing for the rest of my life. For that, I am forever thankful.

And forever, Go Blue.

Section I – Introduction

Although an intangible platform, cyberspace is the lifeline that wires this world. In 2020, we are living on the edge of a technological frontier, and the horizon of possibilities is only expanding. The technology through which we access cyberspace has allowed our world to rapidly advance beyond what we thought was possible. With technological advancement, barriers to access technology have all but disappeared. Cyberspace is everywhere, and most of the planet takes advantage of it every day[1][2]. We now live in a global village. Stating that all places on earth are connected through cyberspace is no hyperbole.

However, despite all of the benefits that technological interconnectedness has brought our planet, the potential risks it brings are tremendous. Throughout the past couple of decades, people have used cyberspace as a medium to harm. Today, cyberspace is being harnessed by both private and public actors as a weapon. A lack of cybersecurity has allowed people to use cyberweapons to commit acts that are illegal in the physical world. The increase in cyber-attacks has brought to the forefront the treacherous consequences of the unregulated use of cyberspace. It poses a pervasive threat to every person who has access to technology, arguably more far reaching than any physical war could ever be. If you do not think that you are at risk of being a target of a cyberweapon, you are wrong.

The possible consequences of unregulated cyberspace use are critical enough to cause alarm. Most alarming is the alleged weaponization of cyberspace by nations for

[1] "GSMA Intelligence." Accessed December 3, 2019. https://www.gsmaintelligence.com/.
[2] "Statistics." Accessed December 3, 2019. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

use against other states. States using cyberweapons against other states constitutes cyberwarfare. Two prominent examples are Stuxnet, which targeted Iran's nuclear program, and the alleged interference of the 2016 United States (US) Presidential Election. In both of these cases, a state has been accused of violating the sovereignty of another state by illegally meddling in its affairs. These actions are illegal under existing international law, specifically the Charter of the United Nations (UN). However, the existing body of international law does not regulate states' use of cyberspace, even though cyberspace is a medium through which states take actions that violate existing international law.

Throughout history, when states have faced a threat untouched by international law, they have come together to negotiate some type of hand-tying agreement or form an international institution for the sake of international security. This has occurred in many areas, especially the three weapons of mass destruction (WMD) that this paper analyzes: nuclear weapons, chemical weapons, and biological weapons. I conceptualize cyberweapons as a new age WMD due to its potential to harm millions of people not directly engaged in conflict. One would assume that because of these similarities, we would see a similar cooperative landscape. However, that is not the case. States have continuously noted how damning a lack of security in cyberspace is to governments and the citizens within their borders. World leaders call for solutions in many international forums, specifically the UN. Specifically, states have called for guidelines on responsible state behavior in cyberspace. Given the public outcry and apparent sense of urgency, it is surprising that states have not yet reached some type of cooperative agreement that ties their hands to freely using cyberspace without rules.

I aim to figure out why states have not reached a hand-tying international agreement on cybersecurity – what we assume would happen. To do this, I seek to

understand what makes a state willing to enter into a cooperative agreement. Intuitively, if states are more willing, then it is more likely that the cooperative outcome will be reached, and vice versa. This view has prompted my research question: why are states willing to cooperate on some security issues and not others? Understanding why cooperation lends itself to security issues more broadly will allow me to critically analyze the specific case of cybersecurity. Cyberspace is just another medium to commit crimes, making it no different than the physical world. The dependent variable I am measuring is state cooperation. I define state cooperation as a binary variable with two potential outcomes: the existence of cooperation, or no cooperation.

I take a treaty-based approach to cooperation. In this paper, cooperation is defined as the act of reaching an international agreement that ties a state's hands regarding the proliferation or use of a certain weapon. Proliferation activities include development, production, stockpiling, and transfer of the weapon[3]. The exact moment in time where cooperation is triggered is when the final form of an agreement is agreed upon by negotiating states and opened for signature. I qualify a cooperative outcome as the result of states working together to produce an international agreement, rather than the act of reaching the agreement. The non-cooperative outcome is the default and represents a world where states have not agreed to enter into a cooperative agreement.

Roadmap of the Paper

It is important to note that there can be many types of cooperation on a security issue. This paper seeks to specifically understand what affects a state's willingness to cooperate on disarmament at the state level. I hypothesize that there are characteristics

[3] International disarmament does not only focus on banning the use of a weapon. It puts just as much importance on eliminating the development, production, stockpiling, and transfer of weapons.

of certain security issues that affect a state's willingness to enter into a cooperative agreement when that agreement requires a state to tie its hands. When a state ties its hands, it commits to not take a particular action in the future. In doing so, it subjects itself to international scrutiny that it will uphold that promise, or face some type of punishment. Each of my two hypotheses suggest that the existence of different characteristics inherent to security issues change a state's willingness to commit to tie its hands. To test this, I employ a comparative analysis of cyberweapons and three traditional weapons of mass destruction (WMD): nuclear weapons, chemical weapons, and biological weapons. There is a plethora of security issues, but I argue that cyberweapons are a new-age WMD, and thus use traditional WMD as a proxy for cyberweapons in order to test my hypotheses.

In the next section, I further delve into the issue of cybersecurity and the existing conversations on cybersecurity cooperation. I additionally attribute the relevant literatures that allow me to properly test my hypotheses. In Section III, I will detail my conceptualization. Since cyberspace is a non-traditional arena of war, the understanding of cyberspace as a cyberweapon – comparable to weapons of mass destruction - is the most integral part of my paper. I argue why that is necessary and justified in this section. In Section IV, I will outline my methodology and provide justification for my research design. I use process tracing to test Hypothesis 1, and my own methodology to test Hypothesis 2[4]. I use the collective action stag hunt game to analyze the real-world implications of my findings. The background information of my case studies appear in Section V. Section VI will be where I do that actual task of process tracing for my hypotheses.

[4] See Appendix B

The Hypotheses

H1: Understanding a weapon's consequences makes states more willing to cooperate

I hypothesize that when states understand the consequences of a weapon, they are more willing to cooperate to avoid the potential consequences of that weapon's unregulated use or proliferation. Entering into a cooperative disarmament agreement circumvents the potential catastrophe of a lack of regulations by codifying a set of rules that tying states' hands. I posit that the need for this outcome is realized through understanding consequences, and it strengthens the urgency of cooperation.

H2: If the strategic value of a weapon is low, states are more willing to cooperate

I hypothesize that the strategic value of a weapon affects a state's willingness to enter into cooperative agreements. A state no longer enjoys the value that a weapon brings if it enters into a cooperative agreement limiting its relationship to the weapon. If the value of the weapon is high, states might be less likely to want to give up the value it believes it will receive. On the flip side, as the value of the weapon gets lower, states might be more willing to give it up.

Each hypothesis is tested individually as if we live in a world where that specific hypothesis holds true, barring consideration of the rest. However, I propose my two hypotheses because I believe an understanding of the consequences and a low strategic value affect a state's motivation to cooperate such that these conditions are necessary for a state to be willing to cooperate. Hypothesis 1 stemmed from my curiosity into why states have not cooperated on an issue that they claim has grave consequences with no

cooperation. That led me to propose Hypothesis 2 – I wondered if there was something about the payoff structure for this strategic interaction that was creating that outcome. It is important to note that in my hypotheses, I say that cooperation becomes more or less likely, rather than will or will not occur. There may be a plethora of factors affecting a state's willingness to cooperate. I am not able to make a definite assertion just by considering two variables.

The evaluation of collected evidence reveals that we have reason to believe both Hypothesis 1 and Hypothesis 2 are at play. In Section VII, I evaluate the current state of cybersecurity to see where the cyber domain differs from traditional WMD. Overall, I find that the causal mechanism proposed in Hypothesis 1 is affirmed in cybersecurity, but Hypothesis 2 is not. This leads me to believe that the causal link found in Hypothesis 1 is not strong enough to overcome the issue that an absence of Hypothesis 2 poses, thus making the existence of both a necessary condition. I conclude my paper by explaining the real-world implications of my hypotheses in Section VIII. To lower the strategic value of cyberweapons and increase the likelihood of reaching the cooperative outcome, I propose action items as reasonable next steps. I propose that states work towards solidifying acceptance for the norm against unregulated cybersecurity and international information sharing to fix the "hacker attribution" problem. This is my biggest contribution to the conversation - identifying what affects a willingness to cooperate allows us to make educated assumptions on the probability of cooperation. Variables that hinder cooperation can be manipulated to aide in cooperation. whereas variables that hinder cooperation can be circumvented. Policy proposals are integral in a field that has few, but needs many. The sooner governments can act, the sooner we can make headway on securing cyberspace.

Section II – Cybersecurity in the Literature

In this section I take a closer look at how the issue of cybersecurity has developed over the decades. I also review the current landscape of cooperation and its literatures. Relevant definitions are located in Appendix A.

History of the problem

Over the past couple of decades, cybersecurity has grown from an interest in small academic communities to a mainstream issue. The awareness of cybersecurity grows with the world's continuously increasing reliance on technology. As new technology emerges to the public, so do new threats. Cybersecurity as a field originated as an academic curiosity into cybercapabilities that was pervasive throughout the 1970s and 1980s[5]. The first known worm was created in 1971. It was not a harmful worm, but rather an experiment to see if a computer program could transcend a single system to a larger computer network[6]. Throughout the 1970s and 1980s, various malwares were created as a result of similar inquiries into the capabilities of computer technology. In 1988, Robert Morris designed a worm that was meant to measure the scope of the internet by counting network connections. A programming error caused the worm to accidentally replicate and overwhelm the machines it infected, causing sectors of the internet around the world to slow down and even crash completely[7]. The Morris worm opened Pandora's Box – it led to a dangerous interest to see if deadlier and more effective worms and viruses could be created. Throughout the 1990s, there was a sharp

[5] Mutune, George. "The Quick and Dirty History of Cybersecurity." *Cyber Experts*, July 21, 2019. https://cyberexperts.com/history-of-cybersecurity/.
[6] Ibid.
[7] Middleton, Bruce. *A History of Cyber Security Attacks: 1980 to Present.* Boca Raton, FL: CRC Press, 2017.

rise in the number of new malwares that were stronger and bigger in scope[8]. This proliferation also led to the creation and popularity of computer security and protection software – the crux of cybersecurity.

At the beginning of the 21st century, the understanding of cybersecurity grew as the cybercapabilities created consequences that transcended cyberspace into the real world. Between 2005-2007, a cybercrime syndicate ran an operation in the US that compromised credit card information from millions of people, bringing millions in profit to the hacking group[9]. This was the first major use of malware for financial gain. More recently, Cambridge Analytica illegally harvested personal data from 87 million unsuspecting Facebook users[10]. This massive breach of personal data hit home how vulnerable people are when relying on technology in their day to day lives. As a response to these threats, countries enacted domestic cybercrime laws. Many countries have even created specific governmental departments that focus specifically on cybersecurity. As of April 2020, 79% of countries have domestic cybercrime laws[11] (cite).

Although domestic efforts are important, cyberspace transcends national borders. It creates global problems that need global solutions. In 2010, the virus Stuxnet destabilized parts of Iran's nuclear program by shutting down machines that were used to enrich uranium. This led to a public understanding that cyberspace could be harnessed to cause physical destruction[12]. Three years earlier, Estonia's most important websites were hit with a denial of service (Dos) attack that was allegedly a Russian

---

[8] "The History of Cybersecurity | Cybersecurity Degree Programs." Accessed April 28, 2020. https://www.coloradotech.edu/degrees/studies/information-systems-and-technology/cybersecurity-history.
[9] Middleton, Bruce. *A History of Cyber Security Attacks: 1980 to Present*. Boca Raton, FL: CRC Press, 2017.
[10] "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times." Accessed May 10, 2020. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[11] "UNCTAD | Cybercrime Legislation Worldwide." Accessed April 28, 2020. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.
[12] 60 Minutes: Stuxnet (Columbia Broadcasting System, 2012), https://search.alexanderstreet.com/view/work/bibliographic_entity|video_work|2856063)

backed attack as a result of a skirmish between native Estonians and ethnic Russians[13]. Six years after Stuxnet, Russian state-backed hacking groups launched an information warfare campaign to influence the outcome of the 2016 US Presidential Election. These three instances together alerted the world that cyberspace could be weaponized by states to interfere with another state's sovereignty[14].

This posed a major problem because cyberspace was being weaponized to take an action that is illegal under existing international law. The UN Charter makes it illegal to interfere in the sovereignty of another state. As long as there is no cybersecurity international law, the most dangerous cyberweapons are available for governments to use against each other or global citizens. Effectively mitigating the risks that unregulated cyberspace poses requires regulation of state behavior in cyberspace that is consistent with regulations in the physical world. Thus, reaching a hand-tying agreement is integral.

Current Landscape of Cooperation

This paper sets out to explain why cooperation that ties a states' hands has not been achieved. It would be remiss to equate this type of cooperation with other forms of cooperation on the issues. There are many types of responses to these problems - disarmament is just one route to global problem solving. States are just one of the many actors that share cyberspace. There are other necessary forms of cooperation that help mitigate the risks cyberweapons pose from other actors like individuals, businesses and non-state groups. These include information sharing and fact-finding, harmonizing domestic laws and standards, and participation in international organizations and

[13] Rueter, Nicholas C. "The Cybersecurity Dilemma," 2011, 72.
[14] The perpetrators of these two instances have only been alleged.

institutions. The current landscape of cybersecurity cooperation aligns more closely with those aforementioned characteristics.

The Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention, is the only binding international agreement on the issue of cybersecurity[15]. The two main goals of the Convention are to achieve a higher level of protection against cybercrime globally and foster international cooperation. States parties agree to fortify substantive domestic criminal and procedural law regarding offenses committed in cyberspace[16]. Parties to the Convention also bind themselves to cooperate with other parties on investigations, proceedings, and evidence collection related to these now criminal offenses[17]. The Convention, which entered into force in 2004, takes sound steps to mitigating cybersecurity risks internationally by committing countries to give legal protection to their citizens from offenses committed in cyberspace.

The Convention entered into force in 2004. Since then, the majority of similar cooperation has rested within international organizations. The International Telecommunications Union (ITU) is the main forum for states to work together to cooperate on cybersecurity. The ITU has a Global Cybersecurity Agenda (GCA) provides a "framework for international cooperation aimed at enhancing confidence and security in the information society"[18]. The five pillars of the GCA are legal framework, technically measures, organizational structures, capacity-building, and international cooperation[19]. Each of these pillars provides recommendations on how to

---

[15] "Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." *International Legal Materials* 20, no. 2 (March 1981): 317–25. doi:10.1017/S0020782900032873.
[16] Ibid.
[17] Ibid.
[18] "ITU Global Cybersecurity Agenda (GCA) - Background Information." Accessed May 10, 2020. https://www.itu.int/osg/spuold/cybersecurity/gca/pillars.html.
[19] Touré, Dr Hamadoun I. "ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)," n.d., 21.

mitigate cybersecurity risks internationally and nationally. The GCA provides guides for international and national implementation of cybersecurity measures it approaches the problem on domestic and international levels, and engages states, international organizations, domestic organizations, and the public[20]. The ITU is focused on strengthening the security of information and technology systems. This is an important aspect of mitigating the use of cyberspace as a weapon. However, the ITU focuses more on promoting cooperation on capacity building than disarmament.

