STAR WARS, POISON GAS, AND CYBERSECURITY: LESSONS FROM THE PAST FOR A BETTER FUTURE

A THESIS

SUBMITTED TO THE

INTERSCHOOL HONORS PROGRAM IN INTERNATIONAL SECURITY STUDIES

Center for International Security and Cooperation

Freeman Spogli Institute for International Studies

STANFORD UNIVERSITY

By

Rachel Hirshman

May 2018

Advisers:
Dr. Herbert Lin and Dr. Coit Blacker

Abstract

Though numerous countries have been victims of hostile operations in cyberspace ranging from espionage of trade secrets to a shutdown of the nation's electrical grid, little progress has been made in the international system towards a formal international agreement to regulate activities in the domain. Much of the existing literature on arms control in cyberspace is pessimistic and emphasizes why cooperation will fail without communicating how cooperation might succeed. This thesis seeks to fill that gap by examining the question: under what conditions will international agreements in cyberspace be more likely? Assessing two historical case studies in the Reykjavik Summit and the Chemical Weapons Convention for their implications regarding such agreements, this thesis explores the conditions which make an agreement in cyberspace more likely through a lens of five variables - technology, geopolitical dynamics, state interests, domestic environments, and information. The most important condition of an international agreement in cyberspace is the willingness of parties to make reciprocal concessions during negotiations. This thesis further finds that the existence of the following conditions increase the likelihood of an agreement: the major players in cyberspace are committed to the objective of an agreement, the use of cyber tools rather than the tools themselves are being regulated, and private sector concerns are included in negotiations. These findings suggest areas of focus for current world leaders seeking to regulate the cyberspace domain. Further, this thesis concludes that cyberspace does not exist in a vacuum and that negotiators on cyberspace have much to learn from historical cases.

Acknowledgments

I am immensely grateful for all who advised, supported, and guided me throughout the process of conceiving and writing this thesis. First, thank you to my primary adviser, Herb, without whom this thesis would not be what it is. Herb consistently provided me with feedback and constructive criticism that forced me to think more critically about my analysis and led to a more thorough and polished final product. Thank you for the many hours that you spent with me from discussing the initial idea over a year ago to the final days sitting over breakfast and deliberating final revisions. Your mentorship and friendship means a lot to me, and I am very lucky to have had you by my side during this project.

Professor Blacker, thank you imparting your wisdom and experience upon us. Thank you as well for your invaluable feedback on numerous chapters that I submitted to you, some with very short notice. I feel fortunate to have been able to work with you throughout this process and know that my writing and analysis is much stronger as a result.

Professor Zegart, I am very thankful for your mentorship and support. Your critical eye on chapter drafts helped develop and solidify my thinking and arguments. Rochelle, thank you for pushing us to think critically about social science methods and for your thoughtful feedback on draft chapters. To all three of you, thank you for creating an environment that allowed all of us, writing on a diversity of topics, to engage with and learn from each other.

Of course I also owe a huge debt to my CISAC cohort whose comradery and persistent support made this process well worth it. Your work ethic, thoughtful engagement, and determination are inspiring and helped push me to be a stronger writer and thinker. To Rachel, I am so thankful for your friendship and loyalty. The many days and nights that we spent together in the Grove and Tridelt computer clusters laughing and working together are to credit for much of the progress that I made on this thesis throughout the year. I am very fortunate for how much our friendship grew this year, and I cannot wait to watch all the incredible things that you do in the future. You are my inspiration.

There are many other individuals who thoughtfully donated their time to discuss the future of international agreements in cyberspace with me. Their insight and feedback were indispensable. Thank you to Andy Grotto, John Hart, Jason Healey, Toomas Ilves, Kris Kasianovitz, Matthew Meselson, Joseph Nye, Philip Taubman, Michael Sellitto, Secretary George Shultz, Rebecca Slayton, and Abraham Sofaer.

To all my wonderful friends who were by my side throughout this year of researching and writing, your encouragement and support means the world to me.

Finally, I owe so much to my family who supported me during the entire process. Dad, thank you for providing edits and comments on a full draft. Mom, Jason, and Anna, thank you for letting me bounce ideas off of you and for listening to me as I talked about topics and events that likely meant very little to you.

