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

6 April 2020

Table of Contents

Table of Contents *1*

Abstract **2**

Acknowledgments **3**

Section I – Introduction *4*

The Hypotheses **7**

Section II – Using the Literature *9*

Section III– Conceptualization *10*

Application of International Legal Norms **11**

Rectifying the Difference Between Traditional Weapons and Cyberweapons **13**

Section IV – Methodology *14*

Process Tracing **14**

Case Studies **16**

Game Theory **17**

Section V – Case Studies *19*

Nuclear Weapons: The Treaty on the Non-Proliferation of Nuclear Weapons **19**

Chemical Weapons: The Chemical Weapons Convention **25**

Biological Weapons: The Biological Weapons Convention **34**

Section VI – Hypothesis Testing *40*

Hypothesis 1: As consequences become more understood and made tangible, cooperation becomes more likely **40**

Hypothesis 2: As the attribution of violation becomes harder, cooperation becomes less likely **56**

Hypothesis 3: When the benefit of the status quo is large enough, cooperation becomes less likely **65**

Hypothesis 4: As the tactical value of a weapon increases, cooperation becomes less likely **76**

Section VII – Conclusion *92*

Findings **92**

Implications **94**

Recommendations **95**

Appendix 1 ..... *97*

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 do states 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 three situations that create obstacles to cooperation on security issues: a lack of understanding of a weapon's consequences, a difficulty attributing an attack to a specific attacker, and when a weapon has a sufficiently high tactical value. 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: methods for global information sharing to better understand the cyberweapons problem and promotion of an international norm against the use of unregulated cyberspace.

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 a 100-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. I'd also like to thank the University of Michigan Law Library for housing me for the past four years. At least 90% of this project was written there.

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 the technological advancement, barriers to access technology have all but disappeared. It is estimated that in 2019, there were 9.32 billion mobile phone connections[1]. 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[2]. Cyberspace is everywhere, and most of the planet has taken advantage of it at some point in this past year. 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 to our planet, the potential risks it brings are tremendous. Throughout the past couple of decades, cyber threats have become more prevalent. Cyberspace is being harnessed by both private and public actors as a weapon. In 2010, the virus Stuxnet destabilized Iran's nuclear program by shutting down machines that were used to enrich uranium. Six years later, Russian state-backed hacking groups launched an information warfare campaign to influence the outcome of the 2016 US Presidential Election. These are just two of the many examples of the mal-use of cyberspace to wreak havoc in another state's affairs. On the more individual level, we can look to Cambridge

[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.

Analytica's illegal harvesting of personal data from 87 million unsuspecting Facebook users. These three examples bring to the forefront the treacherous consequences of cyber-attacks that can harm both states and individuals alike. Cybersecurity 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.

Throughout history, states have come together after a crisis to negotiate some type of agreement or form an international institution to make sure that similar crises never happen again. There has been a plethora of cyberattacks in the past couple of decades. These include attacks on governments and government infrastructure such as Stuxnet and the US election hacking. These cases of cyberweapons being used to target states are emblematic of the potential of states to harness these weapons and use them against each other. Although this may not be considered a "crisis" yet, the possibilities and subsequent consequences are critical enough to cause alarm. States across the globe have outwardly called for solutions to the destabilizing threat of cyber warfare, noting how damning it can be to governments and the citizens within their borders. It is surprising, then, to hear that states have not come together to try and solve this issue like history would suggest. Besides the United Nations Office of Disarmament Affairs (UNODA) taking up research on the issue, there are few comparable attempts to cooperate on a global scale. A United Nations mandated working group, the Group of Governmental Experts (GGE) is mandated to advance responsible state behavior in cyberspace in the context of international security[3]. The group, created in 2013 failed to

[3] "UN GGE and OEWG | GIP Digital Watch Observatory for Internet Governance and Digital Policy." Accessed October 8, 2019. https://dig.watch/processes/un-gge.

come to a consensus on an outcome report, prompting the international community to call the event the "death of the GGE"[4].

The failure of the GGE left a gaping hole in the international conversation on cybersecurity. This was particularly worrisome because cybersecurity is an issue that continues to become more of a threat every day. Technology advances at such a rapid rate, that if relevant actors are not keeping up with the efforts to mitigate the threat, it may run afoul. International non-cooperation leaves both people and states vulnerable to these destabilizing threats. Without an attempt to codify some type of regulation to outlaw the use of cyberspace as a weapon, both public and private actors have nothing holding them accountable. In 2019, the GGE was revived, along with an Open-Ended Working Group (OEWG) on cyberspace. This rebirth was precipitated by a world understanding of how dangerous a lack of cooperation can be.

Through my research, I aim to figure out why states have not cooperated in a deep a sustained manner - the way we assume would happen. To understand cooperation on cybersecurity, it is integral that I broaden the scope to international security and disarmament issues in general. Understanding why cooperation lends itself to security issues more broadly will allow me to critically analyze the specific case of cybersecurity more thoroughly. This view has prompted my research question: why do states cooperate on some security issues and not others? Once I can identify the relationship between cooperation and security issues, I can then provide an additional contribution to the conversation. By understanding where cooperation is strained, I can then propose solutions to remedy these issues. Policy proposals are integral in a field

[4] "The Year in Review: The Death of the UN GGE Process? | Council on Foreign Relations." Accessed March 20, 2020. https://www.cfr.org/blog/year-review-death-un-gge-process.

that has few, but needs many. The sooner governments can act, the sooner we can make headway on protecting people from cyberweapons.

It only seems fitting that I take a non-traditional approach to this problem. Since there is relatively little discourse in political science on the intersection of cooperation and cybersecurity, I had the pleasure of piecing together different parts of the literature as a jumping off point for my project. I will attribute the relevant literature in Section II, and throughout my conceptualization and methodology. In Section III, I will detail my conceptualization. Since cyberspace is a non-traditional arena of war, the understanding of cyberspace as a cyberweapon is the most integral part of my paper. In Section IV, I will outline my methodology and provide justification for my research design. I employ a comparative analysis of four different types of international security and disarmament issues: nuclear weapons, chemical weapons, biological weapons, and cyberweapons. I rely on process tracing and game theory to analyze my cases, and will argue at length why these are the best fit for my research design. My case studies appear in Section V. Section VI, the meatiest part of my thesis, will be where I provide evidence and do that actual task of process tracing for my hypotheses. Section VII will conclude my paper, report my findings, and propose next steps on the issue.

The Hypotheses

For each hypothesis, I collect evidence to support "clues". For any given clue, I evaluate how much that tells me about the likelihood of the hypotheses being at play. Throughout my research, I continually ask the question: "what would we see in a world where this hypothesis holds true?" I propose these four hypotheses because I believe they are all at play in affecting cybersecurity cooperation. Each of the individual

hypotheses is tested as if we live in a world where that specific hypothesis holds true, barring consideration of the rest. However, when trying to answer my research question, it is important to analyze the overall levels of cooperation, taking all hypotheses into consideration. In the real world, all of these hypotheses could play a part in affecting cooperation. There could be a plethora of factors that I have not even considered.

My four hypotheses are:

1) As the consequences of a weapon become more understood or made tangible, cooperation becomes more likely

2) As the attribution of violation becomes harder, cooperation becomes less likely

3) When the benefit of the status quo is large enough, cooperation becomes less likely

4) As the tactical value of a weapon increases, cooperation becomes less likely

For the hypotheses that I did not have enough information or understanding to test, I decided to focus on hypothesis generation. The value of hypothesis generation in this ongoing issue is tremendous, as it sets up the pins for the future political scientists to knock down when the world is in a place where we can better do that. I feel confident that we have enough information known to test hypotheses 1,2, and 4, and make a strong conjecture about their existence. I focus on generating theory and gathering initial evidence for Hypothesis 3. I have found that there is enough evidence to support the existence of causal mechanisms in hypotheses 1,2, and 4. The strength of the clues I gather bolster the aforementioned proposed relationships between a cause, and the subsequent effect on state cooperation. In Section VII, I use each specific hypothesis, in conjunction with the others, to detail why we see more cooperation on traditional weapons of mass destruction than we do for cyberweapons.

Section II – Using the Literature

The cybersecurity cooperation issue is relatively new to academia. The youngness of the cybersecurity issue means there has been little discourse compared to other security issues that have existed for much longer. A characteristic of the existing literature revolves around better understanding cybersecurity and identifying the issues that it poses for governance and cooperation. Bradshaw (2015) posits that cooperation on cybersecurity emerges when there is a high degree of trust and information sharing between actors[5]. However, she acknowledges that cybersecurity involves a plethora of different actors with varying preferences, which can hinder trust and information sharing. These are characteristics of a distribution problem, according to Koremenos (2016), which hinders cooperation[6]. Rueter (2014) also suggests that cooperation is being hindered by a lack of trust. This trust is inherent to the security dilemma: security-seeking states may be uncertain about the intention of other states. He applies this framework to better understand the lack of cooperation with cyberweapons[7]. Chernenko, Demidov, and Lukyanov (2018) provided recommendations for jumpstarting international cooperation that include US - Russia dialogue, requiring state reports of cyber vulnerabilities, and reconvening the GGE. On a larger scale, they proposed the creation of international cyber law, an international cyber court, and a worldwide cyber convention[8].

---

[5] Bradshaw, Samantha. "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," n.d., 24.
[6] Koremenos, Barbara. *The Continent of International Law: Explaining Agreement Design*. Cambridge: Cambridge University Press, 2016. doi:10.1017/CBO9781316415832.
[7] Rueter, Nicholas C. "The Cybersecurity Dilemma," 2011, 72.
[8] "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/.

Rather than focusing on the proposed distribution problem, I am using a comparative analysis to broaden the conversation about cooperation. By understanding why cooperation lends itself to certain security issues more than others, I hope to plant a seed that will grow into a more in-depth conversation on how states can cooperate to mitigate cybersecurity risks. To make this contribution, I will be pulling from multiple literatures: the international law and cooperation literatures. The literature on these issues provides a strong framework for analyzing the cybersecurity problem. Using pre-existing international law principles lends credence to my comparison of traditional weapons of mass destruction to cyberweapons. There is extensive international cooperation literature, which is the basis for understating why, when, and to what degree states cooperate on issues. These two international relations literature subclasses will help me defend my conceptualization.

To justify my methodology, I turn to the process tracing and game theory literature. Process tracing is used to analyze cause and effect, thus making it a strong guide as I work through causal relationships in international cooperation. The game theory literature includes a substantial body of work on using game theory as a metaphor, rather than a formal model, in understanding cooperation.

Section III– Conceptualization

I am conceptualizing the cybersecurity issue as an issue of cyberweapons. It is beneficial to look at cybersecurity as a weapons issue because international law has well-defined regulations of states' use of weapons. There are two important prongs of my conceptualization. The first is the ability to apply international legal norms to

cyberweapons. There is currently no international cyberweapon law codified. However, I argue that in order to understand why that may be, we need to apply pre-existing international legal frameworks to the issue. The second prong justifies why we are allowed to do this in political science discourse. I argue that based on shared norms and characteristics, cyberweapons should be thought of as a weapon of mass destruction.

Application of International Legal Norms

International law has a well-defined framework for dealing with states' use of weapons. Therefore, applying something concrete to an underdeveloped area will help me work through it. I argue that international legal frameworks can be applied to cyberweapons because these weapons are fundamentally the same as tangible weapons, which have been subject to international legal norms and customs for many decades. Looking towards international legal frameworks is a way to better understand potential cybersecurity cooperation. The solution to the problem at hand hinges on government cooperation, so relevant laws and institutions should be applied when considering the issue.

Arguably the most important piece of literature in this regard comes from the Group of Governmental Expert's (GGE) 2013 meeting. The GGE is a United Nations (UN) mandated working group working in the field of information security. Their most notable achievement came in 2013 when they published a report linking international law to cyberspace[9]. 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

[9] 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

relevant international law statutes and norms is an essential cooperative measure to reaching cyber threat elimination[10].

Puyvelde and Brantly (2017) continue this method of analysis on a more theoretical level[11]. They look at the UN Charter for rules regarding war and aggression. 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"[12]. But in Article 51, the Charter confirms the right to "individual or collective self-defense" in the face of armed attack[13]. The main takeaway from the Charter is that nation-states should refrain from aggression, but the use of force is appropriate in the face of an attack[14]. In terms of war, these existing guidelines apply to physical war and armed attacks, which have characterized the traditional arena of war throughout history. Cyberwar is not a physical war and has yet to translate into physical armed attacks. However, the "threat or use of force against… any state"[15] can be understood as the reason behind many cyber-attacks. Cooperation hinges on the common understanding of international legal norms. Therefore, Puyvelde and Brantly propose that in order to be able to move forward with cybersecurity cooperation, states need to reinterpret the principles in the UN charter and apply them to cybersecurity[16]. The GGE and the OEWG reaffirmed the ability to apply the UN charter to cyberspace at their first 2019 session[17].

---

[10] Ibid.
[11] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[12] U.N. Charter art. 2,¶ 4.
[13] Ibid. art. 51
[14] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[15] U.N. Charter art. 94,¶ 1.
[16] Damien Van Puyvelde and Aaron Franklin Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge, UK: Polity Press, 2017)
[17] 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

Rectifying the Difference Between Traditional Weapons and Cyberweapons

The key distinction between cyberweapons and traditional weapons 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, which have been regulated under international disarmament law for decades. 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[18]. 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 a result of the weaponization of cyberspace[19]. This possibility warrants approaching cybersecurity as a disarmament issue.

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, and more generally, society. The discoveries of the destructive capabilities of cyberweapons - namely their ability to remotely control a country's infrastructure and steal private data, has led many to call for limitations on its use. Without limitations in the form of law, the weapon proliferated and evolved.

A/RES/68/98 (24 June 2013), available from undocs.org/A/68/98

[18] "1868 Saint Petersburg Declaration | Weapons Law Encyclopedia." Accessed April 4, 2020. http://www.weaponslaw.org/instruments/1968-Saint-Petersburg-Declaration.

[19] "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/.

Throughout my case studies, namely Hypothesis 1, I will show how this process has mirrored that of traditional weapons of mass destruction.

The emergence of cyberspace as a new arena for war means we need to shift our mindset of disarmament to a more abstract interpretation. We do not fully understand the destructive capabilities of cyberweapons, and we should proceed with caution and a sense of urgency. With weapons of mass destruction, states came together to collectively disarm, or at least prohibit the use of weapons, due to their destructive capabilities. These sentiments exist within the realm of cyberweapons. States have the capabilities to harness cyberspace in the form of a dangerous weapon. These observations lead me to ask two questions: What can explain why cyberwarfare is systematically different from traditional weapons of mass destruction? Why are states not agreeing to collectively control or disarm a weapons proliferation?