The United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is the main international forum for creating hand-tying international cybersecurity law. The GGE is mandated to advance responsible state behavior in cyberspace in the context of international security[21]. The GGE is the forum for states to promote their norms for cyberspace, and to form rules regarding how states should behave in cyberspace[22]. Its most notable achievement came in 2013 when the group published a report decided that the UN Charter, and relevant international law, can apply in cyberspace[23]. The GGE also stressed that the application of relevant international law statutes and norms is an essential cooperative measure to reaching cyber threat elimination[24]. The GGE's 2016-2017 session resulted in an inability to agree

---

[20] Ibid.
[21] "UN GGE and OEWG | GIP Digital Watch Observatory for Internet Governance and Digital Policy." Accessed October 8, 2019. https://dig.watch/processes/un-gge.
[22] "The UN's Group of Governmental Experts on Cybersecurity." *Council on Foreign Relations*. Accessed May 10, 2020. https://www.cfr.org/blog/uns-group-governmental-experts-cybersecurity.
[23] General Assembly resolution 68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
A/RES/68/98 (24 June 2013), available from undocs.org/A/68/98
[24] Ibid.

on a report explaining explicitly how international law applies to cyberspace. This outcome was hailed as the "death of the GGE"[25].

The failure of the GGE to reach an agreement stalled the conversation on cooperation that was greatly needed. In 2019, the GGE was revived, along with an Open-Ended Working Group (OEWG) on cyberspace. The GGE consists of 25 selected member states, and the OEWG involves all interested parties. The OEWG is the forum for interested stakeholders, including business, academia, and NGOs, so the UN can reach a better-informed agreement[26]. Both groups aim to solidify norms, rules, and principles for state use in cyberspace considering both international security and international humanitarian law. The GGE and the OEWG will report their findings back to the UN General Assembly (UNGA) in 2021 and 2020 respectively[27]. The GGE and the OEWG are the forums through which states will reach the cooperative outcome that I conceptualize. The Budapest Convention and the ITU represent other types of cooperation that while important in securing cyberspace as a whole, do not focus on hand-tying agreements at the state level that I believe are integral to mitigating the risk that cyberweapons pose.

Cooperation in the Literature

There are many different cooperative obstacles proposed in the conversation on cybersecurity. Bradshaw (2015) highlights a lack of trust between actors as a major roadblock to cooperation[28]. Bradshaw posits that computer security incident response

---

[25] "The Year in Review: The Death of the UN GGE Process?" *Council on Foreign Relations*. Accessed May 10, 2020. https://www.cfr.org/blog/year-review-death-un-gge-process.
[26] "UN GGE and OEWG | GIP Digital Watch Observatory for Internet Governance and Digital Policy." Accessed October 8, 2019. https://dig.watch/processes/un-gge.
[27] Ibid.
[28] Bradshaw, Samantha. "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," n.d., 24.

teams (CSIRTS) are the key actors in international cooperation to secure cyberspace. CSIRTS around the world work together to respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training[29]. CSIRTS are just one of many actors in the cyber-complex, each with varying preferences. Bradshaw suggest that the high number of actors with varying interests results in a lack of trust among the parties, which hinders information sharing and collaboration among CSIRTS[30]. These are characteristics of a distribution problem, according to Koremenos (2016)[31]. Cho and Chung (2017) also suggest a distribution problem is affecting cybersecurity cooperation. They posit that states consider domestic strategy and policy to be more important than international diplomacy. Differences in the culture, politics, and history of countries forges differences in each countries approach to cybersecurity[32]. Cho and Chung highlight the discrepancies between the US and European Union (EU) countries, and Russia and China in terms of what each believes is the correct approach to cybersecurity. Their paper concludes that because these countries are world leaders, especially in cyber power, cooperation will be very challenging unless their approaches to the problem converge[33].

The two aforementioned views in the literature are emblematic of the competitive, rather than collaborate nature of cyberspace. Bradshaw suggests that the commodification of cyber vulnerabilities and states' attempts to exert power in the cyber domain make for a competitive environment[34]. Reuter (2014) agrees that the

---

[29] Ibid.
[30] Ibid.
[31] Koremenos, Barbara. *The Continent of International Law: Explaining Agreement Design*. Cambridge: Cambridge University Press, 2016. doi:10.1017/CBO9781316415832.
[32] Cho, Yoonyoung, and Jongpil Chung. "Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity." *Pacific Focus* 32, no. 2 (2017): 290–314. doi:10.1111/pafo.12096.
[33] Ibid.
[34] Bradshaw, Samantha. "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," n.d., 24.

nature of cybersecurity is too competitive to make room for successful cooperation. He attributes the security dilemma to the cyber domain[35]. The crux of the security dilemma is that a state might want to increase their defensive military power so it can feel more "secure". This armament may make another state feel less "secure" because states cannot be sure if another state is arming itself for offensive or defensive purposes. The uncertainty about another state's intentions fosters a race for military power that makes cooperation much harder. Reuter acknowledges that this problem is worse in cybersecurity because the non-material nature of cyberweapons makes it nearly impossible for states to know if a state has offensive intentions[36]. This finding is an important implication for the application of game theory to cybersecurity cooperation, as detailed in the next Section.

Chernenko, Demidov, and Lukyanov (2018) provide long-term cooperation recommendations to establish cybersecurity[37]. Their two main long-term goals are creating an international cyber court or similar body to give states a forum to deal with government level-cyber conflicts and to codify cyberattack legislation into international law in the form of a binding convention. These goals are shared by most cooperative efforts such as the GGE, OEWG, and ITU GCA[38]. They (2018) went further to establish short term goals that would help reach their proposed long-term goals[39]. These include restarting the US-Russia dialogue, requiring state reporting of discovered cyber vulnerabilities, starting discussions on a global cybercrime convention, and making cyber incident attribution easier[40]. I agree that these are all steps that need to be taken to

[35] Rueter, Nicholas C. "The Cybersecurity Dilemma," 2011, 72.
[36] Ibid.
[37] "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." *Russia in Global Affairs*. Accessed April 4, 2020. https://eng.globalaffairs.ru/articles/increasing-international-cooperation-in-cybersecurity-and-adapting-cyber-norms/.
[38] Ibid.
[39] Ibid.
[40] Ibid.

ensure cooperation. However, there is no acknowledgement that many of these action items are easier said than done.

Hollis and Waxman (2017) focus on overcoming many of the obstacles to cooperation that make Chernenko, Demidov, and Lukyanov's proposals difficult to achieve[41]. Hollis and Waxman evaluate the Proliferation Security Initiative's (PSI) framework as a guide to furthering cooperation on cybersecurity. The PSI is an initiative created in 2003 to "strengthen the political commitment… and legal authorities necessary to stop, search, and seize vessels suspected of transporting weapons of mass destruction and related materials"[42]. The PSI's cooperation mechanisms are simply a list of actions that participating states are asked to endorse. This approach to cooperation is known as cooperation by a "coalition of the willing". The authors argue that states can successfully implement this format when dealing with cyber threats because the dynamic nature of cybersecurity requires flexibility[43]. Commitment by those that are willing can promote plurilateral cooperation in an area where multilateral cooperation has not been successful. There are merits to a coalition of the willing approach – it starts to fill empty pockets. While it surely takes steps in the right direction, commitment to a multilateral international agreement is necessary in securing cyberspace.

There are many perspectives in the literature that address what is hampering states' abilities to reach a cooperative outcome, despite the forum to do so. Each of these viewpoints has its merits. Complex problems such as international cooperation require multiple approaches. I do not attempt to refute these perspectives, but rather offer a

[41] Hollis, Duncan B, and Matthew C Waxman. "Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)," 2017, 14.
[42] Ibid.
[43] Ibid.

new one. My comparative perspective is unique to the literature, and my hypotheses address characteristics of security issues that I believe are under-discussed. I use WMD as a proxy for cyberweapons because I believe cyberweapons are the new WMD. I hope to start this conversation and bring more political scientists around to my view, which will be discussed in the next Section.

Section III– Conceptualization

The three weapons of mass destruction (WMD) I explore are good case studies to evaluate because states have reached a hand-tying cooperative agreement for each weapon. I use WMD as a proxy for cybersecurity because I conceptualize the cybersecurity issue as an issue of cyberweapons. I first argue that cyberweapons should be regarded in the same manner as traditional WMD. I equate them with WMD due to its similar disruption of the traditional concept of war, and its potential for mass harm. I hypothesize that there are characteristics inherent to WMD that affect a state's willingness to enter into a hand-tying cooperative agreement. I can apply that analysis to cyberweapons in order to deduce why states have not reached a hand-tying cooperative agreement on cyber yet. The second part of my conceptualization reviews the importance of applying international legal frameworks to cyberweapons.

Rectifying the Difference Between Traditional Weapons and Cyberweapons

A key distinction between cyberweapons and traditional weapons of mass destruction is that the former is intangible, while the latter is physical. Beyond the intangibility of a weapon, cyberweapons are fundamentally the same as traditional weapons. Much like nuclear, biological, and chemical weapons, cyberweapons are

created from a medium that can bring a lot of benefits. Nuclear weapons come from a technology that can be used to create clean energy. The precursors for chemical and biological weapons are used to advance scientific discoveries that save lives. Cyberspace similarly allows the creation of technology that has advanced the quality of life of society. All of these mediums can bring a lot of good, but have the potential to be misused and turned into a weapon.

We have seen essentially the same problem come up in history a couple of times before: a new type of weapon threatening the traditional arena of war appears. Like traditional weapons of mass destruction, cyberweapons function in a way that has not been seen in the field of war before. Once cyberweapons became known, relevant actors explored their implications on war. But unlike conventional weapons, weapons of mass destruction have grave implications for society at large. The discoveries of the destructive capabilities of cyberweapons - namely their ability to remotely target a mass of people around the world has led many to call for limitations on its use. Hypothesis 1 shows how this process has mirrored that of traditional weapons of mass destruction. Thus, I believe that cyberweapons should warrant the same level of concern and urgency as traditional WMD and should be treated as such.

Cyberspace is an entity that is shared by all countries. While each country has jurisdiction over the infrastructure that connects them to cyberspace within their borders, no one state has cyberspace as their specific domain. There are no borders in cyberspace. This is very different from physical war, which is regulated to obey physical borders. But, cyberspace is actually very similar to air, sea, and space. Each of these three mediums has space that is not owned by any government. States have collaborated on international law regulating state behavior in these “common spaces”.

Cybersecurity is very similar to that, and thus warrants the same standard for applying international law.

Application of International Legal Norms

International law has a well-defined framework for dealing with warfare itself and the mediums through which states wage war. Looking towards existing international legal frameworks is a way to better understand how to reach international cooperative agreements in new mediums. The multilateral fora for dealing with cyberweapons has fallen under disarmament branches, such as the United Nations Office of Disarmament Affairs (UNODA) and the Disarmament and International Security Committee (DISEC). Within each of these disarmament fora, states have agreed that international law can be applied to cyberspace. The traditional weapons of mass destruction are regulated under international disarmament law, which was cemented in the aforementioned disarmament fora. The 1868 St. Petersburg Conference was the catalyst for international disarmament cooperation. The main takeaway from the conference was that any weapon that caused useless enhancement of pain and suffering or unnecessary death is a violation of humanitarian principles. Thus, any such weapon should be outlawed[44]. Traditional weapons of mass destruction were outlawed under this principle. Cyberweapons have the capability to take on these characteristics, and with constant advancements of technology, the destructive capabilities are unknown. Threat assessments predict that the next major international crisis could realistically be

[44] "1868 Saint Petersburg Declaration | Weapons Law Encyclopedia." Accessed April 4, 2020. http://www.weaponslaw.org/instruments/1968-Saint-Petersburg-Declaration.

a result of the weaponization of cyberspace[45]. This possibility warrants approaching cybersecurity as a traditional disarmament issue.

Arguably the most important piece of literature in this regard comes from the Group of Governmental Expert's 2013 meeting. The GGE is a UN mandated working group acting in the field of information security. Its most notable achievement came in 2013 when it published a report linking international law to cyberspace[46]. In the report, the GGE stressed the need for cooperation among states to combat future cyber threats. The group then affirmed that the application of relevant international law statutes and norms is an essential cooperative measure to reaching cyber threat elimination[47]. The GGE aims to provide an explicit framework for how to apply international law to the cyber domain during its 2019-2021 session[48]

Puyvelde and Brantly (2017) take a step to answer the "how" question[49]. The authors argue that states need to apply specific parts of the UN Charter when writing international cyberwarfare law. Article 2(4) of the Charter says all members shall "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state"[50]. Conversely, Article 51 of the Charter confirms the right to "individual or collective self-defense" in the face of armed attack[51]. The main takeaway from the Charter is that nation-states should refrain from

---

[45] "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." *Russia in Global Affairs*. Accessed April 4, 2020. https://eng.globalaffairs.ru/articles/increasing-international-cooperation-in-cybersecurity-and-adapting-cyber-norms/.
[46] General Assembly resolution 68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
A/RES/68/98 (24 June 2013), available from undocs.org/A/68/98
[47] Ibid.
[48] General Assembly resolution 68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
A/RES/68/98 (24 June 2013), available from undocs.org/A/68/98
[49] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[50] U.N. Charter art. 2,¶ 4.
[51] Ibid. art. 51

aggression, but the use of force is appropriate in the face of an attack[52]. These existing guidelines apply to physical war, which has characterized the traditional arena of war throughout history. Cyber and physical are two different types of warfare that are fought in different arenas. Nevertheless, they are both warfare, and should be regulated as such. Puyvelde and Brantly propose that in order to be able to move forward with cybersecurity cooperation, states need to rework these principles in the UN charter to explicitly govern cyberspace[53].

States have the capabilities to harness cyberspace in the form of a dangerous weapon, and the threat remains unfettered until disarmament law is reached. With traditional WMD, states came together to collectively agree to tie their hands, due to the destructive consequences posed by no regulation. These sentiments exist within the realm of cyberweapons, and have been the catalyst for the re-emergence of the GGE and the OEWG[54]. These observations lead me to ask an important question: Why are states not agreeing to collectively disarm or control a dangerous weapon's proliferation despite the fora to do so?

Section IV – Methodology

I use process tracing to test if there is a causal relationship between my independent variables and cooperation. I test my hypotheses on my three traditional weapons of mass destruction case studies. After I collect those findings, I turn to

---

[52] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[53] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[54] "UN GGE and OEWG | GIP Digital Watch Observatory for Internet Governance and Digital Policy." Accessed October 8, 2019. https://dig.watch/processes/un-gge.

cybersecurity to see how the landscape compares to traditional WMD. Finally, I use game theory to explain how the existence of those causal mechanisms actually impacts the likelihood that states enter into a cooperative agreement.