List of Acronyms

ABM	Anti-ballistic missile
BMD	Ballistic missile defense
BTWC	Biological and Toxin Weapons Convention
BW	Biological weapons
CBI	Confidential business information
CIA	Central Intelligence Agency
CW	Chemical weapons
CWC	Chemical Weapons Convention
DOCs	Discrete organic chemicals
DoD	Department of Defense
GGE	Group of Governmental Experts
GPC	General Purpose Clause
INF	Intermediate-Range Nuclear Forces
IR	International Relations
NPT	Nuclear Nonproliferation Treaty
NSA	National Security Agency
OPCW	Organisation for the Prohibition of Chemical Weapons
PSF	Phosphorous, sulfur, or fluorine
R&D	Research and development
RCAs	Riot control agents
SDI	Strategic Defense Initiative
START	Strategic Arms Reduction Treaty
U.S.	United States
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UNGA	United Nations General Assembly
UNODA	United Nations Office for Disarmament Affairs
USSR	Union of Soviet Socialist Republics
WMDs	Weapons of Mass Destruction

Table of Contents

Table of Figures

Table of Tables

Chapter 1 Introduction

In the vast majority of international security domains, we have witnessed the development of some form of international coordination to establish norms of action, international agreements, and arms control regimes. Some prominent examples are the Nuclear Non-Proliferation Treaty (NPT), which seeks to decrease the threat of nuclear weapons and the United Nations Convention on the Law of the Sea (UNCLOS), which regulates state behavior in international waters. In recent years, world leaders and international institutions alike have called for international engagement to combat the cyber threat that states realize is proliferating and becoming more and more devastating. However, neither a cyber equivalent of the NPT or UNCLOS has been developed nor has any comprehensive international agreement meant to significantly curb the cyber threat been put in place. Why is that the case? And what are the prospects for the evolution of such agreements in the future? This is the puzzle that this thesis seeks to examine. More concretely, it asks: Under what conditions will international agreements in cyberspace be more likely?

This question is important for three primary reasons. First, the threat vectors in cyberspace are diverse, making effective, all-encompassing defense nearly impossible. With fast-paced technological innovation, the increasing number of pathways by which malicious actors can manipulate information technology systems for political or economic gains creates an environment in which the defense is always trying to catch up to the offense at a high economic and labor cost.

Second, cyberspace is an environment unlike most the international system has experienced before in which traditional power dynamics between states are much less relevant. States such as Iran and North Korea, with significantly fewer military and economic capabilities than the major powers, can execute offensive cyber operations that exact significant damages on major

powers. Unlike the nuclear domain where only the major powers, for the most part, have the resources and capabilities to build and maintain a nuclear arsenal, cyberspace is easily accessible even by amateurs.

Last, there is interest in some form of regulation of cyberspace through norms or a formal international agreement as the states with the strongest capabilities like the U.S. are also the most reliant on information technology and therefore the most vulnerable. As a result, U.S. presidents and prominent diplomats in addition to leaders of other great powers have called for international action in cyberspace ranging from the establishment of norms to a comprehensive treaty negotiated at the United Nations (UN).

Given these three characteristics of the cyberspace environment and public statements by international leaders and organizations, an international agreement is sensible according to the historical record and a desired outcome for some of the most powerful states. However, leading scholars of cybersecurity also note that while current defenses are insufficient to defend against the full range of threats, an international regime is implausible and unlikely. Empirically, while some progress has been made to informally codify the application of international law to cyber[1] and to formally establish measures to combat cybercrime[2], little has been achieved that would be regarded as steps towards an international regime for cyberspace.

Theoretical Framework

[1] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013); and Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[2] Council of Europe, *Convention on Cybercrime,* 23 November 2001.

This thesis seeks to fuse the international relations (IR) literature with the literature on cyber arms control to challenge the prevailing skepticism about international cooperation in cyberspace. In addition, this thesis will, through an analysis of past international agreements developed under similar conditions, assess the conditions under which international agreements in cyberspace will be more probable. This type of analysis has not yet, to be my knowledge, been conducted as the majority of the literature has focused on why cooperation will fail, without significant emphasis on how cooperation might succeed.

Additionally, most scholars have studied international cooperation in cyberspace either through analogies or by intently analyzing cyberspace itself. Very few authors have systematically analyzed how prevailing theories of international cooperation in international relations theory may apply to cyber. In conducting this assessment through two case studies, I can empirically analyze the importance and criticality of different explanatory variables. Therefore, I can carefully explain the conditions under which international agreements will be more likely. The two case studies I will use for this analysis are the failed negotiations to eliminate nuclear-armed ballistic missiles at the Reykjavik Summit in 1986 resulting from the introduction of the Strategic Defense Initiative (SDI) and the successful development of the Chemical Weapons Convention (CWC).