Section IV – Methodology

Process Tracing

To answer my research question, I have to gain insight into the nature of cooperation problems. This rather exploratory quest guided me to process tracing as a means of hypothesis testing rather than the analysis of hard data. Process tracing is the practice of tracing a process in order to find a causal mechanism through which the cause brings about the effect[20]. By carefully noting the trajectory of change, we can better understand what causal mechanism is in operation. For this paper, the effect is

[20] Collier, David. "Understanding Process Tracing." *PS: Political Science & Politics* 44, no. 04 (October 2011): 823–30. doi:10.1017/S1049096511001429.

cooperation on a security issue. I test my hypotheses by collecting clues that show if there exists a causal mechanism that has an effect on changing the degree of cooperation. Fairfield and Charman[21] (2017) apply Bayesian analysis to process tracing that I find helpful for my paper. They argue that after assessing the weight of the evidence for each observation, we can infer the probability that a specific causal mechanism is causing the effect. There exists a rational degree of belief that we should have in a hypothesis in light of the information we have collected.

In a world where the hypothesis holds true, we would see certain clues. The existence of these clues holds a certain probative value, blind to the evidence that exists, that helps me assess the rational degree of belief. These probative values are as follows:

(1) Low probative value → not sufficiently useful to prove we have reason to believe the hypothesis holds true

(2) Probative value → sufficiently useful to prove we have reason to believe the hypothesis holds true

(3) High probative value → sufficiently useful to prove we have strong reason to believe the hypothesis holds true

I look for evidence in our world to show the existence of these clues. The supported existence of the clues allows me to evaluate the reasonable probability that the hypothesis holds true. The structure I use to trace this process is: presenting the hypothesis, presenting the clue(s), presenting the evidence for the clues, and then evaluating the probability that the hypothesis holds true. 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

[21] Fairfield, Tasha, and Andrew E. Charman. "Explicit Bayesian Analysis for Process Tracing: Guidelines, Opportunities, and Caveats." *Political Analysis* 25, no. 3 (July 2017): 363–80. doi:10.1017/pan.2017.14.

cyberweapon. For example, nuclear weapon evidence piece 3 for clue two is stylized as "**C2. NW. E3"**. I do this for hypotheses 1 and 2. For Hypothesis 4, I use my own methodology, which is detailed in Appendix 1.

Finding no evidence in a case study is a telling result in of itself. I use Philosopher John Stuart Mill's method of difference to justify why a lack of evidence matters in understanding the degree of reasonability for the hypothesis. This method compares instances of effects and finds what they do not have in common. If there are factors that exist that lead to one outcome, and those factors do not exist and then lead to the opposite outcome, we can infer this factor is the cause[22]. The main limitation to this method is that it attempts to extrapolate a singular cause in order to explain the causal mechanism. I acknowledge that there may be a plethora of factors affecting the cause, thus I cannot use the method of difference to draw a decisive conclusion on its own. I rely on collecting sound evidence to support the existence of clues. The intuition behind Mill's principle signals that when finding no evidence in a case study leads to the opposite outcome, we can use the resulting causal inference to supplement the evidence collected for the hypothesis.

Case Studies

I conduct a case study on traditional weapons of mass destruction (WMD). My three cases are nuclear weapons, chemical weapons, and biological weapons. In order to find out why states have not yet cooperated on cyberweapons, it is necessary to look at security issues more broadly. Nuclear, chemical, and biological weapons were all technological advancements that threatened the traditional arena of war upon

[22] "[S05] Mill's Methods." Accessed April 4, 2020. https://philosophy.hku.hk/think/sci/mill.php.

inception. When each weapon came onto the scene of war at its respective time, there was uncertainty about the nature of the weapons and their consequences. Most, if not all, work on disarmament and protection measures had only been done for traditional weapons. This forced governments to think about different ways to solve these new age issues. We have seen the same thing happening with cyberweapons.

By looking at the nature of cooperation in each of these issues, I can better hypothesize how security issues differ in cooperation problems. Through process tracing, I will be able to evaluate if certain causal mechanisms exist in different cases. These findings will better help me understand how cooperative obstacles can be overcome in cyberweapons.

Game Theory

I turn to game theory to better understand strategic interaction. I use the principles of cooperative games as a guide in evaluating when and where we see cooperation on security issues. I will use the mechanisms of a game to guide an analysis of the cooperation landscape today as if it were a cooperation game. 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 and that utility refers to some ranking of the subjective benefit that an actor receives from a set of objects or events. Rational decision makers choose strategies that aim to maximize their utility[23].

The players in this "game" are countries (international decision makers). Their pure strategies are "cooperate" and "do not cooperate". As this is an analogy, we will assume

[23] 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.

there are no mixed strategies. The players' payoffs are the utility they derive from either of their pure strategies. As utility maximizing rational agents, the players will choose whatever strategy maximizes their payoff. This is the framework we will use to understand the behavior of countries when it comes to international security and disarmament cooperation. Payoff structures are the list of outcomes that are assigned a utility. Payoffs are ranked based off of the welfare that the actor gets from the select strategy after all other players have selected their strategies. From there, we can better understand how countries derive utility. All of my hypotheses try to postulate how countries formulate payoff rankings and thus choose strategies. These strategies are observable after the cooperation "game" is over, and we know all players' selections.

A final assumption is necessary for this paper: utility is derived from a cost benefit analysis. I analyze cooperation in terms of incentives. The utility derived from a payoff incentivizes a strategy to be taken. Cost benefit analysis is the heart of incentives. This cost benefit analysis is woven into my process tracing, especially for Hypothesis 4. I build a case from a set of clues during my evidence gathering stage. I will assign the clues to be a cost or a benefit and then evaluate how they compound to create a net payoff. Here is the template of cost benefit analysis that I am going to use:

1) Net payoff of cooperation > net payoff of non-cooperation —> more likely to cooperate

1) Net payoff of cooperation < net payoff of non-cooperation —> less likely to cooperate

Note that I say less/more likely to cooperate rather than will/will not cooperate. I use this analysis on individual hypotheses as a means of process tracing. However, these hypotheses are not mutually exclusive and there are too many uncertain variables in the world to make an unqualified statement.

Section V – Case Studies

I have chosen the traditional weapons of mass destruction (WMD) as my case studies. 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 into the arena of war forced the world to create a cooperative outcome.

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 the use of nuclear weapons. It is the only ratified agreement regulating the non-proliferation of nuclear weapons[24]. The NPT was precipitated by a changing international taboo against the use of nuclear weapons[25]. 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 fear of a nuclear world war was increased by the reality that even more countries would obtain

[24] The Comprehensive Test Ban Treaty was adopted in 1996, but has yet to be ratified.
[25] "Treaty on the Non-Proliferation of Nuclear Weapons - Main Page." Accessed February 17, 2020. https://legal.un.org/avl/ha/tnpt/tnpt.html#.

nuclear weapons if nothing was done to stop them. This spurred an anti-nuclear rhetoric that seeped into the international discourse[26].

On 8 December 1953, US President Dwight D. Eisenhower gave his "Atoms of Peace" speech to the UN General Assembly. In this 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[27]. Eisenhower warned that the knowledge of nuclear weapons was spreading throughout the world, which warranted international concern. After 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. This agency would also carry out safeguards to promote the sharing of materials and information needed to conduct peaceful nuclear energy research[28]. 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[29].

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. However, the inability of the USSR and the US to cooperate on halting their nuclear arms race at the height of the Cold War rendered the IAEA unable to fully execute its functions. In 1960 and 1964 respectively, France and China started

---

[26] Ibid.
[27] "Atoms for Peace Speech." Text. IAEA, July 16, 2014. https://www.iaea.org/about/history/atoms-for-peace-speech.
[28] Ibid.
[29] Putte, D 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.

nuclear stockpiles. This proliferation, coupled with the Cuban Missile Crisis of 1962, heightened the need for legally binding safeguards against nuclear proliferation[30]. The NPT went into effect in 1970, thirteen years after the creation of the IAEA. Here is the timeline of the international cooperation that lead to the NPT[31,32]:

-29 July 1957: The IAEA enters into force as an international organization independent of the UN to promote peaceful use of nuclear energy.

-17 October 1958: Nuclear non-proliferation is first introduced as a topic that warranted serious consideration at the 13th session of the General Assembly in a draft resolution in the Disarmament and International Security Committee (DISEC, First Committee).

-September 1959: Nuclear-nonproliferation is considered on the agenda of the 14th session of the General Assembly on recommendation from the First Committee.

-20 November 1959: The General Assembly adopts Resolution 1380, which suggests the Ten-Nation Disarmament Committee (TNDC) consider appropriate means to avert the danger of nuclear weapon proliferation. The TNDC consisted of European countries, the USSR, and the US.

-15 March - 28 June 1960: The TNDC meets but does not actually discuss nuclear non-proliferation despite recommendation from the General Assembly

-20 December 1960: General Assembly adopts Resolution 1578 at its 15th session, which enforces the need for a permanent agreement to stop the spread of nuclear

---

[30] Ibid.
[31] The entirety of the following timeline comes from the United Nations Audiovisual Library of International Law's NPT Procedural History page (citation in footnote 31)
[32] "Treaty on the Non-Proliferation of Nuclear Weapons - Main Page." Accessed March 20, 2020. https://legal.un.org/avl/ha/tnpt/tnpt.html.

weapons. The necessity for a better understanding of nuclear proliferation implications is heavily promoted by the General Assembly and DISEC during this session.

-4 December 1961: The General Assembly adopts Resolution 1664 which requests the Secretary-General to make an inquiry regarding the conditions under which non-nuclear weapon states would be willing to enter into an agreement to refrain from acquiring and manufacturing nuclear weapons.

-20 December 1961: The General Assembly resolution 1722 establishes the Eighteen Nation Disarmament Committee (ENDC), the successor of the TNDC, established by the USA and the USSR to negotiate "general and complete disarmament under effective international control".

-15 March and 18 April 1962: The USSR and US respectively present the first draft treaties on general disarmament, which includes articles on nuclear non-proliferation.

-10 October 1964: Nuclear non-proliferation as a specific topic is added onto the General Assembly's agenda for the first time. Before the 19th session, the General Assembly and the ENDC debated nuclear non-proliferation in the more general discussions on disarmament.

-17 August and 24 September 1965: The ENDC meets during the General Assembly's 20th session and the US and USSR respectively introduce the first draft treaty on the non-proliferation of nuclear weapons

-4 November 1966: The General Assembly adopts Resolution 2149, which appealed to all states to take steps to achieve the earliest possible time for the conclusion of a nuclear non-proliferation treaty. It also called for a cessation all activities that would be conducive to proliferation.

-24 August 1967: The USSR and the US submit separate but identical draft treaties on nuclear non-proliferation.

-11 March 1968: The USSR and the US submit a joint draft treaty during an ENDC conference.

-12 June 1968: The General Assembly revises the draft treaty and adopts resolution 2373, in which it commended the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and requested the Depository Governments open the treaty for signing.

-1 July 1968: The Treaty on the Non-Proliferation of Nuclear Weapons was opened for signature in Moscow, USSR, London, UK, and Washington D.C., US.

-5 March 1970: The Treaty enters into force after 40 states and the Depository Governments signed.

-1995: At the 1995 NPT Review Conference, the Treaty was voted to extend indefinitely.

The treaty focuses on 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. The NPT entrusts the IAEA as the inspectorate for ensuring compliance with its non-proliferation and disarmament clauses[33]. The IAEA has two-fold responsibilities: the first is verification of no deviations from peaceful nuclear energy activities for non-nuclear weapon states. The other is verification of the accuracy of activity reports from confirmed nuclear weapon states[34]. The verification of accuracy and non-deviation are how the IAEA monitors compliance with the NPT. The NPT also contains duration provisions in Article X[35]. The duration of the NPT will be reviewed every 25 years, with overall reviews every five years. In 1995, the Treaty was extended indefinitely. The

[33] "Background Information." *UNODA Meetings Place*. Accessed March 13, 2020. https://meetings.unoda.org/section/conf-npt-2020-background-inf/.
[34] "Safeguards Agreements." Text. IAEA, June 8, 2016. https://www.iaea.org/topics/safeguards-agreements.
[35] "Treaty on the Non-Proliferation of Nuclear Weapons (NPT) – UNODA." Accessed April 4, 2020. https://www.un.org/disarmament/wmd/nuclear/npt/text/.

review conferences allow for additional measures to be approved in order to strengthen the NPT, learn about, and adapt non-proliferation measures to the changes in both the state of the world and advancing nuclear technology[36].

There has been success in stopping nuclear proliferation. At its height in 1986, the world nuclear stockpile totaled about 64,500. The USSR stockpiled 40,159 and the US had 23,317 warheads. After the disbanding of the USSR, tensions eased and states began destroying or retiring their nuclear stockpiles[37]. Currently, there are estimated to be around 14,000 nuclear warheads stockpiled. More than 90% of those belong to the US and Russia[38]. The IAEA has facilitated this downward trend, and continues to monitor both confirmed weapon states and non-weapon states for compliance. Even though the NPT is mostly successful in disarmament, it is criticized for its inability to fully promote non-proliferation. Iran is a member of the NPT, but was found in non-compliance by the IAEA in 2009. The IAEA found evidence of Iran's nuclear program prior to 2003, but deemed there were no weaponization activities post 2009[39]. North Korea acceded to the treaty in 1985, but withdrew in 2003. In 2005, North Korea announced the existence of its nuclear weapon program[40]. There are other non-signatories that possess nuclear weapons and do not fall under NPT regulations. India, Pakistan, and Israel are not currently state parties to the NPT. India and Pakistan have publicly announced the existence of their nuclear weapon programs. Israel is generally believed to have nuclear weapons, but commits to a policy of ambiguity[41]. There are an estimated 420 nuclear

---

[36] "Background Information." *UNODA Meetings Place*. Accessed March 13, 2020. https://meetings.unoda.org/section/conf-npt-2020-background-inf/.
[37] "Status of World Nuclear Forces." *Federation Of American Scientists*. Accessed January 21, 2020. https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/.
[38] "SIPRI Yearbook 2019, Summary," n.d., 24.
[39] "Nuclear Weapons: Who Has What at a Glance | Arms Control Association." Accessed January 21, 2020. https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.
[40] "Fact Sheet on DPRK Nuclear Safeguards." Text. IAEA, July 25, 2014. https://www.iaea.org/newscenter/focus/dprk/fact-sheet-on-dprk-nuclear-safeguards.
[41] "SIPRI Yearbook 2019, Summary," n.d., 24.

warheads stockpiled by the non-NPT states. Due to uncertainty about the state of the world and the inability of the NPT to regulate all nuclear weapon states, the threat of nuclear war still remains.

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 proliferation is largely credited to Fritz Haber, a German scientist, who weaponized chemical gasses for Germany to use in World War I[42]. 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[43]. 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[44]. 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[45].

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

---

[42] "A Brief History of Chemical War." *Science History Institute*, May 11, 2015. https://www.sciencehistory.org/distillations/a-brief-history-of-chemical-war.
[43] Ibid.
[44] "Gas in The Great War." Accessed February 18, 2020. http://www.kumc.edu/wwi/medicine/gas-in-the-great-war.html.
[45] Ibid.