Process Tracing

To answer my research question, I have to gain insight into the nature of causal relationships. This rather exploratory quest guided me to process tracing as a means of hypothesis testing. Process tracing is the practice of tracing a process from a hypothesized cause to a specified effect in order to find a causal mechanism through which the cause brings about the effect[55]. I follow the framework of process tracing from Beach and Pedersen (2013)[56]. The authors describe a causal mechanism as a causal chain that links an event with an outcome. Each piece of the chain represents a snapshot of events that need to exist in order to show there is a direct impact from the event to the outcome. These events are clues that the hypothesized causal link holds true. Each of these clues is necessary for the hypothesis to hold true because each part of the chain is necessary to link the subsequent parts of the chain. To support the existence of these clues, diagnostic evidence is collected. I collect evidence across my three case studies. The collection of this evidence supports the existence of the clues, and the existence of clues gives us reasonable belief that the hypothesis holds true. If a clue does not exist, it eliminates the hypothesis from contention[57]. Due to the necessity of evidence to support the existence of a clue, finding that evidence signals strong probative value. I do this for

[55] Collier, David. "Understanding Process Tracing." *PS: Political Science & Politics* 44, no. 04 (October 2011): 823–30. doi:10.1017/S1049096511001429.
[56] Beach, Derek, and Rasmus B. Pedersen. *Process-Tracing Methods: Foundations and Guidelines*. University of Michigan Press, 2013.
[57] Ibid.

Hypothesis 1. For Hypothesis 2, I created my own methodology to measure strategic value[58].

The structure I use to represent this process is as follows: presenting the hypothesis, presenting the clue(s), presenting the evidence for the clues. The evidence is labeled by "**Clue number. Weapon type. Evidence number."** NW represents nuclear weapons, CW represents chemical weapon, BW represents biological weapon, and CY represents cyberweapon. For example, nuclear weapon evidence piece 3 for clue two is stylized as "**C2. NW. E3"**.

Game Theory

I use game theory to understand how the results of process tracing affect the equilibrium outcome. I use the mechanisms of the collective action Stag-Hunt game as an analogy of the cooperation landscape today. Working through the game gives us real-life implications that help better understand cooperative dilemmas in international cooperation. Assumptions that the literatures hold true in a game theory analysis are that all players are rational decision makers according to the rational choice theory. As utility maximizing rational agents, the players will choose whatever strategy maximizes their payoff. The players' payoffs are the utility they derive from either of their selected strategies. Payoffs are ranked based off of the welfare that the actor gets from the select strategy after all other players have selected their strategies[59].

The Stag-Hunt represents the dilemma of choosing to take a high-risk action and cooperate for a higher payoff or choose a low-risk strategy, with no cooperation, for a

[58] See Appendix B for the H2 methodology and why I chose to create my own
[59] Von Neumann, John, Oskar Morgenstern, and Ariel Rubinstein. *Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition).* Princeton; Oxford: Princeton University Press, 1944. Accessed April 5, 2020. doi:10.2307/j.ctt1r2gkx.

lower payoff[60]. Jervis (1978)[61] and Engelmann (1994)[62] support the use of the stag hunt to represent real-life dilemmas present in disarmament when states have to agree to tie hands. The dilemma of the game represents the security dilemma that Rueter (2014) poses[63]. In the Stag-Hunt, there are two Nash equilibrium outcomes: the cooperative outcome (the payoff-maximizing outcome) and the non-cooperative outcome (the risk-minimizing outcome). In cooperation on disarmament, the same outcomes exist: the cooperative outcome is reaching a mutual disarmament, and the non-cooperative outcome is unilateral armament[64]. I use the collective action version of the stag-hunt to represent multiple players, and their need to collectively cooperate to reach the cooperative outcome. The states can only reach the cooperative outcome of mutual disarmament if all states choose disarm, just as the stag in the game can only be caught if all hunters choose stag over hare. If at least one state does not agree to cooperate, then the threat of armament lowers the payoffs that all states face. The players in the game are the states trying to reach an agreement. Their available strategies are disarm (hunt stag) or arm (hunt hare).

---

[60] Kydd, Andrew H. "Game Theory and the Future of International Security." *The Oxford Handbook of International Security*, March 15, 2018. doi:10.1093/oxfordhb/9780198777854.013.13.
[61] Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214. doi:10.2307/2009958.
[62] Engelmann, Wilfried. "Conditions for Disarmament: A Game Theoretical Model." *Group Decision and Negotiation* 3, no. 3 (September 1994): 321–32. doi:10.1007/BF01384332.
[63] Rueter, Nicholas C. "The Cybersecurity Dilemma," 2011, 72.
[64] The Prisoner's Dilemma is usually selected to better understand international cooperation. However, the prisoner's dilemma only has one Nash Equilibrium – the non-cooperative outcome. In the prisoner's dilemma, incentives to defect are sufficiently large so that states are mutually best responding when everyone does not cooperate. In disarmament, the non-cooperative outcome is not payoff- maximizing as represented in the Prisoner's dilemma. The stag-hunt more accurately represents the outcomes and payoffs of international disarmament cooperation because it has two outcomes, and the cooperative outcome is payoff-maximizing.

The payoff matrix is as follows[65]:

		State N: Disarm	State N: Arm
State 1	Disarm	A , A	D , B
	Arm	B , D	C , C

The payoff structure that the individual state faces in the game is: $A > B \geq C > D$[66]. The outcome payoff structure that the individual state faces is: $AA > BD \geq CC > DB$. AA is the cooperative Nash equilibrium and CC is the non-cooperative Nash equilibrium. BD and DB represent the out of equilibrium non-cooperative outcomes. Here is what outcome each payoff represents:

AA: all players choose disarm and the **cooperative outcome** of mutual disarmament is reached.

BD: this state chooses to arm, and receives the payoff from armament. At least one other state chooses to disarm.

CC: all states choose arm. Each state receives the payoff from armament and the **non-cooperative outcome** is reached.

DB: this player chooses to disarm. At least one other player chooses to arm, and this player receives a payoff of D=0.

This game has two equilibrium outcomes: AA (disarm, disarm) and CC (arm, arm). At each of these equilibria, the players are mutually best responding to one another and have no incentive to deviate. AA is seen as the payoff-maximizing equilibrium. Each player receives the highest payoff possible by both selecting disarm. CC is the risk

[65] State N represents the actions of the other states. It only takes one state for BD/DB to be reached, which allows for us to use the Nth state as a representation of the "second player" in the game. AA and CC are reached if all states choose disarm or arm, respectively, which is scaled down and represented on the matrix as if "both players" chose to cooperate or not cooperate.

[66] For this analogy, D=0. There is no benefit to disarming if at least one other state chooses to pursue armament.

minimizing equilibrium[67]. Choosing disarm is the riskier strategy because it introduces the chance that at least one other state will choose arm, and the player who chooses disarm gets nothing because the threat associated with armament is not eliminated[68] [69]. If the player chooses arm, they are guaranteed the security benefits that armament brings. These benefits represent the strategic value of the weapon. Thus, the strategic value is represented in payoffs B and C. States may not want to risk giving up that payoff, and would select arm. Therefore, this is seen as a safe, risk-minimizing outcome[70].

The existence of the two equilibrium is at the crux of the cooperation dilemma. What makes a state willing to choose one outcome versus the other? According to utility maximization theory, one would assume states would reach the cooperative outcome AA. An assumption we hold true is: mutual disarmament results in higher payoffs than mutual armament[71]. Disarmament brings international stability and security. Unilateral armament increases the chance of war and conflict, so it has a lower payoff than disarmament. However, no state wants to be the one "tricked" into disarming, while others arm[72]. This situation represents risk-aversion, and make the non-cooperative outcome (CC) more attractive.

In game theory terms, I want to figure out what makes a state willing to take the risk and achieve the payoff-maximizing outcome. I propose my two hypotheses because I believe understanding the consequences, and a low strategic value make a state more willing to do so. Currently, cybersecurity is in the non-cooperative state. I hope to

---

[67] "Game Theory and Disarmament: Thinking Beyond the Table." *E-International Relations*. Accessed May 10, 2020. https://www.e-ir.info/2018/12/18/game-theory-and-disarmament-thinking-beyond-the-table/.
[68] Kydd, Andrew H. "Game Theory and the Future of International Security." *The Oxford Handbook of International Security*, March 15, 2018. doi:10.1093/oxfordhb/9780198777854.013.13.
[69] The payoff of mutual disarmament is represented in the benefits that the elimination of arms brings, such as international stability, peace, and security.
[70] Ibid.
[71] Engelmann, Wilfried. "Conditions for Disarmament: A Game Theoretical Model." *Group Decision and Negotiation* 3, no. 3 (September 1994): 321–32. doi:10.1007/BF01384332.
[72] Ibid.

explain why that is by better understanding if there were certain aspects of traditional WMD that allowed states to reach the cooperative outcome: AA. This is discussed further in the implications section of Section IV.

Section V – Case Studies

I have chosen the traditional weapons of mass destruction (WMD) as my case studies: nuclear weapons, chemical weapons, and biological weapons. The appearance of cyberweapons on the scene makes these three WMDs seem traditional, but there was nothing conventional about nuclear, chemical, and biological weapons when they first proliferated. At each of their respective beginnings, these new types of weapons disturbed the status quo of warfare. This unprecedented entry of each new type of weapon forced the international community to cooperate to better understand the threat, and subsequently agree to disarm. It is important to contextualize cooperation with the history of how the arrival of a new weapon forced the world to reach a cooperative outcome. Each case study begins with a discussion on the history of the weapon and its subsequent introduction into the public discourse. That is followed by a discussion on the period before each respective agreement was reached. We are currently in the pre-treaty world for cybersecurity, so my case studies remain in the pre-treaty worlds for their respective weapons. I conclude each section with a brief overview of each respective treaty to understand what was agreed upon.

Nuclear Weapons: The Treaty on the Non-Proliferation of Nuclear Weapons

The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) is the main international agreement regulating nuclear weapons. It focuses on affirming the non-

proliferation of nuclear weapons and promoting peaceful, rather than harmful, uses of nuclear energy. The NPT was precipitated by a changing international taboo against the use of nuclear weapons[73]. The use of atomic bombs in Hiroshima and Nagasaki signaled the dangers of nuclear weapon proliferation. During the Cold War, the non-use of nuclear weapons rested on the existence of mutually assured destruction (MAD). However, this was fragile, and was threatened by an increase of tensions between the US and the USSR. The Cuban Missile Crisis of 1962, which pushed the world as close to nuclear war as it has ever come, increased the sense of urgency for nuclear non-proliferation. The fear of a nuclear world war was increased by the reality that even more countries would obtain nuclear weapons if nothing was done to stop them. This spurred an anti-nuclear rhetoric that seeped into the international discourse[74]. The fear of nuclear proliferation is expressed well by former US President John F. Kennedy:

> "There would be no rest for anyone then, no stability, no real security, and no chance of effective disarmament. There would only be the increased chance of accidental war and an increased necessity for the great powers to involve themselves in what otherwise would be local conflicts"

On 8 December 1953, then US President Dwight D. Eisenhower gave his "Atoms for Peace" speech to the UN General Assembly. In his speech, Eisenhower admitted that the "dread secret" of atomic weapons no longer belonged solely to the US. During World War II, the US was the only known stockpiler of nuclear weapons, with the two atomic bombs[75]. Eisenhower warned that the knowledge of nuclear weapons was spreading throughout the world, which warranted international concern. After

---

[73] "Treaty on the Non-Proliferation of Nuclear Weapons - Main Page." Accessed February 17, 2020. https://legal.un.org/avl/ha/tnpt/tnpt.html#.
[74] Ibid.
[75] "Atoms for Peace Speech." Text. IAEA, July 16, 2014. https://www.iaea.org/about/history/atoms-for-peace-speech.

Hiroshima and Nagasaki, the world began to realize the infinitely destructive capabilities of nuclear energy, but also the potential for it to be infinitely helpful. Eisenhower called for the creation of an international atomic energy agency that would control the stockpiles of uranium and other fissionable materials necessary for building a nuclear weapon. This agency would also carry out safeguards to promote the sharing of materials and information needed to conduct peaceful nuclear energy research[76]. During this time, there were both domestic and regional agreements on such topics, but the need for an international agency was seen as the primary way to stop the proliferation of nuclear weapons[77].

The International Atomic Energy Agency (IAEA) statute was approved in 1956 and entered into force in 1957 after negotiations precipitated by the US and the UN. Its main objective is to ensure that nuclear activities were being used for peaceful and not military purposes. In 1958, nuclear disarmament was brought up for the first time to the UN. At this time, The Disarmament and International Security Committee (DISEC) along with the Ten Nation Disarmament Committee (TNDC) stressed that a "general and complete disarmament under effective international control" was necessary to halting nuclear proliferation. In 1962, the US and the USSR respectively presented draft treaties on general disarmament, which included provisions on nuclear non-proliferation. It was not until 1964 that it was debated as a topic separate from general disarmament, upon recommendation from the TNDC's successor, the Eighteen Nation Disarmament Committee (ENDC). In 1965, negotiations for a nuclear non-proliferation

[76] Ibid.
[77] Putte, Vande. "International Atomic Energy Agency: Personal Reflections." *Annals of Nuclear Energy* 25, no. 10 (June 1998): 791. doi:10.1016/S0306-4549(97)00121-7.

treaty officially started. That year, the US and USSR respectively introduced the first draft treaties specifically on the non-proliferation of nuclear weapons.

The majority of NPT negotiations were spent reconciling the differing demands of the nuclear weapon states and non-nuclear weapon states[78]. Non-nuclear weapon states were hesitant to give up their ability to pursue nuclear weapons because they did not want to lose the strategic value that the weapons provided. First and foremost, possession of nuclear weapons deters major conflict. For developing countries, it closes the power gap with world superpowers. Nuclear weapons also protect countries from nuclear blackmail[79]. Non-nuclear weapon states were hesitant to agree to not pursue nuclear activities because it would leave them vulnerable and defenseless against nuclear weapon states[80]. Another main concern was that not engaging in nuclear activity would bar these countries from the benefits of peaceful nuclear activities[81]. This could potentially result in industrial and economic burdens, as nuclear energy had known benefits at the time.

The NPT only bound nuclear weapon states to take steps to agree to reduce their nuclear stockpiles in good faith, but did not require these states to disarm their existing stockpiles. This did not sit well for non-nuclear weapon states, because it did not guarantee that nuclear weapon states would have their hands sufficiently tied[82]. These states, all third world or rapidly developing countries, wanted assurance that nuclear weapon states would not use or threaten to use nuclear weapons against them. They

---

[78] GOLDSCHMIDT, B. *Le Complexe Atomique ; Histoire Politique De Lenergie Nucleaire*. PARIS: FAYARD, 1980. (The Atomic Complex: Political History of Nuclear Energy)
[79] *Nonproliferation Treaty :Hearings before the Ninetieth Congress ... on Executive H, 90th Congress, Second Session, Treaty on the Nonproliferation of Nuclear Weapons.* Washington :, 1968. http://hdl.handle.net/2027/uc1.$b643615.
[80] GOLDSCHMIDT, B. *Le Complexe Atomique ; Histoire Politique De Lenergie Nucleaire*. PARIS: FAYARD, 1980. (The Atomic Complex: Political History of Nuclear Energy)
[81] Ibid.
[82] Ibid.

also wanted a genuine commitment by nuclear weapon states to assist them in the advancement of peaceful applications of nuclear energy. The non-nuclear weapon states supported IAEA safeguards and monitoring to ensure their needs were met[83].