The qualitative analysis is centered on five explanatory variables extracted from the IR literature on international cooperation. The choice of these variables is not meant to be wholly exhaustive but will be assumed to be sufficient for the purposes of this thesis. In addition to assuming that these variables are sufficient, the variables are also assumed to be independent of each

other, even though that may not be the case in reality. The variables are as follows: technology, state interests, geopolitical dynamics, the domestic environment,[3] and information.[4]

Cyberspace and both case studies will be assessed according to this framework of variables to maintain consistency and systematically assess the conditions conducive to international agreements in cyberspace. Because the two cases have opposite outcomes, I can better analyze how the presence or absence of a variable influences the outcome and then how that may generalize to cyberspace. Additionally, qualitative analysis via case studies is the best way to answer the proposed question because international cooperation in cyberspace is relatively non-existent. So, to assess the cyberspace domain and under what conditions we would likely see an international agreement, I have to leverage available knowledge. Grounding the analysis in concrete case studies avoids a heavily theoretical analysis that may not totally capture the intricacies of the technology and the cyberspace domain.

The two case studies - the Reykjavik Summit and the CWC - have been chosen carefully so as to most accurately represent the environment of the cyberspace domain. The circumstances surrounding the Reykjavik Summit represent an environment akin to that of cyberspace. The SDI program was a technology-based revolution in the making. Nobody knew how it was going to

[3] The variable domestic environment refers to the characteristics of the governmental structure of the state (*e.g.,* democracy, autocracy, etc.) and the varying influence of domestic politics on the actions of the state on the international stage. The consequences of a particular domestic environment are particularly relevant when considering the priorities of a state in negotiations. For example, while Russia and China which are autocracies are especially concerned with information spreading that threatens the government's existence, the United States historically supports significant freedoms on expression and information. These positions, therefore, effect negotiating positions and possible treaty outcomes. Private sector involvement is also included in this variable.

[4] Information refers to the information made available to each party during negotiations and subsequently each party's interpretation of the information available to them. More specifically, the information variable encompasses the analysis of negotiating environments under conditions of asymmetric information and the disputes that arise due to conflicting interpretations of available information. Verification and enforcement also belong under the scope of this variable.

evolve, much like the future of technology and capabilities in cyberspace are unpredictable.[5] Further, the circumstances surrounding SDI were characterized by lively debates about the differentiation between offensive and defensive uses of the relevant technology. This same debate exists today regarding cyberspace. But until recently, the general consensus in the cyber literature has been that in the vast majority of circumstances cyber offense and cyber defense are not differentiable. Further, there were conditions of asymmetric information in addition to disagreement over interpretations and definitions analogous to cyberspace. While it can be argued that the negotiations at Reykjavik were unconventional, the principles of the negotiations and related archival records suggest that the participants viewed these talks like conventional negotiations. Regardless of this controversy surrounding the characterization of the summit as formal negotiations, I argue that these talks can still be considered a failed negotiation in the conventional sense just like the CWC resulted from successful negotiations.

The CWC negotiations similarly mirror anticipated future negotiations in cyberspace in many ways. Chemical weapons, like technology in cyberspace, are dual-use (*i.e.*, a chemical which is used to make a weapon is also used by industry to make drugs or other products just as the networks used by adversaries to attack states are used by the private sector for daily activities). Additionally, just like in cyberspace, the materials for a chemical weapons attack are easily accessible, and the chemical weapon can be disguised without much difficulty. The other relevant characteristics of the CWC are that the technology is characterized by a high pace of development and the agreement was multilateral in nature.

[5] Opponents and those skeptical of SDI started referring to the program as "Star Wars." "Star Wars" then became the colloquial term for SDI.

As with any approach, there are weaknesses to the case study analysis that I have chosen. Most prominently, there is not a perfect case study that can fully explain cyberspace, because if that did exist this thesis would be irrelevant. Therefore, the best that can be done is to carefully and thoughtfully choose case studies that can most appropriately be generalized to cyberspace. There will still exist an inherent problem of generalizability, but I controlled for this weakness as much as I could. A small sample size of two case studies further raises issues of inference and generalizability, but one case study independently would not sufficiently cover many of the intricacies of cyberspace that have led scholars of cybersecurity to dismiss the prospects of an international agreement. Similarly, with the time and resource constraints of this thesis, many more case studies would not allow for sufficient in-depth analysis and conclusions.

Argument

Given this analytical framework, this thesis finds that there are four conditions most likely to facilitate international agreements in cyberspace. The conditions are presented in order of relevance to the outcome of negotiations towards an agreement with the first condition being the most deterministic of the outcome. First, and most importantly, states must be willing to engage in reciprocal concessions. Mutual gain comes only if both sides are willing to sacrifice something for the sake of the common good. Second, agreements will be more likely if the major players in cyberspace are committed to the objective of an international agreement. Third, an important condition to making agreements more likely is that the proposed agreement is tasked with regulating the use of cyber weapons rather than the possession of technology or weapons themselves. Last, if the opinions of private sector companies who would be influenced by a proposed agreement and their desire to protect proprietary and confidential information are effectively integrated into the

negotiations for the agreement, the agreement will be much more likely. Evidently, the most important variable in increasing the likelihood of an international agreement is state interests as the first and second conditions listed both fall under that variable. Each of these conditions is elaborated and expanded upon in the following chapter according to the variable they correspond to.