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[46]. 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[47]. After the War, the tensions of the Cold War spurred more research and development of chemical weapons. It was seen as a viable option given nuclear deterrence. Although chemical weapons acted as a deterrence, they continued to proliferate and did not receive due consideration again until 1966, mostly because of overwhelming concern about nuclear weapons. In the 1960s and 1970s, Vietnam and Yemen were suspected of using chemical weapons provided by the USSR[48]. During the Iran-Iraq War, Iraq used mustard gas against Iran's forces and Iraqi Kurds who were backed by the Iranians. The most infamous use of chemical weapons was the deployment of toxic herbicide Agent Orange by the US on Vietnam. Agent Orange was sprayed on the jungles of Vietnam in order to destroy the area where food was grown for the Guerrillas. The forest was effectively rendered useless for food production, which consequently triggered a famine for local civilian populations[49]. The UK also used toxic herbicides against Malaysia around this time[50].

International opinion against chemical weapons spurred negotiations that culminated in The Convention on the Prohibition of the Development, Production,

---

[46] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))
[47] Ibid.
[48] Ibid.
[49] "Agent Orange | Definition, Effects, & Victims | Britannica." Accessed April 4, 2020. https://www.britannica.com/science/Agent-Orange.
[50] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))

Stockpiling and Use of Chemical Weapons and on their Destruction, known as the Chemical Weapons Convention (CWC). It opened for signature in 1993 and entered into force in 1997: seventy-two years after the Original Geneva Protocol. Given the high level of public outrage against chemical weapons that started in the late 1800s, it is surprising that reaching an agreement took so long. To better understand this, it is important to look at the timeline of negotiations[51,52]:

-5 December 1966: The General Assembly passes Resolution 2162 B, which calls for adherence to the 1925 Geneva Protocol. The Assembly delegates the task of constructing an agreement on chemical weapon disarmament to the Eighteen-Nation Committee on Disarmament (ENDC). At this time, chemical and biological weapons were considered under the same topic.

-26 August 1969: The Conference of the Committee on Disarmament (CCD), formerly the ENDC, was expanded to 26 countries. The CCD reiterates the need for urgent consideration on the topic.

-16 December 1971: With the creation of the Biological Weapons Convention, the General Assembly Urged the CCD to treat chemical weapons as a separate topic and to continue working towards an agreement.

-1972-1978: Chemical weapons were on the General Assembly's agenda every year, continuously reiterating the importance of a disarmament agreement, but not making substantial progress on an agreement.

-1978: The General Assembly establishes a Disarmament Commission, a subsidiary organ of the Assembly, that reports to a new Committee on Disarmament. The

[51] The entirety of the following timeline comes from the United Nations Audiovisual Library of International Law's CWC Procedural History page (citation in footnote 51)
[52] "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction - Main Page." Accessed April 4, 2020. https://legal.un.org/avl/ha/cpdpsucw/cpdpsucw.html.

commission is tasked with creating a comprehensive programme for chemical weapon disarmament.

-17 March 1980: The Committee on Disarmament creates an Ad-Hoc Working Group for the duration of the 1980 session to examine and define the issues to be dealt with in negotiations. The Working group is revived every successive session until 1992.

-8 July 1980: The US and the USSR introduce a joint progress report on their bilateral negotiations on chemical weapons disarmament.

-1985: The US and the USSR resume their bilateral negotiations after a five-year hiatus.

-15 December 1989: The Final Declaration of the Conference of States Parties to the 1925 Geneva Protocol (Paris Conference) reaffirms the authority of the Protocol and calls on the Conference of Disarmament (renaming of the Committee on Disarmament) to achieve the conclusion of an agreement as soon as possible.

-18-22 September 1989: At the Government-Industry Conference against Chemical Weapons, government and chemical industry representatives declares their commitment to cooperate together to support a disarmament agreement.

-1 June 1990: The US and the USSR sign a bilateral agreement and commit to cooperate on creating technology to destroy chemical weapons safely, abstaining from producing chemical weapons, and reducing existing stockpiles.

-20 June 1990: The Ad-Hoc Committee on Chemical Weapons expands its mandate to include the "use of chemical weapons" in the scope of prohibition. Under the new mandate, the intensity of negotiations increases.

-3 September 1992: The Conference on Disarmament adopts The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons

and on Their Destruction (CWC) as well as the commission for the Organisation for the Prohibition of Chemical Weapons (OPCW).

-13 January 1993: The Secretary General, the depository for the agreement, opens the CWC for signature in Paris, France.

-29 April 1997: The Chemical Weapons Convention enters into force after Hungary, the 65th county to ratify, submitted its ratification notice.

The CWC was groundbreaking in that it was the first treaty to completely ban the development, stockpiling, and use of a weapon. This posed a major problem for states: 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 parties to the CWC wanted to make sure these two problems were solved through the institutional design of the agreement. In order to do so, a verification mechanism had to be created that was extremely thorough so to ensure total compliance, but not too intrusive. The majority of the negotiation period for the CWC was spent figuring out how to overcome issues that this presented. Here are three main problems that plagued the CWC negotiations:

<u>The Dual Nature of Chemicals</u>[53]

There were concerns that the chemical industry would divert the purpose of chemicals from peaceful to military. This proposed a challenge, since the private sector could not be a party to the treaty. Therefore, success of the treaty relied on cooperation between governments and the chemical industry. The chemical industry pushed back at

[53] Thakur, Ramesh and Chandan, Tejal (2006). *The Chemical Weapons Convention: Implementation, Challenges and Opportunities*. United Nations University Press.

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. These concerns were addressed at the 1989 Government - Industry conference.

Assurance of a Global Ban on Chemical Weapons[54]

Many feared that the CWC would not be comprehensive enough to facilitate total world disarmament. Many states were hesitant to disarm, in the event that other states would continue their chemical weapon programs in secret. Many of these states wanted to retain the use of chemical weapons for retaliation purpose. There was also concern about chemical weapons proliferating outside of the East-West bloc, where they were mainly stockpiled. This fear was precipitated by reports of chemical weapon use in Asia and Africa. These states had an incentive to acquire chemical weapons to close the power gap with nuclear weapon states.

The Political Landscape at the Time[55]

The attempts to codify a disarmament treaty overlapped with the Cold War. East-West tensions accelerated a chemical weapons arm race. Thus, encouraging the development and stockpiling of new, more dangerous chemical weapons. This political landscape was not conducive for a total disarmament treaty and stretched out the duration of negotiations.

To overcome these problems, states expanded the scope of what the CWC covers and included extremely thorough verification and compliance mechanism. 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. The

[54] Ibid.
[55] Ibid.

criteria for a chemical being classified as a weapon was changed from the degree of toxicity to its intended purpose. 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. Expanding the scope of what is considered a chemical weapon allows for easier facilitation of a total weapons ban[56].

The CWC created the OPCW, which is in charge of administering the verification and compliance mechanisms. The OPCW's two main principles are to conduct verification in the least intrusive manner possible, and to use advances in science and technology to increase the effectiveness of verification[57]. Overall, it is considered the fact-finding, consultation, and cooperation forum for states parties. 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[58]. The Executive Council consists of forty-one-member states who are elected every two years. The Council mainly oversees the Technical Secretariat and issues measures regarding non-compliance[59]. The Conference of the States Parties is the plenary organ of the OPCW and oversees implementation of the CWC[60].

The OPCW carries out the verification and compliance mechanism. Here are its main features:

Verification of Destruction[61]

Declarations on chemical weapon stockpiles, live and abandon production facilities, relevant chemical activities, national implementation strategies and related matters are

---

56 "Chemical Weapons Convention." *OPCW*. Accessed April 4, 2020. https://www.opcw.org/chemical-weapons-convention.
57 "History" *OPCW*. https://www.opcw.org/about-us/history.
58 "Technical Secretariat." *OPCW*. https://www.opcw.org/about-us/technical-secretariat.
59 "Executive Council." *OPCW*. https://www.opcw.org/about-us/executive-council.
60 "Conference of the States Parties" *OPCW*. https://www.opcw.org/about-us/history.
61 "History" *OPCW*. https://www.opcw.org/about-us/history.

required of states by the OPCW. The verification of destruction relies on verifying the correctness of these reports. Declared sites and facilities are subject to regular inspections by the Technical Secretariat.

Verification of Non-Diversion[62]

The OPCW has a record of chemicals that have the potential for diversion from peaceful to military uses. Governments must have knowledge of all sites where these chemicals are being handled, and report these declarations on a balance sheet. Verification of non-diversion relies on verifying the correctness of these records.

Challenge Inspections[63]

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 closes routine verification loopholes, which are limited to declared facilities.

Dispute Settlement[64]

If inspections reveal non-compliance, the Technical Secretariat brings the case before the Executive Council or the Council of the States Parties. The Council can decide to take enforcement measures, or bring the case before the UN Security Council to decide on punishment. There exists a traditional inter-state dispute settlement process.

According to Koremenos (2016), the existence of enforcement problems increases the incentive to defect[65]. In order to correct that problem, punishment provisions are incorporated into institutional design. The inclusion of punishment provisions decreases the payoff from defecting on an agreement by threatening severe sanctions on

---

[62] Ibid.
[63] Ibid.
[64] "History" *OPCW*. https://www.opcw.org/about-us/history.
[65] Koremenos, Barbara. *The Continent of International Law: Explaining Agreement Design*. Cambridge: Cambridge University Press, 2016. doi:10.1017/CBO9781316415832.

defectors. Punishment provisions are also incorporated into institutional design when there exists uncertainty about future behavior. With chemical weapons, states vocalized their desire to stockpile for retaliation purposes. Thus, there was uncertainty that states would not continue to develop chemical weapons in secret. This uncertainty also necessitated the addition of a monitoring provision in the CWC. The CWC delegates monitoring to the OPWC because there are large incentives to defect and cheat on self-reports, the alternative form to third-party monitoring. The existence of formal punishment provisions in the CWC, in conjunction with rigorous monitoring methods, deters defection and incentivizes long and robust cooperation.

The institutional design of the CWC allowed it to be successful. The system of declarations and verifications has proven effective. The one place where the CWC has not performed as intended is the timeline for destruction of chemical weapon stockpiles. Destruction is difficult, and technology has not been developed to implement safe and effective chemical weapon destruction on a large scale. Destruction of stockpiles is still ongoing, but is behind schedule in many parts of the world. Despite the existence of the CWC, chemical weapons are still a threat, albeit a different permutation. Chemical terrorism has become a worry, especially after the UN attributed chemical weapons use to ISIS in Syria[66]. Non-state actors are unable to be parties to the Convention, which means there will always be a chance that chemical weapon use will go unregulated. The CWC was written in a way that makes it flexible to the changing times, and states parties have been working to do such at each of the review conferences.

[66] "Both ISIL and Syrian Government Responsible for Use of Chemical Weapons, UN Security Council Told | UN News." Accessed March 24, 2020. https://news.un.org/en/story/2017/11/570192-both-isil-and-syrian-government-responsible-use-chemical-weapons-un-security.

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[67]. 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. The modern-day use of biological weapons started after the foundation of microbiology[68]. The knowledge gained through the study of microorganisms helped form modern medicine, but it also laid out the roadmaps to weaponize organisms. Once this byproduct of scientific discovery was realized, the 1874 Brussels Declaration and the 1899 Hague Declaration prohibited the use of poisonous weapons. Additionally, the Geneva Protocol of 1925 outlawed the development, stockpiling, and use of Biological weapons and toxins. However, these did nothing to deter the development and use of biological weapons. 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[69,70].

These attacks were not successful, but it signaled both the strategic value of such weapon, and its potential consequences to other countries. Many of the world powers began to invest in biological weapons to give them an edge in light of the post-war

---

[67] "What Are Biological and Toxin Weapons?" Accessed April 4, 2020. https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument.
[68] 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.
[69] "Biological Weapons WW1." Accessed February 18, 2020. https://www.arcgis.com/apps/Cascade/index.html?appid=90a21c86f91c484bb3ba8dc64d4ce758.
[70] Jeffrey R. Ryan, *Biosecurity and Bioterrorism: Containing and Preventing Biological Threats*(Amsterdam: Elsevier/BH, Butterworth-Heinemann is an imprint of Elsevier, 2016))

tensions. No biological weapons were used again until World War II, but were developed and advanced in secret[71]. Japan had the largest biological weapons program post first world war. Shiro Ishii, considered the father of biological weapons, created Japan's extensive program. Japan developed bio-weapons to aid their imperialistic goals. The program developed and stockpiled tens of thousands of bio-weapons, and killed thousands of humans in human trials. Most of these victims were Chinese, the main recipient of Japans' bio-weapon attacks during World War II. 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[72]. Tens of thousands of Chinese were killed by Japanese bio-weapons during the war, and more died after. In 1947, two years after Japan surrendered, 30,000 people died due to complications from biological toxin exposure[73]. Biological weapons mimic diseases which have long-term health implications, and also destroy societal infrastructure.

Japan was the only country to use biological weapons during the second world war. There was fear that Germany would use biological weapons. Their attempted use of anthrax during World War I and their continued development and stockpiling of bio-weapons was well known by Allied forces. This fear sparked investment in bio-weapons programs in France, the UK, and the US[74]. 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. After World War II, countries continued their bio-weapons programs. The US, USSR, Japan, Germany, UK, and France all

---

[71] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))
[72] Ibid.
[73] Ibid.
[74] Ibid.

continued their biological weapons programs. During this time, advancements in bioweapons 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[75].

Biological weapons have been the ire of public opinion since the late 1800s. However, a disarmament treaty was not considered until the late 1960s. The negotiations on the Biological Weapons Convention only lasted less than three years. At the time of negotiation, biological and chemical weapons were debated as one topic. However, the UK's draft convention proposed that the topics should be thought of as separate. Biologicals weapons were not used in conventional warfare as frequently as chemical weapons. Chemical weapons posed a larger problem due to their frequent use in World War I, and their use as deterrence. The UK, backed by the US, argued that an agreement on biological weapons should not be delayed just because an agreement on chemical weapons could not be reached[76]. On 25 November 1969, US president Richard Nixon halted America's bioweapons program. This set an international precedence, and countries such as Canada, the UK, and Sweden followed suit. In 1971, the USSR and its allies came around to the view that biological weapons could be dealt with separately. The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Biological

[75] 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.
[76] "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.

Weapons Convention, BWC) was opened for signature in 1972 and entered into force in 1975. Here is a timeline on the cooperation behind the BWC[77,78]:

-1966: Hungary submits a draft resolution in the First Committee that seeks to demand strict and absolute compliance by all states with the principles and norms established by the Geneva Protocol.

-5 December 1966: The General Assembly adopts resolution 2162 B (XXI) that tasks the Conference of the Eighteen-Nation Committee on Disarmament (ENDC) to seek an agreement on the cessation of the development and production of chemical and biological weapons.