The main obstacle to negotiations was that negotiations between the USSR and US regarding an end to their nuclear arms race were not fruitful. The US was supportive of a strict non-proliferation regime monitored by the IAEA. It also supported the idea of a Multilateral Force, where nuclear weapons would be in overseen by NATO crews. The USSR opposed group control of nuclear weapons. The USSR also supported IAEA safeguards as opposed to the existing Euratom safeguards that the Common Market countries implemented. However, the USSR refused to subject themselves to IAEA safeguards, as the NPT did not require the nuclear weapon states to subject themselves to the IAEA[84]. Secret negotiations between the US and the USSR, which culminated in the US dropping the idea of the Multilateral Force, removed the last major roadblock to the NPT[85]. On 1 July 1968, after three years of debate and redrafting, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was opened for signature. The NPT entered into force on 5 March 1970.

The final text of the treaty has three pillars: the non-proliferation of nuclear weapons, the disarmament of nuclear weapons, and the promotion of peaceful uses of nuclear energy. The NPT recognizes the US, Russia, the UK, France, and China as confirmed nuclear weapon states. These states are bound to not transfer nuclear weapons to non-nuclear weapon states, or aide them in producing or manufacturing nuclear weapons. Nuclear weapon states themselves are not forced to disarm, but

---

[83] Ibid.
[84] *Nonproliferation Treaty :Hearings before the Ninetieth Congress ... on Executive H, 90th Congress, Second Session, Treaty on the Nonproliferation of Nuclear Weapons.* Washington :, 1968. http://hdl.handle.net/2027/uc1.$b643615.
[85] GOLDSCHMIDT, B. *Le Complexe Atomique ; Histoire Politique De Lenergie Nucleaire.* PARIS: FAYARD, 1980. (The Atomic Complex: Political History of Nuclear Energy)

rather to engage in future negotiations to end the nuclear arms race. The NPT entrusts the IAEA as the inspectorate for ensuring compliance with its non-proliferation and disarmament clauses[86]. The verification of accuracy and non-deviation reports are how the IAEA monitors compliance with the NPT[87]. Although nuclear weapon states are not subject to IAEA safeguards, the US and the UK voluntarily committed to voluntarily subject themselves to safeguards in order to assuage the fears of non-nuclear weapon states[88].

The NPT also contains duration provisions in Article X[89]. The duration of the NPT will be reviewed every 25 years, with overall reviews every five years[90]. These review conferences were important, because it was known that not all nuclear powers were going to ratify the NPT. France and China, who gained nuclear weapons in 1960 and 1964 respectively, were not expected to join. India was also not expected to join. Although India did not signal strong nuclear capabilities, it was worried that the threat that nuclear China posed to nuclear weaponless India could incentivize India to go nuclear[91].

Chemical Weapons: The Chemical Weapons Convention

Use of chemical weapons has been recorded as far back as 600 BCE. Up until World War I, they were used sparingly, and were not common to war. Their modern-day

---

[86] "Background Information." *UNODA Meetings Place*. Accessed March 13, 2020. https://meetings.unoda.org/section/conf-npt-2020-background-inf/.
[87] "Safeguards Agreements." Text. IAEA, June 8, 2016. https://www.iaea.org/topics/safeguards-agreements.
[88] *Nonproliferation Treaty :Hearings before the Ninetieth Congress ... on Executive H, 90th Congress, Second Session, Treaty on the Nonproliferation of Nuclear Weapons.* Washington :, 1968. http://hdl.handle.net/2027/uc1.$b643615.
[89] "Treaty on the Non-Proliferation of Nuclear Weapons (NPT) – UNODA." Accessed April 4, 2020. https://www.un.org/disarmament/wmd/nuclear/npt/text/.
[90] "Background Information." *UNODA Meetings Place*. Accessed March 13, 2020. https://meetings.unoda.org/section/conf-npt-2020-background-inf/.
[91] *Nonproliferation Treaty :Hearings before the Ninetieth Congress ... on Executive H, 90th Congress, Second Session, Treaty on the Nonproliferation of Nuclear Weapons.* Washington :, 1968. http://hdl.handle.net/2027/uc1.$b643615.

proliferation is largely credited to Fritz Haber, a German scientist, who weaponized chemical gasses for Germany to use in World War I[92]. The Germans carried out the first major chemical weapons attack with Chlorine gas on 22 April 1915 against the French and Algerian Forces in Belgium. The Germans thought they were going to change the course of the war by breaking stalemates in trench warfare[93]. But, by September 1915, the Allied forces had also started using chemical weapons. In 1916, chemical weapons became standard use on both sides, and each side started developing masks to combat its effects[94]. Three main types of chemical weapons were introduced during the War: asphyxiants, blistering agents and blood agents. 124,200 tons of these chemical agents were deployed by both sides. 90,000 soldiers suffered painful deaths, and close to a million more people were left blind, disfigured, or with debilitating injuries, pain, and suffering[95].

Public outrage at the unnecessary suffering caused by chemical weapons lead to the creation of the Geneva Protocol of 1925. The Geneva Protocol banned the use of chemical weapons, but after World War I, world powers still ramped up development of chemical weapons. The USSR, the US, Japan, Germany, Italy, and the UK all heavily stockpiled old and new chemical weapons[96]. At the beginning of World War II, there was international panic that stronger and more devastating chemical weapons would be used. The world began to brace for it, but it never actually happened. Historians have many theories as to why, but the prevailing theory is that parity in chemical weapon stockpiling acted as a form of deterrence[97]. After the War, the tensions of the

---

[92] "A Brief History of Chemical War." *Science History Institute*, May 11, 2015. https://www.sciencehistory.org/distillations/a-brief-history-of-chemical-war.
[93] Ibid.
[94] "Gas in The Great War." Accessed February 18, 2020. http://www.kumc.edu/wwi/medicine/gas-in-the-great-war.html.
[95] Ibid.
[96] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))
[97] Ibid.

Cold War spurred more research and development of chemical weapons. Countries developed "second generation" chemical weapons, such as nerve and incapacitating agents, that were more lethal than the weapons used in WWI. These were seen as a viable military option given nuclear deterrence.

Chemical weapons continued to proliferate and did not get much consideration until the 1960s. In discourse at the UN, chemical weapons were discussed in tandem with biological weapons under the umbrella of general disarmament. At the time, there was a perceived need for a disarmament of chemical weapons, but steps beyond discussion at plenary meetings of the United Nations and relevant bodies were not taken. Negotiations did not pick up in earnest until 1980 when a specific Ad-Hoc group under the Conference on Disarmament was created. Between 1980 and 1984, smaller working groups of the Ad-Hoc group were assigned to work towards a draft convention on chemical weapons disarmament. In 1984, a "rolling text" was introduced. This rolling text was a non-binding draft of the convention that was continuously updated until the Convention was approved in 1993.

Increasing public awareness of the consequences of chemical weapons after World War I put pressure on states to ensure they were never used in war again. The issues that delayed reaching a disarmament agreement did not stem from countries not wanting to give up the value that owning chemical weapons gave them. Across the board, there was agreement that a treaty needed to be reached with a goal of eliminating chemical weapons and avoiding the consequences of their proliferation. The negotiations of the CWC took many years because states wanted to make an agreement that completely banned the development, stockpiling, and use of chemical weapons. This posed a major problem for states during negotiations: how do you write a treaty comprehensive enough to completely ban an entire category of WMD? The CWC's

predecessors, the Geneva Protocol and the Biological Weapons Convention both have limited scope and a lack of verification measures. These fallacies in both did not deter the use of the weapon and each had multiple violations. States negotiating the CWC wanted to ensure these two problems were solved through the institutional design of the agreement. In order to do so, all states had to agree on a verification mechanism and the right scope of the treaty.

The political landscape at the time delayed negotiations significantly. East-West tensions accelerated the chemical weapons arm race during the Cold War[98]. Thus, encouraging the development and stockpiling of new, more dangerous chemical weapons. The Western countries and the Socialist countries also disagreed on the basics of the verification regime[99]. It was not until 1988 that the USSR came around to the Western views on verification, and along with the US, submitted the first draft proposal of the final treaty. The relaxation of tensions between the US and the USSR signaled their committed tying their hands on chemical weapons and set an example for other countries to follow. This was particularly helpful because some states were hesitant to give up chemical weapons in case other states continued programs in secret.

One major obstacle to negotiating the CWC was figuring out how to regulate the chemical industry, since the handling of chemical weapon precursors was concentrated in the private sector[100]. The chemical industry pushed back at the proposed inspection methods, as they saw the agreement as invading their commercial privacy and increasing the possibility of "bad press" for being associated with chemical weapons.

---

[98] Thakur, Ramesh and Chandan, Tejal (2006). *The Chemical Weapons Convention: Implementation, Challenges and Opportunities*. United Nations University Press.
[99] Bernauer, Thomas. *The Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*. New York: United Nations, 1990.
[100] Thakur, Ramesh and Chandan, Tejal (2006). *The Chemical Weapons Convention: Implementation, Challenges and Opportunities*. United Nations University Press.

Industry leaders also claimed compliance with the proposed verification methods would put a large financial burden on many firms in the industry[101]. These concerns were addressed at the 1989 Government -Industry conference.

To resolve the Industry's concerns, states expanded the scope of what the CWC covers and included extremely thorough verification and compliance mechanism that levied the smallest burden possible on the Industry[102]. Article II of the CWC expands the definition of a chemical weapon to include its components plus the equipment needed to make a chemical weapon, rather than the final product. Any toxic or precursor chemical defaults as a weapon, unless it is being developed or produced for purposes that are not prohibited and the quantities and types are consistent with such purposes. This allows for easier facilitation of a total weapons ban without imposing harsh restrictions within the chemical industry. [103]

The CWC created the Organization for the Prohibition of Chemical Weapons (OPCW), which is in charge of administering the verification and compliance mechanisms. The OPCW is made up of three bodies: The Technical Secretariat, the Executive Council, and the Conference of the States Parties. The Technical Secretariat administers the verification system[104]. The Executive Council mainly oversees the Technical Secretariat and issues measures regarding non-compliance[105]. The Conference of the States Parties is the plenary organ of the OPCW and oversees implementation of the CWC[106].

---

[101] Ibid.
[102] "History" *OPCW*. https://www.opcw.org/about-us/history.
[103] "Chemical Weapons Convention." *OPCW*. Accessed April 4, 2020. https://www.opcw.org/chemical-weapons-convention.
[104] "Technical Secretariat." *OPCW*. https://www.opcw.org/about-us/technical-secretariat.
[105] "Executive Council." *OPCW*. https://www.opcw.org/about-us/executive-council.
[106] "Conference of the States Parties" *OPCW*. https://www.opcw.org/about-us/history.

The final verification system is based on verifications of chemical weapons destruction and non-diversion of chemicals from peaceful to military purposes. All parties to the treaty have to submit declarations on chemical weapon stockpiles, live and abandon production facilities, relevant chemical activities, national implementation strategies and related matters to the OPCW. Verification of treaty compliance hinges on the correctness of these reports, confirmed by fact-finding missions and on-site inspections. If a state has doubts about another state party's compliance, it may ask for clarification or request an on-site challenge inspection at the location of doubtful activities. This non-routine verification resolves doubts or ambiguities concerning compliance that cannot be solved by the routine verification system. There also exists a traditional inter-state dispute settlement process.

The CWC negotiators spent many years working through all of the obstacles to cooperation in order to reach their goal of a comprehensive chemical weapons disarmament treaty. The problems they faced were solvable through compromise, because all parties understood the need for a hand-tying agreement. In 1997, 72 years after the Geneva Protocol, the CWC entered into force.

Biological Weapons: The Biological Weapons Convention

Biological weapons are complex systems that disseminate disease-causing organisms or toxins to harm or kill humans, animals or plants[107]. Biological weapons have been used in warfare for centuries. Human bodies that were infected with diseases were used to poison enemies' water supplies and even catapulted over city walls to spread infectious diseases. Biological weapons have been the ire of public opinion since

[107] "What Are Biological and Toxin Weapons?" Accessed April 4, 2020. https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument.

the late 1800s. The first steps to mitigate this risk were the 1874 Brussels Declaration and the 1899 Hague Declaration which prohibited the use of poisonous weapons[108]. The modern-day use of biological weapons started after the foundation of microbiology[109]. The knowledge gained through the study of microorganisms helped form modern medicine, but it also laid out the roadmaps to weaponize organisms. The first modern use of biological weapons was during World War I by the Germans. German forces attempted to infect livestock that was being sent to Great Britain with Anthrax and Glanders. These two pathogens infect animals first, and then infect humans when they come into contact with infected animals[110,111].

These attacks were not successful, but it signaled both the strategic value of such weapon, and its potential consequences to world populations. In the aftermath of World War I, the Geneva Protocol of 1925 outlawed the use of both biological and chemical weapons. However, the limited scope of the Protocol and lack of a monitoring system did not deter the development and use of biological weapons. Many of the world powers began to invest in biological weapons to give them an edge in light of the post-war tensions. No biological weapons were used again until World War II, but were developed and advanced in secret[112]. During the War, Japan poisoned Chinese water wells with cholera and typhus, dropped disease infected insects onto rice fields and trade routes, and sprayed toxic gases down on villages[113]. Tens of thousands of Chinese were killed by Japanese bio-weapons during the war, and more died after. In 1947, two

---

[108] Frischknecht, Friedrich. "The History of Biological Warfare: Human Experimentation, Modern Nightmares and Lone Madmen in the Twentieth Century." *EMBO Reports* 4, no. S1 (June 2003). doi:10.1038/sj.embor.embor849.
[109] Ibid.
[110] "Biological Weapons WW1." Accessed February 18, 2020. https://www.arcgis.com/apps/Cascade/index.html?appid=90a21c86f91c484bb3ba8dc64d4ce758.
[111] Jeffrey R. Ryan, *Biosecurity and Bioterrorism: Containing and Preventing Biological Threats*(Amsterdam: Elsevier/BH, Butterworth-Heinemann is an imprint of Elsevier, 2016))
[112] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))
[113] Ibid.

years after Japan surrendered, 30,000 people died due to complications from biological toxin exposure[114]. Biological weapons mimic diseases which have long-term health implications, and also destroy societal infrastructure.

There was fear that Germany would use biological weapons during the War as well. This fear sparked retaliatory investment in bio-weapons programs in France, the UK, and the US[115]. Germany never used them, though, and historians attribute it to a nasty consequence of biological warfare: pathogens do not respect borders. Germany is located in the middle of Europe, so any attack could have backfired and infected its own people. This consequence of bio-weapons made it an unattractive military strategy. After World War II, countries continued their bio-weapons programs. During this time, advancements in bio-weapons created more types of dangerous toxins such as Brucellosis and Gas Gangrene. States also perfected how to turn infectious diseases such as typhoid, cholera, tetanus, small pox, tuberculosis, and tularemia into ammunition. Weaponization of bacteria related to food poisoning such as salmonella and clostridium botulinum, with an intent to incapacitate rather than kill, proliferated[116].

Another treaty was not considered in earnest again until the late 1960s. In 1966, the UN General Assembly passed a resolution calling for strict observance of the Geneva Protocol. Although this bound UN members states to following the Protocol, there was still a need for another treaty to address shortcomings of the Protocol. Many states submitted reservations to the Protocol that retained the rights to use biological weapons in retaliations. The Protocol became a "no-first use" treaty, therefore technically not

---

[114] Ibid.
[115] Ibid.
[116] Frischknecht, Friedrich. "The History of Biological Warfare: Human Experimentation, Modern Nightmares and Lone Madmen in the Twentieth Century." *EMBO Reports* 4, no. S1 (June 2003). doi:10.1038/sj.embor.embor849.

prohibiting the use of biological weapons. The Protocol also did not have a monitoring and punishment mechanism, so it did not effectively tie states' hands[117].

States knew a stricter, hand-tying agreement was needed to remedy these fallacies. At the time, biological and chemical weapons were discussed in tandem. In 1968, the UK submitted a working paper to the Eighteen Nation Disarmament Committee (ENDC) suggesting that the two topics should be discussed separately. The UK argued that chemical weapons needed a longer negotiation period than biological weapons, and that it should not delay an agreement on biological weapons. Chemical weapons posed a larger threat due to their frequent use in World War I, and their stockpiling value as a deterrent[118].

On 25 November 1969, US president Richard Nixon halted America's offensive biological weapons program and supported the UK's proposal. This set a standard of commitment to hand-tying, and countries such as Canada, the UK, and Sweden followed suit[119]. In 1971, the USSR and its allies came around to the view that biological weapons could be dealt with separately and submitted a proposal to the UN that dealt solely with biological weapons. A final draft of the treaty was approved in late 1971. In total, the negotiations on the Biological Weapons Convention only lasted less than three years. The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction

---

[117] Lambert, Robert W. *International Negotiations on the Biological-Weapons and Toxin Convention /*. [Washington] :, 1975. http://hdl.handle.net/2027/uva.x004347395.

[118] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction - Main Page." Accessed April 4, 2020. https://legal.un.org/avl/ha/cpdpsbbtwd/cpdpsbbtwd.html.

[119] Lambert, Robert W. *International Negotiations on the Biological-Weapons and Toxin Convention /*. [Washington] :, 1975. http://hdl.handle.net/2027/uva.x004347395.

(Biological Weapons Convention, BWC) was opened for signature in early 1972 and entered into force in 1975.[120,121]

Article I of the BWC prohibits the "development, production, and stockpile of microbial or other biological agents, or toxins… that have no justification for prophylactic, protective or other peaceful purposes and weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict"[122]. Articles V and VI constitute a quasi-monitoring system. Article V mandates that states parties undertake consultation and cooperation with one another when any problems arise in the implementation of the convention. Article VI gives states parties the ability to lodge a complaint with the UN Security Council if it believes another state is breaching their obligations. The Security Council has the power to investigate that country without interference or refusal. Article XII mandates review conference every five years and Article XIII gives the convention an unlimited duration[123]. The BWC does not technically ban the use of biological weapons. However, the reaffirmation of the Geneva Protocol bans the use of biological weapons. The combination of these two international agreements signal that a hand-tying cooperative outcome to eliminate biological weapons was reached.

---

[120] The entirety of the following timeline comes from the United Nations Audiovisual Library of International Law's BWC Procedural History page (citation in footnote 77)
[121] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction - Main Page." Accessed April 4, 2020. https://legal.un.org/avl/ha/cpdpsbbtwd/cpdpsbbtwd.html.
[122] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction." http://disarmament.un.org/treaties/t/bwc/text
[123] Ibid.

Section VI – Hypothesis Testing

In this section, I test my two hypotheses. Hypothesis 1 (H1) has two clues. The existence of each clue is necessary to affirm the hypothesis. I collect the same type of evidence to support the existence of each clue among my three case studies. Hypothesis 2 (H2) is tested using my own methodology, which appears in Appendix B.

Hypothesis 1: Understanding a weapon's consequences makes states more willing to cooperate

I hypothesize that as the consequences of a weapon become more understood, states are more willing to cooperate. Consequences often drive cooperation - states agree to disarm to avoid consequences of a potential event. I predict that when the consequences of a weapon become understood and internalized, it provokes more of an urgency to cooperate. I apply hoop-tests to each of these clues. Each clue is necessary to affirm the hypothesis, but not sufficient. If the hypothesis does not pass the hoop-test, the hypothesis is rejected. If this hypothesis were to be true, then we would see two clues:

Clue 1: the consequences of the weapon became understood

Clue 2: the understanding affected willingness to cooperate

Clue 1 would manifest in public declarations that signify the consequences as understood facts. Each declaration is a form of communication that imparts the knowledge of the consequences of the weapon onto other people. Types of evidence would therefore be any type of formal report confirming the damage done, publicized first-hand accounts, or quotes from prominent figures who are close to the subject.

To find evidence to support the existence of **clue 2**, I collect direct quotes from UN resolutions. The preambles of UN resolutions acknowledge the reason for addressing

the topic. It is the place for member states to explain why they are cooperating, thus making it a good place to see if disarmament resolutions were influenced by an understanding of the consequences. Direct calls for cooperation are given in action items in the articles of the resolutions.

C1. NW. E1 – Academic Research

Academic research that confirmed the consequences of nuclear weapons is a signal that these consequences were understood. In 1951, the Joint Commission for the Investigation of the Effects of the Atomic Bomb in Japan released a report detailing the effect of the bomb on human and environmental life, as well as physical infrastructure. The high volume of deaths as a result of the nuclear weapons was an observable consequence. The report estimated that between 60,000 and 80,000 people died instantly in Hiroshima and around 40,000 people reportedly died instantly in Nagasaki. The world observed these deaths and understood how nuclear weapons can wipe out large percentages of cities' populations. Beyond the deaths, the destruction of cities was another observable consequence. In Hiroshima, 61% of the city's buildings were completely burned, and 75.4% of all buildings were at least partially destroyed[124]. In Nagasaki, a third of the city was destroyed[125].

Scholars also conducted scientific studies to better understand the health impacts that nuclear weapons have on people. In the Baby Tooth Survey, scientists found conclusive evidence that above-ground nuclear testing had severe public health risks.

---

[124] Oughterson, A. W., LeRoy, G. V., Liebow, A. A., Hammond, E. C., Barnett, H. L., Rosenbaum, J. D., and Schneider, B. A. Thu . "Medical Effects Of Atomic Bombs The Report Of The Joint Commission For The Investigation Of The Effects Of The Atomic Bomb In Japan Volume 1". United States. doi:10.2172/4421057. https://www.osti.gov/servlets/purl/4421057.
[125] Ibid.

The study found that humans were ingesting cancer-causing radioactive isotopes as a result of fallout from nuclear testing[126]. This report, released in 1951, made people very aware of the severe consequences that nuclear weapons can have on those who are not thought to be directly impacted by them.

C1. NW. E2 – Mass publication of first-hand accounts

The distribution of first-hand accounts of the effects of nuclear weapons in the mass media directly informed average people of the capabilities of nuclear weapons. The immediate news reporting after Hiroshima and Nagasaki alerted people across the world on how destructive nuclear weapons are. Some examples of global headlines are:

"'Tremendous and Awe-Insipiring' Town of Hiroshima Completely Blotted Out"[127]

""Atomic Bomb Smashes Nagasaki in Inferno of Smoke and Flame"[128]

"Japanese Report Death Toll Still Rising in Hiroshima and Nagasaki Months after Atomic Bombings"[129]

Yoshito Matsushige, a Hiroshima survivor, is the only photographer to capture first-hand historical accounts of the bombing of Hiroshima[130]. The Japanese magazine Asahi Gurafu published the photographs for the first time on August 6, 1952 in an

[126] Reiss, Louise Zibold. "Strontium-90 Absorption by Deciduous Teeth." *Science* 134, no. 3491 (November 24, 1961): 1669. doi:10.1126/science.134.3491.1669.
[127] "'Rain of Ruin': How the Guardian Reported the Dropping of the Atomic Bomb on Hiroshima | World News | The Guardian." Accessed May 10, 2020. https://www.theguardian.com/world/from-the-archive-blog/2015/aug/06/hiroshima-atomic-bomb-guardian-1945-archive.
[128] "Atomic Bomb Smashes Nagasaki in Inferno of Smoke and Flame." *Freeport Journal-Standard*. August 10, 1945.
[129] "Japanese Report Death Toll Still Rising in Hiroshima and Nagasaki Months after Atomic Bombings - Newspapers.Com." Accessed May 10, 2020. https://www.newspapers.com/clip/47464888/japanese-report-death-toll-still-rising/.
[130] "Yoshito Matsushige." *Atomic Heritage Foundation*. Accessed May 10, 2020. https://www.atomicheritage.org/profile/yoshito-matsushige.

article titled "First Exposé of A-Bomb Damage". Life magazine published the imagines in September 29, 1952 in an article titled "When Atom Bomb Struck – Uncensored". Matsushige also spoke publicly about his experience. Here are some of his quotes that were published:

"I was bare from the waist up, and the blast was so intense, it felt like hundreds of needles were stabling me all at once. The blast grew large holes in the walls of the first and second floor"[131]

"I saw a burnt streetcar which had just turned the corner at Kamiya-cho. There were passengers still in the car. I put my foot onto the steps of the car and I looked inside. There were perhaps 15 or 16 people in front of the car. They laid dead one on top of another."[132]

C1. NW. E3 – Quotes from Prominent Figures

Many important political and academic figures publicly took a stand against nuclear weapons after internalizing how destructive they are. Nobel Laureate Bertrand Russel, who was a hallmark of British politics and academia in the mid 20th, century put out literature calling on world governments to save the world from the effects of nuclear weapons.

"The prospect for the human race is sombre beyond all precedent. Mankind are faced with a clear-cut alternative: either we shall all perish, or we shall have to acquire some slight degree of common sense"[133]

[131] Matsushige, Yoshito. "Account of the Atomic Bombing of Hiroshima Japan," n.d., 2.
[132] Ibid.
[133] "The Bomb and Civilization." Accessed February 17, 2020. http://www.personal.kent.edu/~rmuhamma/Philosophy/RBwritings/bombCivilization.htm.

From the Russell-Einstein Manifesto, written in tandem with Albert Einstein:

"It is stated on very good authority that a bomb can now be manufactured which will be 2,500 times as powerful as that which destroyed Hiroshima."[134]

"It is feared that if many H-bombs are used there will be universal death, sudden only for a minority, but for the majority a slow torture of disease and disintegration"[135]

"No doubt, in an H-bomb war, great cities would be obliterated. But this is one of the minor disasters that would have to be faced. If everybody in London, New York, and Moscow were exterminated, the world might, in the course of a few centuries, recover from the blow. But we now know, especially since the Bikini test, that nuclear bombs can gradually spread destruction over a very much wider area than had been supposed"[136]

C1. CW. E1– Research Conducted by the United Nations

One of the most important reports on the effects of chemical weapons at the time was the report of the UN Secretary General, U Thant, compiled by a panel of consultant experts from around the globe. The aim of the report is to "provide a scientifically sound appraisal of the effects of chemical and biological weapons and should serve to inform Governments of the consequences of their possible use"[137]. Here are some of the Report's discoveries regarding medical consequences for individuals exposed to chemical weapons:

---

[134] "Russell-Einstein Manifesto." *Atomic Heritage Foundation.* Accessed February 17, 2020. https://www.atomicheritage.org/key-documents/russell-einstein-manifesto.
[135] Ibid.
[136] Ibid.
[137] "Chemical and Bacteriological (Biological) Weapons and the Effects of Their Possible Use :" Accessed May 10, 2020. https://digitallibrary.un.org/record/577282?ln=en.

"lethal chemical agents kill in relatively small doses, and as a rule the amount that causes death is only slightly greater than that which causes incapacitation"[138]

"the nerve-agent casualty who has been exposed to a lethal dose will die of asphyxiation within a few minutes if he is not treaty swiftly"[139]

"At higher dosages [of nerve-agents], the skeletal muscles are affected, weakness, fibrillation and, eventually, paralysis of the respiratory muscles occurring. Death is usually caused by respiratory failure, but heart failure may occur"[140]

"blistering with mustard is comparable to second-degree burns. More severe lesions, comparable to third-degree burns, may last for a couple of months. Blindness may be caused, especially if liquid agent has entered the eyes"[141]

Here is an example of the Report's findings on the dangers that chemical weapons pose to whole populations:

"Given a town with a total population of 80,000, a surprise attack with nerve gas could thus cause 40,000 casualties, half of them fatal, whereas under ideal circumstances for the defense, fatalities might number no more than 2,000. It is inconceivable, however, that the ideal would ever be attained"[142]

C1. CW. E2 – Quotes from World Leaders

The UN provided a forum for world leaders to denounce the use of chemical weapons due to their horrific effects. Here are some quotes from world leaders on the topic, given at the UN:

[138] Ibid. p. 28
[139] Ibid. p. 29
[140] Ibid. p. 29
[141] Ibid. p. 30
[142] Ibid. p. 34

"In some respects, they may be even more dangerous than nuclear weapons because they do not require the enormous expenditure of financial and scientific resources that are required for nuclear weapons." – Former UN Secretary General U Thant[143]

"The use of chemical and biological weapons has long been viewed with revulsion by civilized nations. No peace-making institution can ignore the use of those dread weapons and still live up to its mission" - Former US President Ronald Reagan[144]

"Despite the obvious danger incident to nuclear weapons, it is not to be forgotten that there are other means of mass destruction in the arsenals of states, including chemical weapons. The fact, however unthinkable, is that a few kilograms of poisonous agents from the tens of thousands of tons which are operational in the armies of certain countries, are sufficient to kill several million people…Everything should be done for the elimination of chemical weapons from the face of the earth" – Former USSR leader Leonid Brezhnev[145]

C1. CW. E3 – Publication of First-Hand Accounts

First-hand accounts of chemical weapons were published and invited people who were not involved in the war to understand the actual consequences of chemical weapons. Here are some examples:

[143] Ibid. foreword
[144] "Transcript of Reagan's U.n. Speech on the Nuclear Arms Race." *The New York Times*, June 18, 1982, sec. World. https://www.nytimes.com/1982/06/18/world/transcript-of-reagan-s-un-speech-on-the-nuclear-arms-race.html.
[145] "BREZHNEV'S STATEMENT AND EXCERPTS FROM GROMYKO'S SPEECH - The New York Times." Accessed May 10, 2020. https://www.nytimes.com/1982/06/16/world/brezhnev-s-statement-and-excerpts-from-gromyko-s-speech.html.

"Then there staggered into our midst French soldiers, blinded, coughing, chests heaving, faces an ugly purple color, lips speechless with agony, and behind them in the gas-soaked trenches, we learned that they had left hundreds of dead and dying comrades" – A British solider describes the scene at the Battle of Ypres in 1915, cited in the book *Chemical Warfare*, published in 1921[146].

"What we saw was total death. Nothing was alive. All of the animals had come out of their holes to die. Dead rabbits, moles, and rats and mice were everywhere. The smell of the gas was still in the air. It hung on the few bushes which were left" – This is an excerpt from a letter that German soldier Willi Siebert wrote to his son after the first chlorine gas attack[147].