-1 July 1969: A report from the Secretary-General, prepared by experts in the field, concludes that the prospects for complete disarmament would brighten if the development, production, and stockpiling of chemical and biological weapons would end and they would be eliminated from all military arsenals.

-10 July 1969: The UK submits a draft convention for the prohibition of biological warfare to the CCD (Conference of the Committee on Disarmament).

-9 September 1969: Bulgaria, the Byelorussian Soviet Socialist Republic, Czechoslovakia, Hungary, Mongolia, Poland, Romania, and the USSR submit a draft convention for the prohibition of biological warfare to the General Assembly.

-1971: The CCD decides that agreements on biological weapons and chemical weapons will be decided as two different topics due to the fact that there were already

[77] 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)
[78] "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.

two draft conventions submitted on biological weapons alone, and that chemical weapons would need more time to discuss.

-16 December 1971: The General Assembly adopts resolution 2826 (XXVI) that accepts the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Biological Weapons Convention, BWC).

-10 April 1972: The BWC opened for signature by the USSR, the UK, and the US, the depository governments.

-26 March 1975: The BWC enters into force after ratification from 22 states including the three depository governments.

The scope of the BWC's prohibitions are very limited. Nowhere in the text does it explicitly ban the use of biological weapons. Article I 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"[79]. 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

[79] "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

conference every five years and Article XIII gives the convention an unlimited duration[80].

The BWC is extensively criticized for its lack of a verification system. The convention outlines no formal way to ensure that states are not cheating on the agreement. This is a problem, especially because it is easy to proliferate these weapons in secret. There is no monitoring provision to make sure that peaceful research using biological agents is not being diverted. The only verification methods are in Article V. The only form of accountability is the ability to file a complaint with the Security Council, which has never been invoked, although accusations against countries for suspected bioweapons programs have been publicly levied. A problem with this type of monitoring system is that the US, China, France, the UK, and Russia all have veto power on the Security Council, which applies to any BWC investigations. There have been flagrant violations of the BWC, proven by the existence of the USSR and Iraq's admitted bio-weapons programs after the BWC's ratification. Syria, Iran, North Korea, and Libya have all been accused of violation BWC obligations, but those claims have not been substantiated[81].

Another fallacy of the BWC is that it cannot regulate the use of bio-weapons by non-state actors, since these actors cannot be parties to the convention. Biological weapons have been hailed the "poor man's atomic bomb" because they are easy and cheap to make. Any extremist or terrorist group can easily access bio-agents or toxins for weaponization if they have enough determination[82]. This fallacy has posed problems for the complete disarmament of biological weapons on several occasions. In 1984, the

---

[80] Ibid.
[81] "BIOLOGICAL WEAPONS CONVENTION." Accessed March 28, 2020. https://fas.org/nuke/control/bwc/news/bwc1.htm.
[82] "Biological Warfare: An Emerging Threat in the 21st Century: 1/01." Accessed March 28, 2020. https://news.stanford.edu/pr/01/bioterror117.html.

Rajneesh religious group weaponized salmonella and poisoned 751 people in order to influence a local election in Oregon. In 1995, the Aum Shinrikyo cult used Sarin gas to kill twelve train passengers and injure more than 5,000 in Japan's subway system. In 2001, an unidentified assailant killed five people by sending letters contaminated with anthrax spores to prominent American political and media figures[83]. At every review conference of the BWC, states parties work to address these shortcomings. Currently, the states parties to the BWC are pushing for a more stringent verification system. However, there have not been substantial confidence building measures that adequately address these shortcomings of the BWC.

Section VI – Hypothesis Testing

In this section, I use process tracing to test hypotheses 1,2, and 4. For these hypotheses, I evaluate the existence of evidence to support clues. I then assess the degree of reasonability that we can believe these hypotheses hold true based on the existence of these clues. For Hypothesis 4, see Appendix 1 for an extended look at my methodology. For hypotheses 3, I provide justifications for why this hypothesis should be tested in the future, when there is more information available.

Hypothesis 1: As consequences become more understood and made tangible, cooperation becomes more likely

I hypothesize that as the consequences of a weapon become more understood and made tangible, cooperation becomes more likely. The main distinction between

[83] 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.

traditional weapons of mass destruction and cyberweapons is that the former is tangible, while the latter operates in an intangible, abstract dimension. This hypothesis attempts to connect the tangibility of a weapon's consequences with cooperation. A less tangible consequence is one that actors have yet to understand to its full extent and also cannot be easily observed or defined. Consequences often drive cooperation - states agree to disarm to avoid consequences of a particular event. This relationship between understanding consequences and cooperation is evident in the realm of infectious diseases and climate change. I look at these two case studies to better understand this causal mechanism.

Infectious Diseases

Infectious diseases were one of the first issues that nations realized could not be solved without international cooperation[84]. Due to globalization, infections have the ability to threaten populations across the world. Beyond the effect on human health, they can dismantle the ties that connect our world such as global economies. Cholera, plague, and yellow fever were three global pandemics in the 19th century that affected multiple continents. Cholera, specifically was the most dangerous: it is estimated that hundreds of thousands of people died across the globe during the Cholera outbreaks of the mid 19th century[85].

At the time, individual countries were dealing with the Cholera outbreak on their own by quarantining infected people within the country. However, as globalization took off, the disease crossed borders and destabilized economies that were

[84] "No Nation Can Fight Coronavirus on Its Own - Lawfare." Accessed February 16, 2020. https://www.lawfareblog.com/no-nation-can-fight-coronavirus-its-own.
[85] "Cholera's Seven Pandemics." Accessed February 16, 2020. https://web.archive.org/web/20081216071746/http://www.cbc.ca/health/story/2008/05/09/f-cholera-outbreaks.html.

now interconnected through global trade and finance. As a response, nations came together for the International Sanitary Conference in 1851. This started a series of 14 conferences that addressed international cooperation on the containment of infectious diseases. The Conferences were integral in the eventual formation of the World Health Organization in 1948, the world's primary international organization for fighting global health issues[86].

If my hypothesis holds true, then we would more cooperation when consequences are understood. This phenomenon occurred in infectious diseases. There was a time when there was no cooperation, and the consequences of infectious diseases were not well understood. Nations believed they could solve the issue through quarantine alone. Then, when the breadth of the consequences was better understood, cooperation became more urgent. In this case, the consequences were the observable deaths and the effect on global economies by Cholera.

Climate Change

Climate change is another analogous area where we see support for the existence of a casual mechanism between understanding consequences and cooperation. There is a lack of consensus regarding climate change - no one really knows what is going to happen. For a lot of people, the effects of climate change do not matter because they assume it will not happen to them. They have yet to fully understand the consequences and its severity. This is the intergenerational problem; the people who will be most affected cannot participate in the decision-making process because they are not born

[86] "The Globalization of Public Health : The First 100 Years of International Health Diplomacy / David P. Fidler." Accessed March 20, 2020. https://apps.who.int/iris/handle/10665/74977.

yet. People today cannot understand and believe the consequences, so they are less inclined to do something about it. This also resembles uncertainty paralysis: non-action or the stoppage of a certain discussion because of uncertainty on an issue.

The biggest clue that understanding consequences leads to more cooperation exists as a result of the 2019-2020 Australia brushfires. The fires have destroyed more than 18 million hectares of land, and killed an estimate of a billion animals and over 34 people[87,88]. These consequences are real, tangible, observable and understood by the people living through them in Australia. The result was an immediate call to action on climate change. Nation-wide rallies with attendance in the tens of thousands calling for immediate action on climate change started to happen after governmental inaction on the issue[89]. Protestors and scholars alike were explicit in their observed connection between climate change and the fires. A professor of climate science at the University of Sydney studying the brushfires said "We're probably looking at what climate change may look like for other parts of the world in the first stages in Australia at the moment"[90]. With regards to climate change, we have observed shifts in perception for the need to cooperate when the consequences become more quantifiable.

In a world where this hypothesis were to be the case, then we would see a higher degree of tangibility and understanding correlate to a higher level of cooperation. Thus, we would see this clue:

---

[87] "More than One Billion Animals Impacted in Australian Bushfires - The University of Sydney." Accessed February 16, 2020. https://sydney.edu.au/news-opinion/news/2020/01/08/australian-bushfires-more-than-one-billion-animals-impacted.html.
[88] "Australia Fires: Storms Wreak Damage but Bushfires 'far from over' - BBC News." Accessed February 16, 2020. https://www.bbc.com/news/world-australia-51170994.
[89] Shuttleworth, Kate. "Australia Fire Crisis Fuels Protests Calling for Bolder Action on Climate Change." *Washington Post*. Accessed February 16, 2020. https://www.washingtonpost.com/world/asia_pacific/australia-fire-crisis-fuels-groundswell-of-support-for-bolder-action-on-climate-change/2020/01/10/cc1fea3c-32a6-11ea-971b-43bec3ff9860_story.html.
[90] "More than One Billion Animals Impacted in Australian Bushfires - The University of Sydney." Accessed February 16, 2020. https://sydney.edu.au/news-opinion/news/2020/01/08/australian-bushfires-more-than-one-billion-animals-impacted.html.

Clue 1: An understanding of consequences promotes cooperation, and this is on people's minds at the time[91].

This clue holds strong probative value. If there is evidence that this clue exists, then there is strong reason to believe that this hypothesis holds true.[92]

Nuclear Weapons

C1. NW. E1. – The consequences of nuclear weapons became universally understood after World War II.

The issue of nuclear weapons proliferation was not discussed internationally until after the US dropped two atomic bombs on Japan at the end of World War II. This event was the first time that the devastating effects of nuclear weapons was observable and made known to the entire world. As soon as they happened, news sources brought word of the bombings and destruction to all corners of the world. The total death toll is not actually known, but it is estimated that between 60,000 and 80,000 people died instantly in Hiroshima, with a total of 135,000 dying after from injuries and long-term effects of radiation[93]. Around 40,000 people reportedly died instantly in Nagasaki, and 50,000 total people were estimated to have died from injuries and long-term effects of radiation[94]. The high volume of deaths as a result of the nuclear weapons was an observable consequence. The world observed these deaths and understood how nuclear

[91] The understanding of consequences as they relate to cooperation is acknowledged if it is on people's minds, or, if it is something they are thinking about.
[92] I will use the same set of clues to analyze both chemical and biological weapons. They appeared on the war scene in tandem, and the first declarations against their use did not separate them as two separate issues. They remained a merged topic until the late 1960s. An increased perceived need for cooperation on these issues came after their use in World War I. The clues I will find to link the existence of tangible consequences to cooperation is the observable use and aftermath of these weapons during World War I and World War II.
[93] "BBC - WW2 People's War - Timeline." Accessed February 17, 2020. https://www.bbc.co.uk/history/ww2peopleswar/timeline/factfiles/nonflash/a6652262.shtml.
[94] Ibid.

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[95]. In Nagasaki, a third of the city was destroyed[96].

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. The study found that humans were ingesting cancer-causing radioactive isotopes as a result of fallout from nuclear testing[97]. 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. This danger spurred the US the UK, and the USSR to sign the Partial Nuclear Test Ban Treaty that banned above ground nuclear testing[98].

C1. NW. E2. – An understanding of nuclear weapon's consequences spurred protest movements with average citizens that called for cooperation.

Hiroshima and Nagasaki marked the beginning of an anti-nuclear movement that was carried out by ordinary citizens around the world. The observed consequences of nuclear weapons spurred an activist movement that called for the abolition of nuclear weapons in order to protect the peace and safety of the world. The first example is the Women Strike for Peace group - a women led group of protests that led marches in 60

[95] 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.
[96] Ibid.
[97] Reiss, Louise Zibold. "Strontium-90 Absorption by Deciduous Teeth." *Science* 134, no. 3491 (November 24, 1961): 1669. doi:10.1126/science.134.3491.1669.
[98] This treaty was signed, but never ratified. Signing can be seen as a commitment to upholding the international norm.

US cities in 1961[99]. The second example is the Aldermaston Marches in the United Kingdom. These started in 1958, and drew tens of thousands of people to march against nuclear weapons[100]. Both protest groups called for states to cooperate to abolish the weaponization of nuclear energy.

C1. NW. E3. – An understanding of nuclear weapon's consequences spurred calls to cooperate from influential academic figures.

On a scholarly level, many important political and academic figures called for disarmament of nuclear weapons after observing the horrific effects of the bomb. Nobel Laureate Bertrand Russel, who was a hallmark of British politics and academia in the mid 20th century put out a large amount of literature calling on world governments to save the world from the effects of nuclear weapons.

From The Bomb and Civilization (1945):

"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. A great deal of new political thinking will be necessary if utter disaster is to be averted"[101]

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

"All, equally, are in peril, and, if the peril is understood, there is hope that they may collectively avert it."

---

[99] "Women Strike for Peace | American Organization | Britannica." Accessed March 20, 2020. https://www.britannica.com/topic/Women-Strike-for-Peace.

[100] "People's History of CND - Easter Marches to Aldermaston 1958-60 -." Accessed March 20, 2020. https://cnduk.org/peoples-history-of-cnd-easter-marches-to-aldermaston-1958-60/.

[101] "The Bomb and Civilization." Accessed February 17, 2020. http://www.personal.kent.edu/~rmuhamma/Philosophy/RBwritings/bombCivilization.htm.

"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."[102]

C1. NW. E4. – An understanding of nuclear weapon's consequences motivated world leaders to call for cooperation.

As the consequences of nuclear weapons became better understood, world government leaders turned to cooperation on disarmament as the only reasonable way to avert this peril. This can be shown by a slew of resolutions and draft resolutions proposed at the United Nations General Assembly sessions. Starting in 1958, States' UN representatives starting consistently calling for an international treaty or institution to solve the problem of nuclear weapons proliferation. By reading the resolutions, it is observable that the need for cooperation stemmed from the knowledge of the consequences of nuclear weapons.

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"[103]

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,"

"Bearing in mind the profound concern evinced by the peoples of all countries regarding the testing of nuclear and thermo-nuclear weapons,"[104]

---

[102] "Russell-Einstein Manifesto." *Atomic Heritage Foundation.* Accessed February 17, 2020. https://www.atomicheritage.org/key-documents/russell-einstein-manifesto.

[103] General Assembly draft resolution A/C.1/L.206 (17 October 1958), available from undocs.org/A/C.1/L.206

[104] General Assembly resolution 14/1402, Suspension of Nuclear and Thermo-nuclear Tests

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"

"Believing in the necessity of an international agreement"

"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"[105]

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"[106]

The language of these texts shows us that there is a clear peril that needs to be solved. The usage of words such as "profound concern" and "dangers" signify that the concern was understood. The call for international agreements in Resolutions 1576 and 1578 show that these concerns heightened the perceived need for cooperation.