"Gas! Gas! Quick, boys! — An ecstasy of fumbling, Fitting the clumsy helmets just in time; But someone still was yelling out and stumbling, and floundering like a man on fire or lime . . . Dim, through the misty panes and thick green light, as under a green sea, I saw him drowning" – a verse from the poem "Dulce et Decorum Est" written by British solider Wilfred Owen about his own experiences with chemical weapons in WW1[148].

Beyond physical effects, chemical weapons had scarring psychological effects on victims. A 1918 US Army report described how gas fright and gas shellshock became commonplace:

"Someone yelled "GAS!" and said their food had been gassed. All the men were seized with gas fright and a few minutes later made their way to the Aid Station. They came in in stooping posture, holding their abdomens and complaining of pains in the

---

[146] Fries, Amos A., and Clarence J. West. *Chemical Warfare*. New York: McGraw-Hill Book Co., 1921.
[147] "First-Hand Accounts of the First Chlorine Gas Attack." *100 Years of Chemical Weapons*, February 9, 2015. http://chemicalweapons.cenmag.org/first-hand-accounts-of-the-first-chlorine-gas-attack/
[148] Foundation, Poetry. "Dulce et Decorum Est by Wilfred Owen." Text/html. *Poetry Foundation*. Poetry Foundation, May 10, 2020. Https://www.poetryfoundation.org/. https://www.poetryfoundation.org/poems/46560/dulce-et-decorum-est.

stomach, while their faces bore anxious, frightened expressions and some had even vomited"

This quote is a first-hand account of PTSD from a chemical weapon – the food was not actually poisoned[149].

C1. BW. E1 – Research Conducted by the United Nations

Below are excerpts from the 1969 UN Secretary General's report on the effects of biological weapons. Here are the medical effects on individuals of specific biological weapons:

"The lung or respiratory form is most severe, and unless early treatment with antibiotics is resorted to, death ensues within two or three clays in nearly every case" – on Anthrax[150]

"Such aerosols could result in a high proportion of deaths in a heavily exposed population. Immunization could not be expected to protect against a heavy aerosol attack. The soil would remain contaminated for a very long time and so threaten livestock farming"– on Anthrax[151]

"sweating and muscle pains follow after an incubation period of from one to three weeks. In most cases, recovery from the disease occurs after some weeks of illness…Treatment presents great difficulties" – on Coccidioidomycosis[152]

---

[149] Frischknecht, Friedrich. "The History of Biological Warfare: Human Experimentation, Modern Nightmares and Lone Madmen in the Twentieth Century." *EMBO Reports* 4, no. S1 (June 2003). doi:10.1038/sj.embor.embor849.
[150] "Chemical and Bacteriological (Biological) Weapons and the Effects of Their Possible Use :" Accessed May 10, 2020. https://digitallibrary.un.org/record/577282?ln=en.
[151] Ibid. p. 40
[152] Ibid. p. 40

"three to-five-day incubation period. The patient suffers from severe general symptoms and, if untreated, normally dies within two to three days. A patient with pneumonic plague is extremely contagious to contacts" – on the Bubonic Plague[153]

The report also assessed the effects of biological weapons on whole populations:

"no civilian populations are protected. Unprotected military or civilian personnel would be at complete risk, and panic and irrational behavior would complicate the effects of the attack. The heavy burden that would be imposed on the medical services of the attacked region would compound disorganization, and there would be a major risk of the total disruption of all administration services"[154]

C1. BW. E2 – Quotes from World Leaders

Biological and chemical weapons were discussed in tandem before the singing of the BWC. The evidence collected to support chemical weapons is also evidence collected to support the case of biological weapons.

"In some respects, they may be even more dangerous than nuclear weapons because they do not require the enormous expenditure of financial and scientific resources that are required for nuclear weapons." – Former UN Secretary General U Thant[155]

"The use of chemical and biological weapons has long been viewed with revulsion by civilized nations. No peace-making institution can ignore the use of those dread weapons and still live up to its mission" -Former US President Ronald Reagan[156]

---

[153] Ibid. p. 41
[154] Ibid. p. 41
[155] Ibid. foreword
[156] "Transcript of Reagan's U.n. Speech on the Nuclear Arms Race." *The New York Times*, June 18, 1982, sec. World. https://www.nytimes.com/1982/06/18/world/transcript-of-reagan-s-un-speech-on-the-nuclear-arms-race.html.

"Biological weapons have massive, unpredictable and potentially uncontrollable consequences. They may produce global epidemics and impair the health of future generations" – Former US President Richard Nixon[157]

C2. NW. E1 – UN Resolution Language

GA Draft Resolution A/C.1/L.206 1958 - the first draft resolution on the issue of nuclear non-proliferation

"*Recognizing further* that the danger now exists that an increase in the number of states possessing nuclear weapons may occur"[158]

GA Resolution 1402 - Suspension of Nuclear and Thermonuclear Tests (1959)

"*Desiring* to safeguard mankind from the increasing hazards resulting from tests of nuclear and thermonuclear weapons,"[159]

"*Bearing in mind* the profound concern evinced by the peoples of all countries regarding the testing of nuclear and thermo-nuclear weapons,"[160]

GA Resolution 1576 - Prevention of the Wider Dissemination of Nuclear Weapons (1960)

"*Recognizing* the urgency danger that now exists that an increase in the number of States possessing nuclear weapons may occur… and the difficulty of maintaining world peace"[161]

---

[157] Department Of State. The Office of Electronic Information, Bureau of Public Affairs. "166. Statement Issued by President Nixon, November 25, 1969." Department Of State. The Office of Electronic Information, Bureau of Public Affairs., September 19, 2007. https://2001-2009.state.gov/r/pa/ho/frus/nixon/e2/83597.htm.
[158] General Assembly draft resolution A/C.1/L.206 (17 October 1958), available from undocs.org/A/C.1/L.206
[159] General Assembly resolution 14/1402, Suspension of Nuclear and Thermo-nuclear Tests A/RES/14/1402 (21 November 1959), available from undocs.org/A/14/1402
[160] Ibid.
[161] General Assembly resolution 15/1576, Prevention of the Wider Disseminations of Nuclear Weapons A/RES/15/1576 (20 December 1960), available from undocs.org/A/15/1576

"*Believing* in the necessity of an international agreement"[162]

"*Believing* further that, pending the conclusion of such an international agreement, it is desirable that temporary and voluntary measures be taken to avoid the aggravation of this danger"[163]

GA resolution 1578 - Suspension of Nuclear and Thermo-nuclear tests (1960)

"*Recognizing* further that agreement on the cessation of test of nuclear and thermo-nuclear weapons is not only imperative but urgent"[164]

C2. CW. E1 – UN Resolution Language

GA resolution 2603 (XXIV) – Question of Chemical and Bacteriological (Biological) Weapons (1969)

"*Considering* that chemical and biological methods of warfare have always been viewed with horror and been justly condemned by the international community,"[165]

"*Considering* that these methods of warfare are inherently reprehensible because their effects are often uncontrollable and unpredictable and may be injurious without distinction to combatants and non-combatants, and because any use of such methods would entail a serious risk of escalation,"[166]

---

[162] Ibid.
[163] Ibid.
[164] General Assembly resolution 15/1578, Suspension of Nuclear and Thermo-Nuclear tests A/RES/15/1578 (20 December 1960), available from undocs.org/A/15/1578
[165] General Assembly resolution 24/2603, Question of chemical and bacteriological (biological) weapons A/RES/24/2603 (16 December 1969), available from undocs.org/A/24/2603

[166] Ibid.

"*Emphasizing* the urgency of the need for achieving the earlier elimination of chemical and bacteriological (biological) weapons,"[167]

"*Recommends* to all Governments the wide distribution of the report so as to acquaint public opinion with its contents…"[168]

GA resolution 2662 (XXV) – Question of Chemical and Bacteriological (Biological) Weapons (1970)

"*Deeply convinced* that the prospects for international peace and security, as well as the achievement of the goal of general disarmament under effective international control, would be enhanced if the development, production and stockpiling of chemical and bacteriological (biological) agents for purposes of war were to end and if those agents were eliminated from all military arsenals,"[169]

"*Commends* the following basic approach, contained in the joint memorandum, for reaching an effective solution to the problem of chemical and biological methods of warfare:"

"(a) it is urgent and important to reach agreement on the problem of chemical and bacteriological (biological) warfare;"[170]

GA Resolution 38/187 (1983)

"*Convinced* of the need for the earlier conclusion of a convention on the prohibition on the development, production, and stockpiling of all chemical weapons and on their destruction, which would significantly contribute to general and complete disarmament under effective international control"[171]

---

[167] Ibid.
[168] Ibid.
[169] General Assembly resolution 25/2662, Question of chemical and bacteriological (biological) weapons A/RES/25/2662 (7 December 1970), available from undocs.org/A/25/2662
[170] Ibid.
[171] General Assembly resolution 38/187, chemical and bacteriological weapons A/RES/38/187 (20 December 1983), available from undocs.org/A/38/187

"*Expressing* profound concern at the intended production and deployment of binary chemical weapons"[172]

"*Appeals* to all states to facilitate in every possible way the conclusion of such a convention"[173]

C2. BW. E1 – UN Resolution Language

The evidence from UNGA Resolutions 2603 and 2662 collected for chemical weapons is evidence for biological weapons because they were discussed in tandem up until the ratification of the BWC. 1972, UN member states worked to reach an agreement on chemical weapons alone.

GA resolution 2603 (XXIV) – Question of Chemical and Bacteriological (Biological) Weapons (1969)

"*Considering* that chemical and biological methods of warfare have always been viewed with horror and been justly condemned by the international community,"[174]

"*Considering* that these methods of warfare are inherently reprehensible because their effects are often uncontrollable and unpredictable and may be injurious without distinction to combatants and non-combatants, and because any use of such methods would entail a serious risk of escalation,"[175]

---

[172] Ibid.
[173] Ibid.
[174] General Assembly resolution 24/2603, Question of chemical and bacteriological (biological) weapons A/RES/24/2603 (16 December 1969), available from undocs.org/A/24/2603

[175] Ibid.

"*Emphasizing* the urgency of the need for achieving the earlier elimination of chemical and bacteriological (biological) weapons,"[176]

"*Recommends* to all Governments the wide distribution of the report so as to acquaint public opinion with its contents…"[177]

GA resolution 2662 (XXV) – Question of Chemical and Bacteriological (Biological) Weapons (1970)

"*Deeply convinced* that the prospects for international peace and security, as well as the achievement of the goal of general disarmament under effective international control, would be enhanced if the development, production and stockpiling of chemical and bacteriological (biological) agents for purposes of war were to end and if those agents were eliminated from all military arsenals,"[178]

"*Commends* the following basic approach, contained in the joint memorandum, for reaching an effective solution to the problem of chemical and biological methods of warfare:"

"(a) it is urgent and important to reach agreement on the problem of chemical and bacteriological (biological) warfare;"[179]

[176] Ibid.
[177] Ibid.
[178] General Assembly resolution 25/2662, Question of chemical and bacteriological (biological) weapons A/RES/25/2662 (7 December 1970), available from undocs.org/A/25/2662
[179] Ibid.

Given the existence of evidence **C1. NW. E1, C1. NW. E2, C1. NW. E3, C1. CW. E1, C1. CW. E2, C1. CW. E3, C1. BW. E1, and C1. BW. E2,** we have reason to believe that Clue 1 exists in our world.

Given the existence of evidence **C2. NW. E1**, **C2. CW. E1, and C2. BW. E1,** we have reason to believe that Clue 2 exists in our world.

Thus, we have strong reason to believe that Hypothesis 1 holds true.

Hypothesis 2: If the strategic value of a weapon is low, states are more willing to cooperate

I hypothesize that the strategic value of a weapon affects a state's willingness to enter into hand-tying cooperative agreements. The strategic value of a weapon is the intrinsic value that a country places on ownership of that weapon. I hypothesize that there is a causal link between strategic value and willingness to cooperate because states can only "enjoy" the full value of a weapon if it does not agree to tie its hands. The value of a weapon is therefore the payoff from choosing an armament strategy – (B) or (C). The payoff ranking for states ranks mutual disarmament (A) > (B) and (C). Therefore, we assume that the strategic value of a weapon has to be lower than the value placed on mutual disarmament. I aim to measure the strategic value of a weapon to affirm that a low strategic value triggers a causal mechanism that results in a higher willingness to enter into cooperative agreements. In Appendix B, I explain my methodology for testing this hypothesis[180].

[180] See Appendix B for the full explanation of the methodology.

C1. NW. E1 – Deterrence Value

In most cases, the reason a country stockpiles a weapon is so the country can deploy the weapon during a time of conflict. Nuclear weapons are different in that the bulk of their value comes from their status as a deterrent. Nuclear weapons were used twice in 1945, and not once again for the next 75 years. Even at the height of the cold war, neither the USSR nor the US, the two world leaders in nuclear stockpiles, detonated a nuclear weapon for any reason besides testing. As parity among nuclear weapon states was achieved, the use of nuclear weapons was deterred via the principle of mutually assured destruction (MAD). MAD is based off of the fear of retaliation. If a state attacked another country with nuclear weapons, that country, or its allies, would use nuclear weapons in retaliation. MAD was simplified into: whoever shoots first, dies second. The annihilation from the exchange of nuclear weapons is a consequence so large that it almost renders the weapon unusable[181]. Looking through the lens of deterrence, there are benefits to stockpiling nuclear weapons.

C1. NW. E2 – Costs and Benefits

The benefits of deploying nuclear weapons are extremely low compared to the costs that the ensuing nuclear winter would cause. The costs of mutual annihilation are far greater than the costs of remaining in the status quo, regardless of the state of nature. A nuclear winter, as some scientists suspect, would have harmful impacts on

[181] "Strategy - Strategy in the Age of Nuclear Weapons." *Encyclopedia Britannica*. Accessed January 5, 2020. https://www.britannica.com/topic/strategy-military.

the world for up to millennia after the attack[182]. The fear of one's population suffering from retaliatory attacks deters a country from using their nuclear weapons in the first place. In considering the value a weapon has to a country's arsenal, it is important to consider the frequency with which the weapon is used to achieve policy goals. MAD makes it so that the chances of nuclear weapons being launched are near zero. The value of a weapon, when only quantifying the ability to use it, would be almost zero if the conditions of the world make it so it cannot be used.

In a scenario in which nuclear weapons are used, there are severe humanitarian, environmental, infrastructure, and public health externalities. The consequences, shown in Hypothesis 1, result in the elimination of human and animal life, infrastructure, and livable land. The understanding of the destructive capabilities of nuclear weapons created an international taboo against their use that is deeply entrenched in society.

Nuclear weapons derive their value as a deterrent. The costs of using the weapon are greater than the benefits, as supported by the collected evidence in H2 and H1. The consequences are understood to be too high, and although deterrence is valued, the existence of any nuclear weapons increases the possibility that the consequences will be realized. Therefore, I assign nuclear weapons to have a **low strategic value** compared to the value placed on mutual disarmament.

C1. CW. E1 – Deterrence Value

Historians theorize that the reason chemical weapons were never used in World War II was because of their property as a deterrence. There was mass development and

[182] "Nuclear Winter." *Encyclopedia Britannica*. Accessed January 5, 2020. https://www.britannica.com/science/nuclear-winter.

stockpiling of chemical weapons in the periods between the first and second world wars among world powers. The parity of chemical weapon ownership increased fears of retaliation. This is a positive benefit for chemical weapons.

C1. CW. E2 – Costs and Benefits

At the time, there was international consensus that it is socially taboo to use chemical weapons. This norm incentivizes states to punish users of chemical weapons, whether it be with an actual sanction, or making that violator into a pariah. Humanitarian concerns kickstarted the campaign against the use of chemical weapons. It is a weapon that causes unnecessary psychological and mental pain and suffering. The impetus for cooperation to ban chemical weapons was to ban states from being able to use the cruel method as a way of gaining the upper hand during war. The reactions to the use of chemical weapons proves more consequential to a state than the benefits from its use in terms of policy outcomes.

C1. CW. E3 – Effectiveness of the Weapon

The initial impetus for the mass development of chemical weapons during World War I was their ability to break stalemates during trench warfare. Chemical weapons were valuable due to a lack of conventional ammunition and the inability of conventional weapons to allow one side to get leverage over the other on the

battlefield[183]. The psychological fear induced by chemical weapons also enhanced the effects of traditional weapons. After the style of warfare shifted away from trench warfare, the initial conditions under which chemical weapons were useful no longer existed[184]. The existence of gas masks starting at the middle of World War I also renders chemical weapons ineffective. Chemical weapons offered a benefit for close range warfare. Due to the changing landscape of war, the strategic value of chemical weapons diminished. There are little to no benefits of having chemical weapons in a military arsenal for potential deployment.

Chemical weapons derive a small value as a deterrent. The public humanitarian taboo against chemical weapons triggers large costs for their use. Chemical weapons are also relatively ineffective due to the changing nature of war and available counter-measures. Therefore, I assign chemical weapons to have a **very low strategic value** compared to the value placed on mutual disarmament.

C1. BW. E1 – Deterrence Value

Biological weapons do not have a value as a deterrent. For it to have value as a deterrent, states would have to make public their stockpiling of biological weapons and use it to make credible threats. This never happened, because biological weapons violate humanitarian principles[185]. There is such a strong international taboo against the

[183] Fitzgerald, Gerard J. "Chemical Warfare and Medical Response During World War I." *American Journal of Public Health* 98, no. 4 (April 2008): 611–25. doi:10.2105/AJPH.2007.111930.
[184] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))
[185] "Deterrence, without Nuclear Winter." *Bulletin of the Atomic Scientists*, March 9, 2015. https://thebulletin.org/2015/03/deterrence-without-nuclear-winter/.

use of biological agents used to purposely infect humans that states have historically only developed these weapons in secret.

C1. BW. E2 – Costs and Benefits

At the time, there was a widely believed international norm against the use of biological weapons. This norm is that using biological weapons is immoral and inhumane. The vast acceptance of this norm was an effective deterrence for its use. Violating the norm is rationale for states to punish violators. States would be expected to turn a violator into a pariah, and reject it publicly. The shame of violating an international humanitarian norm would hurt this country's credibility and could affect cooperation with that country in the future. If the violator was found to be diverting biological research for harmful use using new technology, it could potentially lose the ability to use new technology in the future[186]. This harms dynamic innovation, which can cause the country to lag behind other countries that have high levels of innovation and research.

C1. BW. E3 – Effectiveness of the Weapon

Biological weapons are attractive due to the ease with which they can proliferate. First, the ingredients for bio-weapons are easily accessible. Anthrax can be found in nature, as it is a naturally occurring bacteria. The equipment needed to make a bio-weapon double as basic medical research equipment. Both agents and the equipment

[186] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))

needed can be bought easily from commercial medical supply companies. Biological weapons are also relatively cheap to make - they are referred to as the "poor man's atomic bomb".

Another pro of biological weapons is their ability to inflict damage without killing humans. One aspect of biological weapons is their ability to destroy an enemy's infrastructure. In World War II, Japan released diseased insects on China's rice fields, one of their main sources of food[187]. There is evidence that the USSR's biological weapons program dedicated a considerable amount of research to weapons that could destroy an enemy's food supply, economy, and morale. Strong infrastructure supports strong nations[188]. A country that wants to weaken an enemy can use biological weapons to strategically debilitate the foundations with which a nation stands on. This threat is very real because of advances in biology, especially in gene-editing techniques.

Advances in black biology - the diversion of gene manipulation for harmful purposes - have given scientists the ability to weaponize infections in a more efficient way[189]. Black biology can be used to increase the virulence and potency of a pathogen[190]. This is a very terrifying reality, but adds incredible valuable for biological weapons. With the existence of black biology and the right motive, scientists could realistically replicate this virus into a weapon with global consequences[191].

Outbreaks of infectious diseases can be made to look like natural outbreaks. This gives biological weapons a plausible deniability effect and thus are harder to attribute

---

[187] Ibid.
[188] Frischknecht, Friedrich. "The History of Biological Warfare: Human Experimentation, Modern Nightmares and Lone Madmen in the Twentieth Century." *EMBO Reports* 4, no. S1 (June 2003). doi:10.1038/
[189] Charlet, Katherine, and Katherine Charlet. "The New Killer Pathogens: Countering the Coming Bioweapons Threat." *Carnegie Endowment for International Peace*. Accessed April 5, 2020. https://carnegieendowment.org/2018/04/17/new-killer-pathogens-countering-coming-bioweapons-threat-pub-76009.
[190] "Chemical and Bacteriological (Biological) Weapons and the Effects of Their Possible Use :" Accessed May 10, 2020. https://digitallibrary.un.org/record/577282?ln=en.
[191] "Biological Warfare: An Emerging Threat in the 21st Century: 1/01." Accessed April 5, 2020. https://news.stanford.edu/pr/01/bioterror117.html.

to an attacker. Biological weapons, because of the aforementioned characteristics, are valuable to countries that do not have nuclear weapons[192]. This type of weapon is seen as an equalizer, that would put them on a more level playing field with countries that have military superiority.

There is a seemingly extensive list for why biological weapons have high strategic value to a country. Its ability to inflict high levels of damage at a low cost with the protection of plausible deniability gives it high value as an addition to a country's military strategies. However, biological weapons are incredibly unpredictable and thus are not used often. It also has no value as a deterrence. Therefore, I assign biological weapons to have a **low strategic value** compared to the value placed on mutual disarmament.

Given the existence of evidence **C1. NW. E1 and C1. NW. E2,** I conclude that nuclear weapons have **low strategic value.**

Given the existence of evidence **C1. CW. E1, C1. CW. E2 and C1. CW. E3,** I conclude that chemical weapons have **very low strategic value.**

Given the existence of evidence **C1. BW. E1, C1. BW. E2 and C1. BW. E3,** I conclude that biological weapons have **low strategic value.**

According to game theory principles, rational decision makers select the strategy that maximizes their payoff. **Thus, it gives me reason to believe that this hypothesis holds true.**

[192] Ibid.

Section VII – Testing Cybersecurity

In the last section, I found reason to believe that causal mechanisms exist in both Hypothesis 1 and Hypothesis 2. Traditional WMD are a proxy for cyberweapons. So, these causal mechanisms are affirmed in cyber. However, the non-cooperative outcome has not been reached in cybers, so the existence or lack of existence of my proposed causal mechanisms help us better understand why cooperation has not been reached in the cyber domain.

Hypothesis 1: Understanding a weapon's consequences make states more willing to cooperate

If this hypothesis were to be true, then we would see two clues:

Clue 1: the consequences of the weapon became understood

Clue 2: the understanding affected willingness to cooperate

Clue 1 would manifest in public declarations that signify the consequences as understood facts. Each declaration is a form of communication that imparts the knowledge of the consequences of the weapon onto other people. Types of evidence would therefore be any type of formal report confirming the damage done, publicized first-hand accounts, or quotes from prominent figures who are close to the subject.

To find evidence to support the existence of **clue 2**, I collect direct quotes from UN resolutions. The preambles of UN resolutions acknowledge the reason for addressing the topic. It is the place for member states to explain why they are cooperating, thus making it a good place to see if disarmament resolutions were influenced by an understanding of the consequences. Direct calls for cooperation are given in action items in the articles of the resolutions.

C1. CY. E1 – The Nature of Cybersecurity

As technology advances, the world is alerted to the new capabilities of cyberweapons by observing them. Some of the known consequences are denial of service attacks (DoS), file damage, ransomware, and data theft. Cyberspace can also be harnessed to carry out acts that are illegal in real life such as theft, extortion, and espionage[193][194]. The consequences of cyberweapons are familiar because anyone who has access to cyberspace can be a target. Unlike nuclear, chemical, and biological weapons, the average person is far more likely to be a victim of a cyberweapon at one point in their life. It is estimated that in 2019, there were 9.32 billion mobile phone connections[195]. This means that there are more than one billion more mobile device connections than there are people on Earth. The International Telecommunication Union (ITU) estimated that 4.1 billion people, or 53.6% of the world's population, were using the internet in 2019[196]. Cyberspace is everywhere, and most of the planet has taken advantage of it at some point in this past year. There have been many observed consequences of cyberattacks that can affect any one of those 9.32 billion connections with ease.

[193] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014))
[194] Other consequences and capabilities of cyberweapons are detailed when testing hypothesis 2
[195] "GSMA Intelligence." Accessed December 3, 2019. https://www.gsmaintelligence.com/.
[196] "Statistics." Accessed December 3, 2019. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

C1. CY. E2 – Public Reports of Attacks

Many companies are attacked with cyberweapons and are forced to publicly report the damages. That form of public acknowledgment signals the damages that cyberweapons can cause. Here are examples of companies that publicly reported the damages cyberweapons caused them:

eBay: Hackers access personal data from all 145 million users including emails and passwords. Hackers stole credentials from company employees to breach the company's datasets and remain unnoticed for months[197].

Marriot International: Hackers stole data from 500 million customers, including contact information, passport numbers, travel information, and other personal information. The credit card numbers and expiration dates of more than 100 million customers were believed to be stolen[198].

Facebook: Data firm Cambridge Analytica illegally harvested Facebook data from 87 million unsuspecting users. It used the data to build voter profiles in an attempt to influence American elections[199].

The victims of these cyberweapons could be anyone, since they cover social media platforms and companies that the average person is likely to frequent. There are also observed consequences of cyberweapons used by states, against other states. In 2010,

---

[197] "Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees - Business Insider." Accessed May 10, 2020. https://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5.

[198] Sanger, David E., Nicole Perlroth, Glenn Thrush, and Alan Rappeport. "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing." *The New York Times*, December 11, 2018, sec. U.S. https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[199] "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times." Accessed May 10, 2020. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Stuxnet infiltrated Iran's nuclear program. The virus took control of around 1,000 centrifuges that were enriching uranium, and made their motors tear the machines apart from the inside out[200]. Enriched uranium is an integral ingredient in nuclear weapons. The virus was thought to be designed by Israel and the US in order to slow Iran's nuclear program, since Iran making nuclear weapons was a threat to both countries. This was the first time that the world was really made aware of the capability of cyberweapons to infiltrate physical infrastructure. The virus itself opened the doorway for other actors to do the same, because once the virus is online, it provides a textbook like lesson on how others can replicate and modify it[201].

C1. CY. E3 – UN Mandate Language

The language of the OEWG's mandate acknowledges that the consequences of cyberweapons are understood:

"*Confirming* that ICTs are dual-use technologies and can be used for both legitimate and malicious purposes"[202]

"*Expressing concern* that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely"[203]

[200] 60 Minutes: Stuxnet (Columbia Broadcasting System, 2012), https://search.alexanderstreet.com/view/work/bibliographic_entity|video_work|2856063)
[201] Ibid.
[202] General Assembly resolution 73/27, Developments in the field of information and telecommunications in the context of international security A/RES/73/27 (5 December 2018), available from undocs.org/A/73/27
[203] Ibid.

"*Expressing concern* that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security,"[204]

C2. CY. E1 – UN Mandate Language

The language of the GGE and the OEWG's mandates acknowledge the need for cooperation:

GGE mandate

"*Noting* that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,"[205]

"*Underscoring* the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies,"[206]

OEWG mandate

"Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security"[207]

---

[204] Ibid.
[205] General Assembly resolution 73/266, Advancing responsible State behaviour in cyberspace in the context of international security A/RES/73/266 (22 December 2018), available from undocs.org/A/73/266
[206] Ibid.
[207] General Assembly resolution 73/27, Developments in the field of information and telecommunications in the context of international security A/RES/38/187 (5 December 2018), available from undocs.org/A/73/27

"States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect"[208]

Given the existence of evidence **C1. CY. E1, C1. CY. E2,** and **C1. CY. E3,** we have reason to believe that Clue 1 exists in our world.

Given the existence of evidence **C2. CY. E1,** we have reason to believe that Clue 2 exists in our world. **Thus, we have strong reason to believe that Hypothesis 1 holds true.**

Hypothesis 2: If the strategic value of a weapon is low, states are more willing to cooperate

I hypothesize that the strategic value of a weapon affects a state's willingness to enter into hand-tying cooperative agreements. The strategic value of a weapon is the intrinsic value that a country places on ownership of that weapon. I hypothesize that there is a causal link between strategic value and willingness to cooperate because states can only "enjoy" the full value of a weapon if it does not agree to tie its hands. See Appendix B for the methodology for H2.

C1. CY. E1 – Deterrence Value

[208] Ibid.

A cyberweapon can be used as a deterrent. The threat of punishment via a cyberweapon can be used to dissuade an adversary from escalating conflict. Cyberweapons can also be written so that their effect is reversible. The promise to reverse an effect if the target takes a certain action is also a credible form of coercion[209]. However, information sharing within the IT community creates parity in cybercapabilities and makes it harder to build effective weapons. In this condition, a cyberweapon loses its ability to deter.

C2. BW. E3 – Low Associated Costs

The most well-understood value of a cyberweapon is its flexibility. A cyberweapon uses code to create an action that would otherwise have to be done with soldiers, kinetic weapons, or spies[210]. Therefore, it is not limited to the same physical constraints. To act, an actor does not need to be in a specific location. To build and deploy a cyberweapon, an actor only needs the right technology and access to a network. The ability to remotely "detonate" a cyberweapon gives a lot more flexibility for its use[211]. Another advantage of such a malleable weapon is that it can be coded and designed to fit very specific goals. This is beneficial for two specific reasons. First, the code for a cyberweapon can be written with extreme precision so that it attacks a specific target. The ability to distinguish between a target and non-combatants, unlike most WMD, limits the number of civilian casualties. It also limits the risk involved to the personnel

[209] Smeets, Max, and Herbert S. Lin. "Offensive Cyber Capabilities: To What Ends?" In *2018 10th International Conference on Cyber Conflict (CyCon)*, 55–72. Tallinn: IEEE, 2018. doi:10.23919/CYCON.2018.8405010.
[210] Ibid.
[211] Ibid.

who "delivers" the attack. These personnel are safer sitting behind a computer screen than flying over a war-zone and dropping a bomb[212].