Biological and Chemical Weapons

C1. BW. E5. – The founding of microbiology alerted people of the potential consequences of biological weapons. International cooperation is the direct response to this understanding.

A/RES/14/1402 (21 November 1959), available from undocs.org/A/14/1402

[105] 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

[106] 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

World War I was the first time that biological and chemical weapons were used in warfare. Before then, there was limited information on their destructive capabilities. After the founding of microbiology as a science, people started to become more aware of the dangers that biological agents pose to society. The threat that this new information carried was the direct push for diplomats to cooperate. The result was two declarations that forbid the use of poison and poisoned weapons: The 1874 Brussels Declaration and the 1899 Hague Declaration[107].

C1. BW/CW. E6. – The consequences of biological and chemical weapons became universally understood after World War I given first-hand accounts and reports of causalities.

In World War I, European countries on both sides of the war used various biological and chemical weapons as a means of maiming and killing their enemies. The following information on causalities, injuries, and damage from these weapons was made available and received by the public.

Chemical weapons

Chemical weapons caused 1.3 million casualties. Out of those casualties, 100,000-260,000 were civilians and around 200,000 were deaths[108]. Even after the war ended, people were still feeling their consequences. In 1920 alone, 40,000 civilians and 20,000 military personnel died from lasting injuries as a result of exposure to chemical

[107] 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.
[108] "A Brief History of Chemical War." *Science History Institute*, May 11, 2015. https://www.sciencehistory.org/distillations/a-brief-history-of-chemical-war.

weapons[109]. Here are the types of chemical weapons that were used and their known effects:

Tear Gas[110]

Tear gas causes tearing in the eyes and trouble breathing. It was used as a weapon but since the symptoms resolved themselves quickly, it was abandoned in favor of other deadly chemical weapons.

Chlorine[111]

Chlorine reacts with water in the lungs to form Hydrochloric acid. This acid causes coughing, vomiting, and eye irritation. At a more concentrated dose, it causes a quick death.

Phosgene and Diphosgene[112]

Phosgene and Diphosgene are liquids that cause suffocation. They are colorless, so soldiers did not know they had ingested the poison. The liquid slowly filled their lungs and they died a slow painful death over the course of 48 hours.

Mustard Gas[113]

Mustard Gas is a liquid that irritates the eyes, skin, and respiratory tract acting as a blistering agent. It also reacts with DNA to cause cell death.

It is also important to understand the first-hand accounts of these weapons:

---

[109] 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.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.

"You could see where men had clawed at their faces, and throats, trying to get breath. Some had shot themselves. The horses, still in the stables, cows, chickens, everything, all were dead. Everything, even the insects were dead."[114]

"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"[115]

Beyond physical effects, chemical weapons left psychological scars:

"For miles around, scared soldiers woke up in the midst of frightful pandemonium and put on their masks, only to hear a few minutes later the cry of "All safe." . . . Two or three alarms a night were common. Gas shock was as frequent as shellshock"[116]

Biological Weapons

Once these chemical weapons were used, their consequences became more tangible and better understood to the world. The same happened with biological weapons, on a smaller scale. There were two main biological weapons used during World War I: anthrax and glanders. Anthrax is a deadly biological agent that primarily infects animals. Humans become infected with anthrax when they come into contact with infected animals. The Germans weaponized anthrax and used it to infect livestock that was being shipped to the British[117]. Anthrax is extremely dangerous, it has a 50% mortality rate. Glanders is an infection that was also weaponized in order to infect

---

[114] "Biological Weapons WW1." Accessed February 18, 2020. https://www.arcgis.com/apps/Cascade/index.html?appid=90a21c86f91c484bb3ba8dc64d4ce758.
[115] 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.
[116] Ibid.
[117] Edward M. Spiers, *A History of Chemical and Biological Weapons* (London: Reaktion, 2010))

humans through animals - namely horses. Glanders manifests as pulmonary or bloodstream infections in humans[118]. Biological weapons were not used as much as chemical weapons were, so their consequences did not induce immediate panic. However, microbial research on the effects of biological agents supplemented these observable consequences with scientific backing. This gave more reliability to the fact that biological agents were a concern.

C1. BW/CW. E7. – The understanding of consequences of biological and chemical weapons precipitated international cooperation.

Once the consequences of biological and chemical weapons were better understood, there was an increased perception of the need for cooperation. As a direct response, the Geneva Protocol of 1925 was signed. The preamble of the Protocol acknowledged the direct link between understanding consequences and a need for cooperation:

"Whereas the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices, has been justly condemned by the general opinion of the civilized world"[119]

This Protocol banned the use of chemical and biological weapons in war. The intent behind the protocol was to ban the use of these weapons in any future wars. The intent is justified by the need to avoid the understood humanitarian consequences of the two weapons.

---

[118] "A Brief History of Chemical War." *Science History Institute*, May 11, 2015. https://www.sciencehistory.org/distillations/a-brief-history-of-chemical-war.

[119] United Nations, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, 17 June 1925, available at: https://www.refworld.org/docid/4a54bc07d.html

Cyberweapons

I did not find evidence to support Clue 1 for cyberweapons. Rather, I found the opposite – a lack of understanding of consequences for cyberweapons and an acknowledgement that it creates an obstacle to cooperation. There have been many observed consequences of cyberattacks. These include, but are not limited to, denial of service (DoS), file damage, physical damage, ransomware, and data theft. Although cyberspace is lawless, the actions such as theft, extortion, and physical damage done in cyberspace are comparable to real life crimes. Cyberweapons also impose incredible economic externalities on victims. Most of the costs come from cleaning up from an attack and building prevention capabilities for the future[120]. The lack of understanding about cyberweapon threats comes from the inability to predict what the future effects are. Technology turns over so quickly due to constant innovation. With every new day, the world is constantly pushing the frontier of technological innovation. Due to the uncertainty about tomorrow's cyberspace capabilities, we cannot have complete information regarding the consequences of cyberweapons. There may be effects that we do not know about because they have not been developed yet. Therefore, the breadth of consequences is less quantifiable. Given the wide range of cyberweapons, there is also uncertainty about the effect that will manifest through a cyberattack. The consequences are only felt after the fact, and even then, they are often not realized.

In 2010, the virus Stuxnet destabilized Iran's nuclear program by shutting down machines that were used to enrich Uranium. The virus, believed to have been developed by the US in conjunction with Israel, hacked into the mainframe of Iran's nuclear program. It then took over control of around 1,000 centrifuges that were

---

[120] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014))

enriching uranium, and made their motors tear the machines apart from the inside out[121]. This was the first time that the world was really made aware of the capability of cyberweapons to infiltrate physical infrastructure. This ability signaled some more concrete consequences of cyberweapons to the world. While Stuxnet allowed the world to be more aware of the consequences of cyberweapons, it also taught us that we only know a fraction of its capabilities. The lack of understanding of threats even after examples come to light have been expressed by many countries and international institutions.

Here are some quotes to show that this problem is on people's minds:

"There is much uncharted territory in the world of cyber-policy, law and doctrine. We can't tell what has and what hasn't happened"[122] - Keith Alexander, the former head of the U.S. Cyber Command

"With the constant advancements in current technologies comes a new wave of security challenges"[123]- TrendLabs 2015 Report Published by the International Telecommunications Union

"Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. [We] must therefore keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime"[124] - Interpol

---

[121] 60 Minutes: Stuxnet (Columbia Broadcasting System, 2012), https://search.alexanderstreet.com/view/work/bibliographic_entity|video_work|2856063)

[122] 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.

[123] "A Rising Tide: New Hacks Threaten Public Technologies," n.d., 46.

[124] "Cybercrime." Accessed February 27, 2020. https://www.interpol.int/en/Crimes/Cybercrime.

"The expanding use of ICTs [Information and Communication Technology] in critical infrastructures and industrial control systems creates new possibilities for disruption"[125] - Group of Governmental Experts (GGE) 2015

These public statements by entities well-versed on the issue are evidence that we currently do not have full understanding of the consequences of cyberweapons. With a lack of understanding comes the inability to make them tangible. How can we make consequences tangible if we do not know what they are yet? This sentiment is reflected in the steps that the international community is taking to mitigate the issue. Due to the iterative nature of this problem, the international community cannot successfully cooperate on the issue without having an understanding on what they are cooperating on. This is the focus of current international happenings. In the GGE and the OEWG's mandates, General Assembly Resolution A/RES/73/27, the GGE "Decides… to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security"[126]. The GGE's current agenda includes informal intersessional consultative meetings with diplomats and experts in the field to better understand future threats of cyberweapons.

Of the 16 countries that submitted preliminary working papers to the OEWG, 10 dedicated sections to outlining the need and proposed directions for better understanding existing and potential threats with a purpose of furthering cooperative efforts[127]. The International Committee of the Red Cross on International Humanitarian

---

[125] General Assembly resolution 70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
A/RES/70/174 (22 July 2015), available from undocs.org/A/70/174

[126] 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

[127] "Open-Ended Working Group – UNODA." Accessed April 5, 2020. https://www.un.org/disarmament/open-ended-working-group/.

Law and Cyber Operations during Armed Conflicts submitted a position paper urging the OEWG and GGE to work towards a better understanding of the human cost of cyberweapons. The Global Commission on the Stability of Cyberspace also submitted a position paper calling for a better understanding of cyberspace norms in order to be better prepared for emerging threats[128]. The word choice of "potential" threats in all of these documents, as a distinction from existing, inherently implies the existence of an unknown group of consequences. The urging to get closer to a consensus further implies that there are threats that are not fully realized.

Using Mill's method of difference, I propose that the lack of evidence, and the observation of the opposite result in the cyberweapon case study lends support for the belief that Hypothesis 1 holds true.

Given the existence of evidence **C1. NW. E1, C1. NW. E2, C1. NW. E3, C1. NW. E4, C1. BW. E5, C1. BW/CW. E6, and C1. BW/CW. E7**, we have reason to believe that Clue 1 exists in our world. Thus, we have strong reason to believe that Hypothesis 1 holds true.

Hypothesis 2: As the attribution of violation becomes harder, cooperation becomes less likely

I hypothesize that as the attribution of violation becomes harder, cooperation becomes less likely. Attribution refers to the ability to formally identify the user of a weapon. An attribution problem, as I call it in the rest of this section, is when attribution of a perpetrator is sufficiently difficult that it could realistically not happen. This

[128] Ibid.

attribution mostly occurs after the use of the weapon. But, I use the word violation to mean either the development, stockpiling, or use of the weapon. Attributing the use of an illegal weapon to a perpetrator often hinges on verification of treaty non-compliance. In the theoretical construct of the world where Hypothesis 2 would be the case, we would see this clue manifest:

Clue 1: there is acknowledgement of an attribution problem and that its effects pose problems for cooperation

The absence of an attribution problem alone does not give us reason to believe the hypothesis holds true. However, the existence of an attribution problem triggers a theoretical justification for how the mere existence of those clues strongly implies the existence of a cooperation problem. Thus, we can reason that the absence of an attribution problem does not trigger that specific cooperation problem. By levying large costs on defectors, punishment provisions lower the payoff for non-cooperation. However, the effectiveness of punishment provisions relies on the ability to identify a violator to punish. In areas where it is difficult to attribute a violator to punish, punishments are pointless. It becomes an ineffective way to raise the cooperation payoff above the non-cooperative payoff. Thus, an obstacle to cooperation still remains. The existence of obstacles to cooperation such as this lower the probability that cooperation will be achieved. Conversely, the lack of an attribution problem removes an obstacle to cooperation, which increases the probability that cooperation will be achieved.

The existence of evidence for both parts of Clue 1 plus the theoretical justification gives Clue 1 high probative value. The existence of Clue 1 gives us strong reason to believe the hypothesis holds in our world.

Nuclear Weapons

I did not find evidence of an attribution problem with nuclear weapons. I also did not find evidence that this attribution problem created an obstacle to cooperation. Before the NPT, the world had almost complete information on what states had nuclear weapons. Today, we continue to have that information, and we also have reliable information on what states have the capabilities to build nuclear weapons. Building a nuclear weapon is very costly, and many states do not have the money or infrastructure to support that endeavor. It also requires importing rare and expensive materials, the buying of which can be observed by other states. The existence of near complete information on what states are capable of producing and using nuclear weapons, and those that stockpile them, provide clues that the attribution is very easy. In a world where this hypothesis holds true, that means we would see more cooperation. This outcome is evident with the existence of the NPT.

Chemical Weapons

I did not find evidence of an attribution problem with chemical weapons. There is also no evidence that an attribution problem created cooperation obstacles during the negotiations of the CWC. Rather, during negotiations, states worked together to avoid the attribution problem that plagued the BWC. The attribution of chemical weapons hinges on the existence of ex-post evidence. The body of this evidence comes from fact finding missions and chemical forensics, which are both available and accessible mechanisms[129]. In response to alleged chemical weapon use in Syria, the UN launched an investigation using a balance of independent, impartial on-site fact-finding missions

[129] "Fact-Finding Mission." *OPCW*. Accessed March 24, 2020. https://www.opcw.org/fact-finding-mission.

and forensics. The fact-finding team used in depth microbial laboratory studies to analyze samples from autopsies of victims of the attacks[130]. The studies revealed that based on unique markets, the chemical gasses used in the attacks were very likely to have been made from the same precursor chemicals that came from declared Syrian stockpiles. Testimony from scientific exports supported these findings. The results were combined with witness statements, on-site investigations, and information collected from other states about Syria's chemical weapon program to make sure the report was credible and reliable[131,132]. The fact-finding mission used well established criminal investigation methods to attribute chemical weapon use. The evidence needed to build a sound case are relatively easy collect and widely available, thus increasing the chance that a fact-finding mission will successfully attribute an attack[133]. The type of information needed to complete contemporary fact-finding missions were available at least twenty-five years before the CWC went into effect. This proposition is supported by the fact that the IAEA was using the same methods for fact-finding twenty-five years before the NPT was opened for signature.

Biological Weapons

C1. BW. E1: Public acknowledgement of the attribution problem for biological weapons**.**

[130] Koblentz, Gregory D., and Jonathan B. Tucker. "Tracing an Attack: The Promise and Pitfalls of Microbial Forensics." *Survival* 52, no. 1 (March 2010): 159–86. doi:10.1080/00396331003612521.
[131] "Both ISIL and Syrian Government Responsible for Use of Chemical Weapons, UN Security Council Told | UN News." Accessed March 24, 2020. https://news.un.org/en/story/2017/11/570192-both-isil-and-syrian-government-responsible-use-chemical-weapons-un-security.
[132] "Collateral Damage? The Chemical Weapons Convention in the Wake of the Syrian Civil War | Arms Control Association." Accessed March 24, 2020. https://www.armscontrol.org/act/2018-04/features/collateral-damage-chemical-weapons-convention-wake-syrian-civil-war.

It is well acknowledged in academia that biological weapons are hard to detect because they are easily accessible and cheap to make. The ingredients of biological weapons are often naturally occurring, giving the weapon a plausible deniability characteristic. Bio-weapon attacks can easily be covered up as natural outbreaks. Ingredients for bio-weapons and the equipment needed to make them can also be easily sourced from hospitals or commercial medical supply companies[134]. The cost of doing this is far lower compared to other weapons that require specific infrastructure, expensive rare ingredients, high volumes of research, development, and testing[135]. The ease with which biological weapons can be produced do not bar many actors from having access to them.

C1.BW.E2: Acknowledgement that the lack of attribution ability causes an enforcement problem by government leaders and decision makers.

This attribution problem is also acknowledged by world leaders and decision makers. This problem was only recognized after the signing of the BWC. States quickly realized that further cooperation was needed create additional protocols in order to solve this problem. Thus, the BWC Review Conferences, and other relevant parties, since 1986 have been trying to codify more international law solving this issue. :

"Scientists must be able to determine, first, what was the source of the event that caused the disease; second, determine if the event was natural or deliberately caused; and third, be able to track down its origins. That is an extremely difficult set of tasks… Without good technology, we can't confirm what happened or even begin the process

[134] "Biological Warfare: An Emerging Threat in the 21st Century: 1/01." Accessed March 5, 2020. https://news.stanford.edu/pr/01/bioterror117.html.
[135] Charlet, Katherine, and Katherine Charlet. "The New Killer Pathogens: Countering the Coming Bioweapons Threat." *Carnegie Endowment for International Peace*. Accessed March 5, 2020. https://carnegieendowment.org/2018/04/17/new-killer-pathogens-countering-coming-bioweapons-threat-pub-76009.

of determining attribution"[136] – Paula A. DeSutter, US Assistant Secretary for Verification, Compliance and Implementation

Assistant Secretary DeSutter linked the attribution problem to the enforcement problem:

"If we can't determine who the guilty party is, there can be no consequence for the action, and there is nothing to deter more biological events from occurring. There is no deterrence value to the agreement… The formula is very simple. State Parties have a responsibility to live up to their obligations. If they do not, they deny the other parties the benefits of the agreement."[137]

The link between the attribution problem and an enforcement problem was on the agenda of the second Biological Weapons Convention Review Conference. One of the stated goals of the review conference was:

"Confirming the common interest in strengthening the authority and the effectiveness of the Convention, to promote confidence and co-operation among State Parties,"[138]

This common interest stemmed from the acknowledged attribution problem, which rendered the quasi-verification system in Article V ineffective. To fix this problem recommended measures to help solve the attribution problem:

"The conference, mindful of the provisions of Article V and Article X, and determined to strengthen the authority of the Convention and to enhance confidence in

---

[136] Department Of State. The Office of Electronic Information, Bureau of Public Affairs. "Attribution and Deterrence of Biological Weapon Use." Department Of State. The Office of Electronic Information, Bureau of Public Affairs., October 27, 2008. https://2001-2009.state.gov/t/vci/rls/rm/111767.htm.

[137] Ibid.

[138] "Report of the Committee of the Whole" Accessed March 15, 2020. https://www.unog.ch/bwcdocuments/1986-09-2RC/BWC_CONF.II_09.pdf.

the implementation of its provisions, agrees that the States Parties are to implement, on the basis on mutual co-operation, the following measures

Exchange of data, including name, location, scope and general description of activities, on research centers and laboratories that meet very high national or international safety standards established for handling, for permitted purposes, biological materials that pose a high individual and community risk or specialize in permitted biological activities directly related to the Convention.

Exchange of information on all outbreaks of infectious disease and similar occurrences caused by toxins that seem to deviate from the normal pattern as regards type, development, place, or time of occurrence. If possible, the information provided would include, as soon as it is available, data on the type of disease, approximate area affected, and number of cases.

Encouragement of publication of results of biological research directly related to the Convention, in scientific journals generally available to States Parties"[139]

Cyberweapons

C1. CY. E3: Public acknowledgement by government leaders and decision makers of the cybersecurity attribution problem.

Cyberweapons are deployed from behind a screen, remotely. A person can carry out an attack on an entity from the opposite side of the world, since cyberspace connects all technology on the planet. All that one needs to commit a cybercrime is access to technology, which makes the pool of potential attackers unfathomably large. This presents a large problem with attribution: there are so many potential perpetrators that

[139] Ibid.

it is very hard to identify just one. Technology has advanced in such a way that hackers can easily hide their identities and leave no 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[140]. 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[141]. The US's Federal Bureau of Investigations (FBI) relayed the difficulty of this problem, when trying to answer the question of who is behind cyber-attacks. They could be:

"computer geeks looking for bragging rights, to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal personal information and sell it on black markets, to spies and terrorists looking to rob our nation of vital information or launch cyber strikes"[142]

Stuxnet is a great example of the attribution problem. Stuxnet's code is heavily encrypted, so the exact perpetrators of the attack have not been identified. All that is known is that the worm came from a cyber espionage group called the Equation Group. The Equation Group has been able to author code that conceals their identities and location. The Kaspersky Lab, the multinational cybersecurity group that found Stuxnet and identified the Equation Group has not been able to attribute an allegiance between the Equation Group and a country[143]. There is intense speculation that Stuxnet was

---

[140] "To Identify a Hacker, Treat Them Like a Burglar | WIRED." Accessed April 5, 2020. https://www.wired.com/story/case-linkage-hacker-attribution-cybersecurity/.
[141] "Russian Hacker False Flags Work—Even After They're Exposed | WIRED." Accessed April 5, 2020. https://www.wired.com/story/russia-false-flag-hacks/.
[142] "Cyber Crime — FBI." Accessed April 5, 2020. https://www.fbi.gov/investigate/cyber.
[143] "Equation: The Death Star of Malware Galaxy | Securelist." Accessed April 5, 2020. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

designed in tandem between Israel and the US, however that has not been confirmed. The attack on Iran's nuclear program happened over ten years ago, and there is only speculation on the identity of the perpetrators.

This attribution problem was acknowledged by the GGE in their 2015 report:

"The malicious use of ICTs can be easily concealed and attribution to a specific perpetrator can be difficult, allowing for increasingly sophisticated exploits by actors who often operate with impunity"[144]

C1. CY. E4: Public acknowledgement by government leaders and decision makers that the cybersecurity attribution problem affects cooperation.

One of the main goals of the GGE's 2013 report is to establish the rules on responsible state behavior in cyberspace:

"Member States have repeatedly affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. Further progress in cooperation at the international level will require an array of actions to promote a peaceful, secure, open and cooperative ICT environment… These include common understandings on the application of relevant international law and derived norms, rules and principles of responsible behavior of States"[145]

"The potential for the development and the spread of sophisticated malicious tools and techniques, such as bot-nets, by States or non-State actors may further increase the

---

[144] General Assembly resolution 70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/RES/70/174 (22 July 2015), available from undocs.org/A/70/174

[145] 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

risk of mistaken attribution…The absence of common understandings on acceptable State behavior with regard to the use of ICTs increases the risk"[146]

The existing fear of mis-attribution is the core of the cyberweapon attribution problem. If there is no way to verify the perpetrator, then enforcing any type of punishment is incredibly difficult.

Using Mill's method of difference, I propose that the lack of evidence, and the observation of the opposite result in the nuclear weapons and chemical weapons case studies lend support for the belief that Hypothesis 2 holds true.

Given the existence of evidence **C1. BW. E1, C1. BW. E2, C1. CY. E3 and C1. CY. E4** we have strong reason to believe that Clue 1 exists in our world. Thus, we have strong reason to believe that Hypothesis 2 holds true.

Hypothesis 3: When the benefit of the status quo is large enough, cooperation becomes less likely

I hypothesize that when the benefits of the status quo are high enough, cooperation becomes less likely. To this paper, the status quo is a world without cooperation. If the payoff that an actor derives from non-cooperation, and therefore no deviation from the status quo, is higher than the payoff from deviating from the status quo, the actor will not cooperate. There are many factors that influence an actor's payoff list, one of the more influential ones being the domestic lobby. Lobbyist groups spend billions of dollars every year to push government policy in a certain direction. The government-lobby relationship is usually a mutually beneficial partnership where both sides receive net positive benefits from entering in the relationship. This quid pro quo is

[146] Ibid.

influential enough to sway the workings of governments across the world. This observation leads me to propose the question: if the benefit the government receives in the status quo from lobbying is high enough, would that affect a states' willingness to cooperate on an international level?

In a world with perfect information, we would be able to collect evidence that show that a specific degree of influence that an industry lobby has on the government correlates to a certain degree of cooperation. This intuition constitutes the "clues". In order to properly test this, there would need to be evidence for traditional weapons of mass destruction and cyberweapons. Presently, the type of lobbying we would need to see for cyber in order to make a connection between disarmament aims and lobbying does not exist publicly. The topic of international disarmament of cyberweapons has not been in the public eye for long enough to allow for this relationship to come to fruition. In the future, when the possibility that governments will have to give up their use of cyberweapons, and thus threatening the proliferation of this weapon in the private sector, we will be able to find enough clues to properly assess if this hypothesis holds true. In this section, I will lay the groundwork for this argument in hopes of generating a theory and creating stepping stones to test it in the future.

Disarmament treaties inherently constrain an actor's actions regarding the treaty subject. This is including, but not limited, weapon research and development, testing, and manufacturing. Now more than ever, governments are contracting those tasks out to private companies. Any state party to a treaty that contracts out defense work to private companies will pass on the treaty's constraints to those contractors. Here is a hypothetical example: imagine the US enters into an international treaty where it has to limit its stockpile of submarines that carry nuclear weapons. The corporation that produces missiles for US submarines, would have to limit or cease production of this

missile. The resulting reduction in revenue for the company is contrary to the firm's profit maximizing goals. Therefore, it would oppose the treaty as it is a roadblock too maximizing profit. A reasonable course of action would be for the corporation to lobby the Senate to not ratify this treaty. Alternatively, the corporation could lobby the government to give them lucrative contracts for other defense materials or weapons. If the corporation has a strong enough influence on the government, the singular corporation could affect how the US engages in foreign policy. The special relationship that the firm and the government had in the hypothetical, in addition to its consequences, is an example of the military industrial complex (MIC). The MIC is the phenomenon that I use to guide my argument for this hypothesis.

The Military Industrial Complex

The Military Industrial Complex (MIC) is a term first coined by Dwight D. Eisenhower in his 1961 farewell from office address. The complex describes a network of individuals and institutions that combine a profit motive with the planning and implementation of strategic policy[147]. The network includes the military, the executive and legislative branches of government, and defense-related industries. Although there is not one agreed upon definition of the phenomena, it is generally agreed that it encompasses the alliance between a county's military establishment and private companies in related fields. The MIC tracks the influence that each party has on the other. Eisenhower cautioned that certain industries would encourage military policy in a way that is not representative of public opinion. More recent scholars have echoed his sentiment: we have to be vigilant against the influence of a lobby that pushes for

[147] "Military-Industrial Complex | Definition, Elements, Influence, & Facts | Britannica." Accessed April 5, 2020. https://www.britannica.com/topic/military-industrial-complex.

government spending on military in the name of profit[148]. Corporations are profit-maximizing actors. Transitively, their motives are inherently concentrated in accumulating wealth and minimizing costs.

Eisenhower identified that the influence of the military industry complex in America is very strong. The MIC also holds up in other countries. I do a small case study of the MIC in two other parts of the world: Russia and China. Although this is a small sample size, these three countries are world leaders in international relations, specifically in disarmament. If the MIC holds up in these cases, it supports the reasonability of my hypothesis.

The American Military Industrial Complex

The military industrial complex in the US is most apparent in the act of government contracting. Over the past two decades, there has been an increase in American military action, spending, and government defense contracting. Most agencies of the US Government contract out the bulk of research, development, and production of war related items to private businesses. Businesses are awarded government contracts through a bidding process, where the contracts are awarded to the businesses that "bids" with the lowest cost estimate for the project[149].

From an economic perspective, the relationship between the government and industry makes sense. When an economy divides labor tasks and allows certain firms to specialize in production of a certain good, the economy is more efficient and can

[148] James Ledbetter, Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex (Icons of America) (Yale University Press, 2011))
[149] "How to Become a Federal Government Contractor | USAGov." Accessed January 26, 2020. https://www.usa.gov/become-government-contractor.

maximize production of goods while minimizing costs[150]. Government contracting fits this model. It is more efficient and cost effective to contract out certain jobs to companies that specialize in a service, so that government agencies can focus on their specialties. However, the practice of defense contracting has strayed from this model, which has prompted intense scrutiny of the industry and military relationship. Scholars have touted the idea that abuses of defense contracting is emblematic of unfair influence of industry on military policy. I will look at two aspects of this relationship in order to evaluate this claim. The first is by looking at defense contracting over the past two decades. I will then supplement this by looking at the effect of the industry lobby on.

Defense Contracting from 2000-Present

The Department of Defense does the most contracting out of all government agencies. The defense industry (which I will just call "the industry") has contributed a yearly average of 2.068% of the US's Gross Domestic Product (GDP) for all industries between FY (fiscal year) 2000 and FY2018. The yearly average output in nominal value over this period is 647.33 billion dollars[151]. The value of the defense industry to the government reaches far beyond dollar amounts. The products the industry produces, namely weapons, allows the US to assert itself to both allies and enemies as a world military power that is not to be messed with. This intangible value is the benefit that the government receives in entering into this relationship with the industry.

This intangible value added to the government increases during times of war. The prime example of this is defense spending post 9/11, and throughout the 2000s. With

[150] Smith, Adam, 1723-1790. The Wealth of Nations / Adam Smith ; Introduction by Robert Reich ; Edited, with Notes, Marginal Summary, and Enlarged Index by Edwin Cannan. New York :Modern Library, 2000.
[151] "Defense: Top Contributors to Federal Candidates, Parties, and Outside Groups | OpenSecrets." Accessed January 25, 2020. https://www.opensecrets.org/industries/contrib.php?ind=D&Bkdn=DemRep&cycle=2016.

the start of the war on terror, the US's journey to assert itself as a world leader in the fight against terrorism was concentrated in upping its military spending[152]. Between FY2001 and FY2003, U.S. defense nominal spending went from $432.9 billion to $553.3 billion. That $120.4 increase was double China's defense spending in one year. In 2003, China spent nominally $62.5 billion on defense, and they remained the second highest defense spender after the US. In 2008, at the height of US Involvement in the Middle East, defense spending reached its peak. The US spent over $700 billion on defense that year. That is four times the next highest spender's (China) defense spending during that year (108.2 billion)[153]. Out of that $700 billion spent in 2008, over $400 billion was contracted out to private companies. Between FY2004 and FY2010, over 215 billion went to weapon procurement. Most of that money went to the major defense contractors: Lockheed Martin, Boeing, Northrop Grumman, Raytheon, and General Dynamics[154]. From FY2000 to FY2017, Department of Defense contracts went from a nominal value of $189 billion to $320 billion. In 2008, defense contracting reached a peak of $450 billion. Throughout this time, defense contracting constituted roughly 8% of the federal budget[155].