C1. CY. E3 – Effectiveness of the Weapon

Cyberweapons move war into an intangible platform, which gives the weapon an extremely covert nature. This makes it harder for the target, or third parties, to identify and punish the perpetrator of the attack. This is known as the hacker attribution problem. The problem is exacerbated with the development of technology to hide a perpetrator's trail. Perpetrators employ tactics to hide their Internet Protocol (IP) addresses such as using Virtual Private Networks (VPN) or proxy servers. An IP address is the cyber version of your actual address, it identifies your location and server used to "host" you[213]. Lack of an address that tethers a hacker to a specific location allows them to often slip into the void of cyberspace. Code has been developed to plant "red flags" that hackers use to lead investigators in the wrong direction when tracing an attack back to a source[214].

Knowing the chances of being caught and punished are low incentivizes an actor to value that outlet. Another value derived from covertness is the ability to use a cyberweapon as a form of non-public coercion. Cyber operations do not need to be exposed publicly. An actor can use a cyberweapon and then threaten to expose the target's vulnerability to the public. If the actor does not expose this, then the target can

---

[212] George Perkovich and Ariel Levite, *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017))
[213] "To Identify a Hacker, Treat Them Like a Burglar | WIRED." Accessed April 5, 2020. https://www.wired.com/story/case-linkage-hacker-attribution-cybersecurity/.
[214] "Russian Hacker False Flags Work—Even After They're Exposed | WIRED." Accessed April 5, 2020. https://www.wired.com/story/russia-false-flag-hacks/.

carry on without the public knowing that another actor has exploited a vulnerability in their system. This capability allows cyber actions to be a strong credible threat that can de-escalate conflict[215].

Cybercapabilities have many defensive purposes. Malware can be written to initiate both pre-emptive and preventative strikes. Nitro Zues is a US designed malware that intended to disable Iran's air defenses. Though never used, Nitro Zeus was a pre-emptive attack option as a result of the imminent threat that Iran's nuclear program carried[216]. Stuxnet, which was used, derailed the threat of an Iranian nuclear attack by destroying physical inputs for Iran's nuclear program. This is an example of the preventative capabilities of a cyberweapon. Cybercapabilities are also extremely cheap compared to other weapons. This makes it an attractive weapon for countries that don't have the money or resources to build large military arsenals. To put this into perspective, a one-hour denial of service attack can cost as low as $38[217]. One nuclear warhead supposedly costed North Korea $18-$53 million dollars[218].

There are relatively few inputs needed to build a cyberweapon. The main input is labor, but the skills needed to create a cyberweapon are highly transferrable, so labor is a cheap input. Cybercapabilities also benefit from the shared experiences effect. As more malwares are coded, the process to build one becomes standardized. It takes less time, effort, and money to write new codes, because many code writers just build off

---

[215] Smeets, Max, and Herbert S. Lin. "Offensive Cyber Capabilities: To What Ends?" In *2018 10th International Conference on Cyber Conflict (CyCon)*, 55–72. Tallinn: IEEE, 2018. doi:10.23919/CYCON.2018.8405010.
[216] Ibid.
[217] "Price of Website Disabling DDoS Attacks Fall to US$38 per Hour as Botnets Proliferate in China, Vietnam | South China Morning Post." Accessed April 5, 2020. https://www.scmp.com/tech/enterprises/article/1820464/price-website-disabling-ddos-attacks-fall-us38-hour-botnets.
[218] Blumberg, Yoni. "Here's How Much a Nuclear Weapon Costs." *CNBC*, August 8, 2017. https://www.cnbc.com/2017/08/08/heres-how-much-a-nuclear-weapon-costs.html.

already existing malwares[219]. This also adds to the adaptability value of a cyberweapon - they can be customized to fit any nature of attack or any goal.

There are a handful of aspects that detract from the value that the aforementioned characteristics provide. The biggest is the transitory nature of cyberweapons[220]. The constant development of cybercapabilities means that a weapon can only be effective for a short amount of time. A weapon only has temporary access to a computer system or network to cause damage, which inherently limits its destructive capabilities. Once the weapon is used, the target builds defenses against that particular attack. This renders the weapon effectively useless. There needs to be even more development of new weapons, which racks up time and costs, in order to stay ahead of the curve and create useful weapons. A byproduct of this is that there is more parity in cybercapabilities. It is a cheap weapon to build, and many of the inputs are easily accessible. This gives actors the means to build strong defensive cybercapabilities that can protect against attacks[221]. Cyberweapons are not as effective in deterring adversary action as other kinetic weapons such as traditional WMD. It also means cyberweapons are not as effective in compellence, because a parity in cybercapabilities lowers the credibility of using a cyberweapon as a threat.

Cybercapabilities offer a flexible, cheap, multipurpose, precise and covert weapon option. Although there are some drawbacks, those conditions also lead to more technological development, which could be seen as a positive. Therefore, after the evaluation of the evidence, I conclude that **cyberweapons have high strategic value**.

---

[219] "How Much Does a Cyber Weapon Cost? Nobody Knows." *Council on Foreign Relations*. Accessed April 5, 2020. https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows.
[220] Smeets, Max, and Herbert S. Lin. "Offensive Cyber Capabilities: To What Ends?" In *2018 10th International Conference on Cyber Conflict (CyCon)*, 55–72. Tallinn: IEEE, 2018. doi:10.23919/CYCON.2018.8405010.
[221] Ibid.

Section VIII – Conclusion

Findings

Hypothesis 1:

C1. NW. E1, C1. NW. E2, C1. NW. E3, C1. CW. E1, C1. CW. E2, C1. CW. E3, C1. BW. E1, and C1. BW. E2 supports the existence of Clue 1. Clue 1 is necessary for Hypothesis 1 to hold true. **C1. NW. E1, C1. CW. E1, and C1. BW. E1** supports the existence of Clue 2. Clue 2 is also necessary for Hypothesis 1 to hold true. **Thus, it gives me strong reason to believe this hypothesis holds true.**

Hypothesis 2:

Nuclear Weapons: Given the evaluation of clues **C1. NW. E1, and C1. NW. E2,** I have ascertained that nuclear weapons have low strategic value compared to the value of deterrence.

Chemical Weapons: Given the evaluation of clues **C1. CW. E1, C1. CW. E2, C1. CW. E3** I have ascertained that chemical weapons have very low strategic value compared to the value of deterrence.

Biological Weapons: Given the evaluation of clues **C1. BW. E1, C1. BW. E2, C1. BW. E3** I have ascertained that biological weapons have low strategic value compared to the value of deterrence.

According to game theory principles, rational decision makers select the strategy that maximizes their payoff. **Thus, it gives me reason to believe that this hypothesis holds true.**

Cybersecurity

After evaluating the cybersecurity case, I found that the causal mechanism affirmed in Hypothesis 1 exists in the cyber domain. Upon analysis of Hypothesis 2, I determined that cyberweapons have a high strategic value, thus the causal mechanism affirmed in Hypothesis 2 does not exist in the cyber domain.

Implications

After coming to these conclusions, I bring attention back to my research question: why are states willing to cooperate on some security issues and not others? When I set out to answer this question, I wanted to use my findings to understand why reaching a cooperative hand-tying agreement continues to pose a challenge in the cyber domain. I affirmed the causal mechanisms in Hypotheses 1 and 2 by testing them on traditional WMD. I justified why WMD serves as a proxy for cyberweapons. By looking at the cybersecurity case, I found that the causal mechanism in Hypothesis 1 holds. There is clear evidence that people understand the consequences of cyberweapons, and that it incentivizes states to cooperate to avert these consequences. This is a necessary condition to cooperation. Where cybersecurity diverges from traditional WMD is in the strategic value of the respective weapons.

Using my own methodology, I surmised that traditional WMD have lower strategic values than the value placed on mutual disarmament. I found that cyberweapons actually have quite a large strategic value compared to the value placed on mutual disarmament. Using game theory, I posit that weapons with lower strategic values make states more willing to enter into a hand-tying cooperative agreement. On the flip side, weapons with larger strategic values might influence states to choose an armament

strategy to enjoy the strategic value payoff, rather than collectively tie-hands and reach the payoff-maximizing outcome.

These results help make clearer why states are willing to cooperate on some issues and not others. My findings allow me to posit that states are having a harder time reaching a cooperative agreement on cyberweapons because the high strategic value detracts from their willingness to cooperate. Obstacles of that nature are not ideal in an area where states agree cooperation needs to happen to avoid understood consequences. The causal mechanism found in Hypothesis 1 is necessary, but not enough to push states over this cooperative obstacle. This leads me to believe that a low strategic value is essential in reaching cooperative outcomes.

A silver lining of this revelation is that the strategic value of a weapon is malleable. The changing landscape of war and technology alters the costs, benefits, and effectiveness of weapons. When the strategic value of a weapon changes, the payoffs of selecting "arm" strategies change as well. To reach the cooperative outcome, the strategic value, represented by the non-cooperative payoff, needs to be lowered so that the risk-minimizing equilibrium is not more attractive than the payoff-maximizing outcome.

Limitations and Extensions

The scope of this paper is limited by the nature of cybersecurity – it is an issue that changes every day. With time comes new understandings of the nature of the issue. It is like building a puzzle without looking at the box. As we find individual pieces that fit together, we get a better sense of what the bigger picture might be. We also might find that the pieces we already found do not fit. Only time will be able to help us complete the puzzle and see the full picture. One area of my paper that could be

strengthened from collecting more information is my methodology for measuring strategic value. I believe that as we learn more about cyberweapons, there will be more considerations for its value. While I support my method as is, I wish to expand the level of analysis in the future.

In this paper, I attempt to better understand causal mechanisms given the information that I have. Through process tracing, I was able to affirm that a causal mechanism existed. Process tracing has its limitations. It is a qualitative discipline that is still being updated and fleshed out by political scientists. Process tracing justifiably affirms the direction of the causal mechanism. This finding was very important for my analysis, but I recognize the probative value it holds is subjective. I justified why the reader should believe in this probative value. In the future, I would consider adding another layer to strengthen this probative value, maybe by seeing if there are applicable quantitative considerations.

There is a long list of things that can affect a state's willingness to cooperate. I cannot make a judgement on why states are or are not willing to cooperate based on two factors. There may be factors that will be integral to understanding in the future, when we have more information. However, I believe I did a sufficient job analyzing the factors I propose.

My conceptualization of cyberweapons as a new-age weapon of mass destruction sets up a framework for evaluating other potential causal mechanisms in the future. One major conversation that continues to plague states is the issue of non-state actors within a state's borders. Cyberspace is just as available to non-state actors as it is to states. This problem poses a lot of questions that states have not been able to fully answer yet such as: what responsibilities does the state have regarding malicious use of cyberspace within its own borders? These conversations are also happening in the

realm of traditional weapons of mass destruction. I implore future political scientists to delve deeper into this issue, using weapons of mass destruction as a proxy for cyberweapons, as I did.

Recommendations

There are important steps that states can take now, given the information we already have, to increase the likelihood of reading a hand-tying cooperative agreeement. States can work together to lower the non-cooperative strategic value of cyberweapons. In Section II, I detailed other forms of cooperation that were important to securing cyberspace. These arenas are going to be really important to help overcome obstacles to reaching a hand-tying agreement. Specifically, here are two preliminary steps that decision makers can take:

(1) Work to promote an international taboo against the unregulated use of cyberspace

Despite the changing nature of cyberspace, the world knows enough now to warrant concern. International decision makers should work to build acceptance of the norm that unregulated use of cyberspace by governments is harmful to all people. In the traditional WMD cases, the growing taboo against the use of the respective weapons put international pressure on states to cooperate. The backlash a state receives from "violating the norm" for cyberweapons, similar to in traditional WMD, would help pressure states into reaching a cooperative agreement.

(2) Create an international effort to help solve the "hacker attribution problem"

The inability to trace an attack back to a source is one of the most valuable characteristics of cyberweapons. It poses a difficult problem for international lawmakers: how can you punish a state if you cannot determine which state is

responsible? The NPT and the CWC have strong verification and monitoring mechanisms to help identify states that are cheating on the agreements. Cyberspace, being intangible and invisible, needs this, but makes it very hard. International lawmakers should create a streamlined process for sharing open-source information in an effort to create technology that can help identify perpetrators of cyberattacks. This will make cyberweapons lose a lot of its perceived value.

As mentioned before, this is a problem that will take time and more information to solve. A better understanding of the reasons why states are willing to cooperate can help shorten this time period. Lowering the strategic value of cyberweapons is integral in pushing states away from a non-cooperative outcome. As I have shown, the understanding of consequences is not enough to make a state willing enough to cooperate to overcome the barrier that a weapon with high strategic value poses. I believe that by taking the two aforementioned "next steps", states can be in a better space to achieve a hand-tying cooperative agreement, as well as common long-term goals, such as the ones provided by Chernenko, Demidov, and Lukyanov (2018). By taking a comparative approach, I believe my findings provide a unique perspective that can help decision makers reach sufficient levels of international cooperation. It is important that relevant parties keep contributing to this conversation. We are all worse off with unregulated cyberspace, whether we are playing the cooperation game, or just observing.

Appendix A

Relevant Definitions[222]

Cyber infrastructure: An electronic information and communications systems and services and the information contained therein

Cyber-attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity

Cyberspace: The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation

Cyberwarfare: The actions by a nation-state or international organization to attack and attempt to damage another nation's computers or Information and Communication(s) Technology (ICT)

[222] Selected from The National Initiative for Cybersecurity Careers and Studies (NICCS) Glossary at https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Data Breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information

Denial of Service (Dos): An attack that prevents or impairs the authorized use of information system resources or services

Information and Communication(s) Technology (ICT): Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Malware: Software that compromises the operation of a system by performing an unauthorized function or process

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer

Appendix B

Standard for collecting evidence

Each country's government, especially their executive or military branches, place intrinsic values on ownership of different types of weapons. It is difficult to quantify the exact value that an object, or a class of objects, has. Most attempts to do this rely on monetary assessments. For example, the US Government Accountability Office conducts weapon system analyses every year to assess the monetary value of military weapons. I have created an innovative and original way to assess value that does not involve monetary costs. I assess the value of a weapon by evaluating the costs, benefits, and effectiveness of each of the weapons. The characteristics are found using a guiding set of questions that intuitively would be reasons to or to not invest in the weapon.

Assumptions

Value, as measure it, is the value of having a weapon at one's disposal. Therefore, it is an assumption that the value is represented in the armament strategies (B) and (C) with no hand tying. The individual payoff ranking for the stag-hunt is $A > B \geq C > D$. Therefore, we can assume that the value of the weapon with no hand-tying is lower than the value given to mutual disarmament.

Guiding Questions

(1) If the weapon were to not be used, is there value in stockpiling?

Rationale: Some weapons derive their value from being stockpiled, not used. I consider the deterrence value of stockpiling a weapon in my analysis.

(2) Are there more benefits than costs associated with using the weapon?

Rationale: I hypothesize that a weapon is seen as having high strategic value when it can achieve an objective while retaining a net positive payoff to a user. A net positive payoff is when the relative benefits of a weapon are greater than the relative costs of the weapon. Intuitively, if a weapon brought more costs than benefits, an actor would not use it according to rational choice theory. Therefore, I do a qualitative cost benefit analysis when evaluating

(3) Is it an effective weapon?

Rationale: There could be many reasons why a weapon is not effective anymore. It could be the changing landscape of war, the emergence of better-suited weapons, or the development of effective counter-measures. Understanding if, rationally, an actor would use this weapon to achieve its goals needs to be considered when ascertaining value.