As per the aforementioned economic model, these transactions made theoretical sense. However, in practice, the huge increase in defense spending and contracting did not always make economic sense. One integral example is a 2002 contract between Boeing and the Department of Defense. Boeing signed a leasing agreement with the

---

[152] Schwartz, Moshe, John F Sargent Jr, and Christopher T Mann. "Defense Acquisitions: How and Where DOD Spends Its Contracting Dollars," n.d., 29.
[153] William D Hartung, "The Military-Industrial Complex Revisited: Shifting Patterns of Military Contracting in the Post-9/11 Period," *Watson Institution for International and Public Affairs*, 2011, https://watson.brown.edu/costsofwar/papers/2011/military-industrial-complex-revisited-shifting-patterns-military-contracting-post-911)
[154] Ibid.
[155] Ibid.

Department of Defense to supply 100 commercial 767 planes to be converted into refueling tankers for the conflict in the Middle East. The new 767s would replace the Air Force's current fleet of 410 KC-135Rs and 126 KC-135Es. The leasing agreement totaled $26 billion dollars[156].

Mitchell Daniels Jr., director of the Office of Management and Budget (OMB) released a memo analyzing the deal. In the memo, Daniels stated that actual per unit cost of a commercial 767 is $90 million. He calculated that the nominal value of the leasing agreement should be approximately $1 billion[157]. The OMB conducted an Economic Service Life Study and a Tanker Requirement Study and found that out of the current fleet of over 600 carriers, only 6 would need to be replaced before 2040. The current fleet at the time had a total fuel carry capacity of 105 million pounds, whereas the new fleet of 767s only had a 103-million-pound capacity[158]. Daniels made three recommendations in a second memo to the Senate based on these findings:

(1) Do nothing. The OMB estimated that the costs of maintaining the current fleet is an increase of $23 million each year. However, these costs are far smaller than spending $26 billion.

(2) Buy the planes at face value. It does not make economic sense to spend $25 billion more than you have to. That excess money could be allocated among the department for different uses.

(3) Convert the 126 KC-135Es to the KC-135R model. This would cost only $3.2 billion, still far lower than $26 billion[159].

---

[156] Ibid.
[157] Mitchell E. Daniels, "Memo to Senator John McCain," Office of Management and Budget § (2001))
[158] Mitchell E. Daniels, "Memo to Senator John McCain," Office of Management and Budget § (2002))
[159] Ibid.

The three recommendations highlighted two major problems with the deal. First, there was no urgent need for 100 new 767s. The two studies performed by the OMB determined that 530 carriers out of the then-current 536 carrier fleet would be operational for the next 38 years. Second, it made no economic sense. Congress could have saved at maximum $25 billion dollars by not making this deal. These funds could go to strengthening weaker parts of the Defense budget, or be allocated to other departments that need the funds more. This deal seems like a bad idea and runs contrary to how a government should run. Boeing made $26 billion from this deal. At the time, the contract was predicted to grow exponentially, and eventually bring the manufacturing giant a profit of around $100 billion[160]. Boeing, as a profit maximizing firm would enter into any deal that would bring in an inflated revenue compared to their costs.

The military industrial complex is a two-way beneficial relationship: the value that the deal brought to the government therefore would have had to exceed the cost of spending $25 billion more than needed in order for it to be worthwhile. One conjecture on the US's benefit is that it felt an updated arsenal of weapons would push them towards a military hegemony. It would also give them credibility and an edge in the war on terror[161]. Another conjecture is the benefits that the industry lobby has on individual members of government. The individual voting members of the US congress receive lobbying money, specifically in the form of campaign donations. They then are influenced to vote a particular way that benefits the source of the lobby, which is the

---

[160] "Rules Circumvented on Huge Boeing Defense Contract - The Washington Post." Accessed January 26, 2020. https://www.washingtonpost.com/archive/politics/2003/10/27/rules-circumvented-on-huge-boeing-defense-contract/fd9df9c4-4bf2-4604-b392-e926b43f9834/.

[161] William D Hartung, "The Military-Industrial Complex Revisited: Shifting Patterns of Military Contracting in the Post-9/11 Period," *Watson Institution for International and Public Affairs*, 2011, https://watson.brown.edu/costsofwar/papers/2011/military-industrial-complex-revisited-shifting-patterns-military-contracting-post-911)

weapons industry in this case. In FY2016, the top 100 lobbyists generally spent $289M on lobbying and got $262B in contracts in return. For defense and aerospace specifically, the median return on investment was $1,120 for every dollar spent lobbying[162]

This existing evidence allows shows that the domestic lobby has an effect on government weapons policy through the existence of the military industrial complex.

The Military Industrial Complex in Russia

The military industrial complex in Russia is less convoluted than in the United States because most of their defense industry is either state owned, or has direct ties to top levels of Russian government. The government of the former Soviet Union operated on the principle of Nomenklatura. This was the principle that job opportunities were given to those deemed worthy based on a criterion of origin, professional history, readiness to fall in line with party orders, and loyalty to their superiors[163]. The resulting de facto class of communist party elites held influential posts in both the government and important industries. Although the nomenklatura seemingly died with the breakup of the Soviet Union, it has a lasting effect on the distribution of government and industry leaders in Russia today. In 2020, nomenklatura has a milder yet still nepotistic feel to it. Those who run Russia's state-owned corporations give a good illustration of the Russian political system as a whole.

Rostec is Russia's military industry company. The state-owned behemoth incorporates over 700 companies and employs over a half a million people. Rostec oversees research and development of military technologies, and owns plants where

[162] "Top Federal Contractors Spend Millions on Influence, Get Billions in Contracts." Accessed February 4, 2020. https://www.pogo.org/press/release/2017/top-federal-contractors-spend-millions-on-influence-get-billions-in-contracts/.
[163] "Nomenklatura | Politics | Britannica." Accessed April 5, 2020. https://www.britannica.com/topic/nomenklatura.

that technology is turned into actual weaponry. Rostec not only monopolized Russia's military industry, but controls a large part of Russia's civilian industries: mostly automobile, airline, and titanium companies. The CEO of Rostec, Sergey Chemezov is a member of Vladamir Putin's inner circle. Rostec merged with Marathon Group (pharmaceutical assets), whose co-owner is the son in law of the Russian minister of Foreign Affairs[164]. Typically, vertical mergers happen when the two firms in question can create synergies. However, this merger is suspected to be a political grab by the Russian government to take state ownership of industries that provide them power and clout on the international level. It is also a reflection of the system of patronage that is deeply rooted in the Russian government. It is a mutually beneficial relationship, where actors act to maximize the utilities of each other, rather than thinking about the social benefit to the society as a whole. Disarmament would mean the reduction in business for the defense industry, which negatively impacts those in the government who profit off of that industry. Therefore, it is easy to postulate that the needs of the defense industry influence the decisions of the Russian government when it comes to weapons control and disarmament.

The Military Industrial Complex in China

Due to the centralized nature of the Chinese government, the military industrial complex takes a different form than in the United States. Rather than lobbying as the fundamental tie between the military and industries, the Chinese government is in the process of combining the two through the state controlled Civilian Military Integration

[164] "The Inner Workings of Rostec, Russia's Military-Industrial Behemoth | Wilson Center." Accessed February 4, 2020. https://www.wilsoncenter.org/blog-post/the-inner-workings-rostec-russias-military-industrial-behemoth.

(CMI) program. The Chinese government purports that the only way to build a military capable of winning informationalized wars is to integrate the military with civilian industries. Consolidating industry and military cuts costs and streamlines efficiency, and the Chinese Communist Party (CCP) believes this is the way to increase international defense competitiveness[165,166].

One of the main drivers between this consolidation is China's problems with their defense budget. The budget is currently not big enough to pay for all of the Peoples' Liberation Army's (PLA) development plans. Slow economic growth in China has constrained defense spending, and government officials are reluctant to increase budget allocation for fears that it would have a negative impact on the economy as a whole. CMI is a proposed solution to this resource constraint. It plans to eliminate any overlap in research and manufacturing between different industries and the military. The military and relevant industries will overlap and share technology, research, development, logistics, training, and all their associated costs. The CCP hopes to broaden the base from which the PLA draws funding from by integrating its supply chain into its industry. By cutting costs, China plans to increase their output and profit gains, mostly in the defense and technology industries[167].

This plan, while driven by economic factors, hands over control of civilian industries to the CCP. The elimination of a wholly civilian sector gives the defense sector more power and influence. Their research, development, and most importantly, policy proposals will have a great effect on the PLA's policy because it is going to be the base from which they get their funding, equipment, and technology. Technological

---

[165] Chang, Parris H. "China's Military-Industrial Complex: Its Influence on National Security Policy," n.d., 11.
[166] "Xi, Huawei and China's Powerful Military-Industrial Complex." *Nikkei Asian Review*. Accessed December 31, 2019. https://asia-nikkei-com.proxy.lib.umich.edu/Editor-s-Picks/China-up-close/Xi-Huawei-and-China-s-powerful-military-industrial-complex.
[167] Lafferty, Brian. "CIVIL-MILITARY INTEGRATION AND PLA REFORMS," n.d., 34.

advancement in order to beat technological challenge or warfare is the goal of the PLA. Therefore, achieving their goal relies on the defense industry which has the power to influence that policy in turn[168].

This relationship will create synergies, but can have an effect when it comes to cooperation. Like Russia, the symbiosis between the industry and the military makes it so a negative effect on one negatively effects the other. This would prime the government to consider the defense industry when making decisions that affect their military and through that, their military power. China has already received international scrutiny for abusing cyberspace, especially the theft of intellectual property. When it comes time to enter into cyber disarmament cooperation, it will be important to consider how the CMI initiative affects the government's willingness to disarm their share of cyberspace.

The relationship that is a product of the military industrial complex is going to be important to consider in the future. Once we obtain more information in the future, I implore political scientists to test the reasonability of this hypothesis.

Hypothesis 4: As the tactical value of a weapon increases, cooperation becomes less likely

I hypothesize that as the tactical value of a weapon increases, cooperation becomes less likely. Conversely, as the tactical value of a weapon decreases, cooperation becomes more likely. The intrinsic value that a country assigns to a weapon brings to a country can affect the payoff structure for international cooperation. This begs the question: if the value of a weapon is sufficiently high, does that affect the cooperative outcome? I

[168] Ibid.

measure the tactical value of a weapon by equating the tactical value of a weapon with the benefit that the weapon gives to a country's strategy. In Appendix 1, I further detail and justify my methodology for measuring the tactical value of a certain weapon. In the theoretical construct where this hypothesis was to be the case, then we would see this clue:

Clue 1: net positive payoff (tactical value) and existence of relevant obstacles to cooperation

To find this evidence, I use a set of guiding principles that is found in Appendix 1. The tactical value of the weapon alone has low probative value. I thus look for evidence regarding the existence of cooperation problems. That also has a standalone low probative value. However, the two pieces of evidence together have probative value, and I can use that to determine if we have reason to believe this hypothesis holds true.

Nuclear Weapons

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 nukes 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[169]. Looking through the lens of deterrence, there are substantial benefits to holding nuclear weapons.

Value of Use

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 the world for up to millennia after the attack[170]. 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 low 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. On top of the destructive physical consequences the use of nuclear weapons would incur,

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

users of nuclear weapons would face harsh sanctions are penalties from other countries. These consequences are of the likes of the arms bans and economic embargo on Iran. The effects of the embargo have seeped beyond just punishing the Iranian government. The embargo has had a negative impact on the Iranian economy, which disproportionately effects those who are from rural, low income areas. As a part of the sanctions, Iran's ability to use foreign assets was frozen, which has consequently disabled Iran from seeking international aid to purchase necessary medicines[171]. Many have called this a humanitarian crisis, as there is a shortage of access to live-saving drugs.

Cost - Benefit Analysis

When looking at the big picture effects of stockpiling and using nuclear weapons, the costs far outweigh the benefits. It is hard to find any substantial benefit to using a nuclear weapon beyond retaliatory deterrence. When weighing that benefit against the costs, I assign nuclear weapons a negative net payoff. Therefore, I conclude that this weapon has no tactical value[172].

Cooperative Outcome

A high level of cooperation was achieved for nuclear weapons. This is emblematic in the creation of the International Atomic Energy Agency (IAEA) and The Nuclear Non-Proliferation Treaty (NPT). The confirmed nuclear weapon states did not have to give up their stockpile of nuclear weapons under the NPT. To appease non-nuclear weapon

[171] Cellan-Jones, Rory. "How Renewed US Sanctions Have Hit Iran Hard." *BBC News*, December 9, 2019, sec. Middle East. https://www.bbc.com/news/world-middle-east-48119109.

[172] This assessment prompts the question: if nuclear weapons have no tactical value, why did nuclear weapon states keep them? I acknowledge that limitations of my analysis in completely understanding how tactical value applies to nuclear weapons. If I had more time and the means, this is a question I would further look into.

states, the confirmed nuclear weapon states agreed to non-proliferation and sharing of nuclear energy research for peaceful use. The ability of this compromise to be reached, and the sustained cooperation on both the IAEA and NPT show high levels of cooperation without obstacles stemming from incentives to defect.

Chemical Weapons

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 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. However, it is a small benefit, because the landscape of war has shifted away from that which called for chemical weapons. This change is discussed in the next section.

Value of Use

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[173]. 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

[173] 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.

existed[174]. Today, there is not a lack of ammunition that would create a need for a chemical weapon. The existence of gas masks also renders chemical weapons ineffective. Chemical weapons offered a benefit for close range warfare. Now, since wars can be fought from afar, using technology such as drones and inter-continental ballistic missiles, the strategic value of chemical weapons is diminished. There are little to no benefits of having chemical weapons in a military arsenal for potential deployment.

There is 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.

Cost – Benefit Analysis

These clues give me support to assign a negative net payoff to chemical weapons. The strategic value of the weapon has sufficiently diminished due to a shift in the conditions of war away from one that made it a useful weapon. The consequences of the using the weapon outweigh the benefit of stockpiling and using the weapon due to low deterrence value. When weighing that benefit against the costs, I assign chemical

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

weapons a negative net payoff. Therefore, I conclude that this weapon has no strategic value.

Cooperative Outcome

Although the negotiations of the CWC took a long time, this is not emblematic of problems stemming from incentives to defect. Rather, the prolonged nature was because there was a general consensus among states to avoid that these obstacles needed to be avoided. The existence of the CWC and OPCW and their relative success in prohibiting the proliferation of chemical weapons is emblematic of high levels of cooperation with no problems stemming from incentives to not cooperate.

Biological Weapons

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 would never happen, because biological weapons threaten large populations of people[175]. There is such a strong international taboo against the use of biological agents used to purposely infect humans that states have historically only developed these weapons in secret.

Value of Use

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

[175] "Deterrence, without Nuclear Winter." *Bulletin of the Atomic Scientists*, March 9, 2015. https://thebulletin.org/2015/03/deterrence-without-nuclear-winter/.

nature, as it is a naturally occurring bacteria. The equipment needed to make a bioweapon double as basic medical research equipment. Both agents and the equipment 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". For comparison, North Korea is estimated to have spent between $18 million to $53 million on each individual nuclear warhead[176]. Comparatively, one assessment puts the cost of producing one military grade biological weapon at less than $100,000. Such program requires five biologists and take just a few weeks using equipment that is readily available[177]. This scenario resembles a more "sophisticated" biological weapons program, which implies that they could be made at an even lower cost. This implication is supported by the ability of individuals and small groups to gain access to biological weapons (anthrax and salmonella).

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. 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[178]. 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.

---

[176] 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.
[177] "CHEMICAL AND BIOLOGICAL WEAPONS:
THE POOR MAN'S BOMB." *Federation Of American Scientists*. Accessed April 5, 2020. https://fas.org.
[178] 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/

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[179]. Black biology can be used to increase the virulence and potency of a pathogen. This is a very terrifying reality, but adds incredible valuable for biological weapons. In 2020, COVID-19 has tanked the global economy and, left millions of people without jobs, homes, and incomes. With the existence of black biology and the right motive, scientists could realistically replicate this virus into a weapon with global consequences[180].

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 to an attacker, as found in Hypothesis 2. The Soviet Union's biological weapons program accidentally released anthrax into a small town. They were not held accountable because they successfully covered it up as a natural outbreak due to tainted meat. Biological weapons, because of the aforementioned characteristics, are valuable to countries that do not have nuclear weapons[181]. 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 nuclear stockpile. However, it is important to note that the value derived from these weapons can only be collected if they are deployed. There widely believed international

---

[179] 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.
[180] "Biological Warfare: An Emerging Threat in the 21st Century: 1/01." Accessed April 5, 2020. https://news.stanford.edu/pr/01/bioterror117.html.
[181] Ibid.

norm against the use of biological weapons. This norm is that using biological weapons is immoral and inhumane. The vast acceptance of this norm is an effective deterrence for its use. Adherence to the norm is rationale for states severely punishing 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. This harms dynamic innovation, which can cause the country to lag behind other countries that have high levels of innovation and research.

I have mentioned that plausible deniability reduces the chances of being linked to an attack. However, this characteristic does not completely protect a country from being found out, it just reduces their chances. In 2018, a former Russian military officer and his daughter were in England. They were double agents for Russian and British intelligence. Russia was suspected of carrying out the attempted assassination to punish them. Russia denied this claim. Regardless, England used textual clues and a criminal investigation to build a pretty compelling case against Russia. As a result, England and 28 other countries expelled 153 Russian diplomats from the country. Since, the relationship between England and Russia has been strained[182,183]. This situation is an example of the strength of the international norm against the use of biological weapons. Even though Russia was not attributed, plausible deniability does not protect actors

[182] "Russian Spy Poisoning: What We Know so Far." *BBC News*, October 8, 2018, sec. UK. https://www.bbc.com/news/uk-43315636.
[183] "U.K. Charges 2 Men in Novichok Poisoning, Saying They're Russian Agents - The New York Times." Accessed April 5, 2020. https://www.nytimes.com/2018/09/05/world/europe/russia-uk-novichok-skripal.html.

completely, especially in an age of espionage. Knowing the type of reaction countries could have against violators is a deterrent.

Another cost of using biological weapons is that pathogens do not respect borders. If a country chose to use a biological weapon against an enemy, there is no guarantee that the biological agent would not spread to other countries, including the perpetrator's own. This is widely believed to be the reason that Germany did not use biological weapons in World War II. There is also evidence that Japan accidentally infected over 1,000 of its own during biological attacks on China[184]. Unpredictable winds, changing terrain, and movement across borders makes this fear plausible. This is an extreme risk that some countries are not willing to take, when also considering the costs of being attributed to the attack and punished.

Cost – Benefit Analysis

Biological weapons have a high value stemming from their low cost, plausible deniability effect, and low difficulty to build. However, they are rarely used and have no value as a deterrence. They also have an incredibly strong taboo against their use, which would result in harsh consequences if a biological weapons user is identified. When weighing the costs and benefits, I assign a net neutral payoff to biological weapons. This corresponds to no tactical value.

Cooperative Outcome

The BWC was opened for signature only two years after negotiations started. The UK and the US purported that biological weapons posed a less intractable problem than

[184] 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/

chemical weapons, while still carrying a very serious threat. This stems from the fact that although many world powers developed and stockpiled biological weapons, they were rarely used. This sentiment was widely accepted, and an agreement was reached with few roadblocks to cooperation. This is reflective of a high level of cooperation.

Cyberweapons

To assess the tactical value that a cyberweapon has, I will be considering cybercapabilities more generally. Cybercapabilities is the more general category under which cyberweapons fall, and are often used to characterize a country's cyberweapon arsenal. The definition of a cybercapability that I will be using is "a capability designed to access a computer system or network to damage or harm living or material entities"[185]. It is important to think about this more generally, because a cyberweapon does not constitute one specific type of weapon. Rather, the customization of cyberspace to replicate a variety of weapons or other actions that a military could use in real life.

Deterrence Value

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. 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.

[185]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.

Value of Use

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. 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. 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 cybercapability 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 who "delivers" the attack. These personnel are safer sitting behind a computer screen than flying over a war-zone and dropping a bomb[186].

Cyberweapons move war into an intangible platform, which gives the weapon an extremely covert nature. The secretive nature of a cybercapability limits the exposure that the actor has to the target. Espionage is a very common form of cybercapabilities because it allows the actor to act as a burglar for information without actually having to go somewhere and steal it. This makes it harder for the target, or third parties, to identify the perpetrator of the attack. This reduces the risk that the perpetrator will be caught and subsequently punished. When weighing the costs and benefits of a certain method of action, knowing the chances of being caught and punished are low, incentivizes an actor to choose that outlet. Another value derived from covertness is the

[186] George Perkovich and Ariel Levite, *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017))

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 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[187].

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[188]. 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[189]. One nuclear warhead supposedly costed North Korea $18-$53 million dollars[190]. 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

---

[187] 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.
[188] Ibid.
[189] "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.
[190] 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.

coded, the process to build one becomes standardized. There is a lot of information sharing within the IT community, so it is not hard to find specific codes. It takes less time, effort, and money to write new codes, because many code writers just build off already existing malwares[191]. 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[192]. 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[193]. 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. Parity also limits swaggering. Swaggering is the ability to use the ownership of a weapon to display a country's might and power. Cyberweapons have a non-material ontology and often cannot be "showed

---

[191] "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.
[192] 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.
[193] Ibid.

off"[194]. It also seems less impressive, or threatening, if there is more cyberweapon parity between countries.

Cost – Benefit Analysis

Cybercapabilities offer a flexible, cheap, multipurpose, precise and covert weapon option. Although there are some drawbacks, those conditions also spur more technological development, which could be seen as a positive. Therefore, I conclude that cyberweapons have a net positive payoff. This corresponds to positive tactical value. This supports the existence of clue 1, with low standalone probative value.

Cooperative Outcome

In the lens of this Hypothesis, I surmise that cyberweapons are too valuable to a country to incentivize cooperation. Currently, there is limited cooperation to regulate cyberweapons. While there is agreement that this is something that needs to be done and can be done in international law, the conditions for successful cooperation have not been met. This is reflective of a low level of cooperation due to obstacles to cooperate. This supports the existence of clue 1, with low standalone probative value.

Here are the overall results for Hypothesis 4.

	Tactical Value	Cooperation Problem
Nuclear Weapons	No	No
Chemical Weapons	No	No
Biological Weapons	No	No
Cyber Weapons	Yes	Yes

[194] Ibid.

The existence of evidence for positive tactical value and cooperation problems in the cyberweapons case supports the existence of clue 1. The existence of clue 1 gives me reason to believe that Hypothesis 4 holds true. The lack of tactical value and existence of no related cooperation problems for nuclear, chemical, and biological weapons further supplements that we have reason to believe this hypothesis is the case. This proposition is justified through Mill's method of difference.

Section VII – Conclusion

Findings

Hypothesis 1:

C1. NW. E1, C1. NW. E2, C1. NW. E3, C1. NW. E4, C1. BW. E5, C1. BW/CW. E6, and C1. BW/CW. E7 supports the existence of Clue 1. Clue 1 has high probative value. The lack of evidence and the opposite outcome in the cyberweapons case study supplement this value. Thus, it gives me strong reason to believe this hypothesis holds true.

Hypothesis 2:

C1. BW. E1, C1. BW. E2, C1. CY. E3 and C1. CY. E4 supports the existence of Clue 1. Clue 1 has high probative value. The lack of evidence and the opposite outcome in the nuclear weapons and chemical weapons case studies supplement this value. Thus, it gives me strong reason to believe this hypothesis holds true.

Hypothesis 4:

I found evidence that supports both halves of clue 1 in the cyberweapons case. Clue 1 has probative value. The lack of evidence and the opposite outcome in the nuclear

weapons, chemical weapons, and biological weapons case studies supplement this value. Thus, it gives me reason to believe this hypothesis holds true.

Hypothesis 1 and 2 have high probative values, and thus give us strong reason to believe these hypotheses are the case in our world. Hypothesis 4 relies on low probative value collected evidence. With the addition of theoretical justifications that I defend in Appendix 1, I conclude that Hypothesis 4 has probative value. Thus, we have reason to believe this hypothesis is also the case in our world. Given reasonable belief that Hypotheses 1,2, and 4 are the case, I believe that these three things affect cooperation on international security issues:

(1) The degree to which consequences of a weapon are understood

(2) The attribution problem that the weapon poses

(3) The level of tactical value of the weapon

Hypothesis 3 represents a limitation that I faced. When thinking about the clues I would need to see to support a belief in this hypothesis, I recognized that those did not yet exist in the world. Rather than assign low probative value to these clues and try to piece together a loose argument, I focus on hypothesis generation. The issue of cyberspace generally is one that will take many years to tackle, since it is both relatively new, and changing as technology advances. I believe in the future, there will exist clues with high probative value and sufficient evidence to support them. I contribute a unique stepping stone to better understanding cooperation with the generation of Hypothesis 3's theory.

Implications

After coming to these conclusions, I bring attention back to my research question: why do states 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 cooperation on cybersecurity continues to pose a challenge. I have found evidence that a lack of understanding cyberweapon consequences, a large attribution problem, and a high level of tactical value are all creating obstacles to international cooperation on certain issues. I believe that these three challenges are affecting the cooperative payoff structure for states. More specifically, each individual problem compounds to make the non-cooperative payoff higher than the cooperative payoff. This situation is metaphorically reflective of the prisoner's dilemma. Although all states would be better off cooperating, their individual preferences are to not cooperate. The "cooperative game" ends in a world without cooperation, because all actors select the not-cooperate strategy. When no one cooperates, each actor receives the lowest possible payoff. This is because the individual non-cooperative payoff hinges on the assumption that other states will cooperate, and non-cooperators will get to free ride off of those benefits. However, when no actor cooperates, there are no benefits and everyone is made worse off.

We are seeing this play out in real life. In order to avoid the non-cooperative outcome, the individual cooperative payoff needs to be higher than the non-cooperative payoff. As aforementioned, my findings indicate that the state of the world is making the non-cooperative payoff sufficiently high. Thus, I believe that cooperation will hinge on taking measures to lower the non-cooperative payoff sufficiently below the cooperative payoff.

Recommendations

Unfortunately, a big factor in changing the payoff structure relies on time. Cyberspace is an issue that we are collecting new information on every single day. 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. However, only time will be able to help us complete the puzzle and see the full picture. Once we see the full picture, we will have a better sense of exactly what we need to do to cooperate.

Although the prognosis of "wait it out" seems grim, there are steps that can be taken to shorten the duration of time. This is where my paper makes the biggest contribution. Cyberweapons are not that different than traditional weapons of mass destruction. A lot of the characteristics of cyberweapons that increase its non-cooperative payoff existed and have subsequently been avoided in nuclear, chemical, and biological weapons cooperation. Cybersecurity decision makers should use these three weapon case studies to figure out what actions they can take to limit the cooperative obstacles they face. Specifically, here are two preliminary steps that decision makers can take:
(1) Share information globally to better understand the issue. This can be helpful in two areas:

(A) Understanding the consequences of cyberweapons. International lawmakers should establish a forum for different world actors to exchange information on known consequences. One feature of this forum should be a database of all known consequences. As new consequences emerge, world leaders should be pressured to share that information with the database.

(B) Creating technology to solve the attribution problem. 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.

(2) Work to promote an international taboo against the unregulated use of cyberspace. Despite the incomplete nature of the information the world has, there is still enough to warrant concern. International decision makers should work to build acceptance of the norm that unregulated use of cyberspace is harmful to all people. with the hopes that it pressures relevant actors to cooperate with more urgency.

As mentioned before, this is a problem that will not be solved for a while. A better understanding of the reasons why can help shorten this time period. 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 1

Each country's government, especially their executive or military branches, place intrinsic values on ownership of different types of weapons. For some, this value may be greater than the value (payoff) that they receive from cooperating to regulate this weapon. 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 tactical value that does not involve monetary costs. I assess the value of a weapon by evaluating the characteristics of each of the weapons. The characteristics are found using a guiding set of principles that intuitively would be reasons to or to not invest in the weapon. I conceptualize value as the net benefits that ownership of a weapon incurs on the specific country.

Assumptions:

(1) the existence of tactical value lowers incentives to cooperate by increasing the payoff to not cooperate. Non-cooperating would mean retaining the benefits of having the weapon in some capacity. Cooperating would mean limiting or completely erasing the benefits of having the weapon in some capacity.

(2) Negative net payoff concludes no tactical value. There cannot be anything less than no tactical value.

(3) There is a whole range of tactical value that the weapon can have. Each level correlates to a certain degree of effect on cooperation. For the sake of simplicity, I

assume that either tactical value exists and thus hinders cooperation or it does not exist and incentivizes cooperation.

Steps

(1) Find attributes of having the weapon at your disposal

(2) Assign each one to be a pro (benefit) or con (cost)

(3) Do a cost benefit analysis to figure out if that weapon has a net positive payoff or a net negative payoff[195]

(4) If net positive, then we conclude tactical value

(5) If net negative, then we conclude no tactical value

Guiding attributes

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

If the weapon were to be used…

(2) What are the chances of attribution and punishment?

(3) Is there an international taboo against the use of the weapon that would incentivize punishment?[196]

(4) Is it multipurpose?

(5) Is it cost effective?

(6) Would another weapon be better suited for achieving the same goal?

[195] This is done in a vacuum, not in a strategic setting where the payoff depends on what others do.
[196] The time frame for the existence of an international taboo is before international cooperation