Therefore, this thesis argues that the more of these conditions that are present the more likely an agreement will be. A shortcoming of this argument is that it does not assess precisely what combination of conditions is better than others. Additionally, given that the conclusions are drawn from a structured analysis of the two case studies, there are likely variables that are not exhaustively addressed in this thesis. For example, one could envision leadership personalities as another variable to account for in assessing the likelihood of an international agreement. While this variable is important, it requires much more subjective analysis that does not align with the approach taken in this work. Further, the conditions derived from this thesis's analysis are not meant to be deterministic of an international agreement but are rather descriptive of conditions that increase the probability of an agreement. This thesis's conclusions, however, still make a novel and important contribution to the literature.

Scope and Assumptions

The analysis that generated these conditions and this thesis's argument is predicated on various assumptions about the international system and state behavior. First, this thesis assumes that the international system is anarchic. Secondly, this thesis assumes that international behavior is shaped by state behavior not state power and that state behavior, for the most part, reflects do-

mestic preferences and domestic actors. Additionally, the international agreements and negotiations under consideration pertain to behavior between states and actions reasonably accepted to be conducted by a state.[6]

There are also various topics that are out of scope for this work's analysis. Assessing whether the resulting international agreement is effective is beyond the scope of this thesis and would be overly speculative and exceptionally complicated. There is still great value in negotiations and agreements regardless of their effectiveness. As will be seen in the case of the Reykjavik Summit, negotiations can lay the groundwork for future success in negotiations. Cyber activities by non-state actors, as important as they may be, are also beyond the scope of this thesis which emphasizes cyber activities between states. Further, my analysis will not be normative in nature but rather without judgment about state activity or the likely outcome. Similarly, I will not be assessing the underlying reasons why the contemporary cyberspace environment is the way it is despite there being many interesting questions that can be examined on this subject.

Definitions

Before proceeding, it is important to define clearly the key terms embedded in this thesis. The key terms to be defined are cyberspace, state, anarchy, regime, cooperation, and international agreement. The conception of cyberspace is highly contested. The U.S. Department of Defense (DoD) characterizes cyberspace as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processers and controllers."[7]

[6] There is significant disagreement about what activities the state is responsible for and what activities can be considered to be conducted by rogue or independent actors. A discussion of this issue of state responsibility, while important, will not be discussed in this thesis.

[7] United States, Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* JP 1-02 (Washington, D.C.: Defense Technical Information Center, 2016), 58.

While the DoD explicitly states the systems and infrastructure that compose cyberspace, the European Commission vaguely defines cyberspace as "the virtual space in which the electronic data of worldwide PCs circulate."[8] Despite this variation, almost all the prominent definitions of cyberspace agree that cyberspace includes both tangible and virtual elements and includes the transmission of information. This thesis proceeds with the definition purported by the DoD as it captures the key conceptual arguments of the definitional disagreements but still retains elements of specificity.

Like cyberspace, there are a wide variety of conceptions of "state" in international relations. Some scholars regard states as simply a structure of political rule over a territory while others specify explicit conditions that must be met for an entity to be regarded as a state (*e.g.*, recognized diplomatically by other states, stable population within its borders). This thesis takes a middle ground between these perspectives so as not to be overly restrictive in its definition but also not too broad so as to unnecessarily increase the number of actors being analyzed. Therefore, a state is defined as "a central authority with the ability to make and enforce laws, rules, and decisions within a specified territory."[9]

The following definitions are not plagued as much by disagreements. In line with the word's etymology of "without a leader," anarchy is defined here as "the absence of a central authority with the ability to make and enforce laws that bind all actors."[10] The widely-accepted definition of regime was put forth by Stephen Krasner: "Regimes can be defined as sets of implicit or

[8] EU Commission Information Society Website. Available at: http://ec.europa.eu/archives/ISPO/infocentre/glossary/i_glossary.html#c.
[9] Jeffry A. Frieden, David A. Lake, and Kenneth A. Schultz, *World Politics: Interests, Interactions, Institutions*, 2 edition (New York: W. W. Norton & Company, 2012), 63.
[10] Ibid., xxviii.

explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice."[11] The definition of cooperation in the IR literature has also become standardized and relatively undisputed. The scholars Robert Keohane, Kenneth Oye, Joseph Grieco and Peter Haas all define cooperation occurring "when actors adjust their behavior to the actual or anticipated preferences of others, through a process of policy coordination."[12]

Finally, while the United States makes a clear distinction between the terms "treaty" and "executive agreement," this thesis will treat treaties and international agreements synonymously. At a high level, William Slomanson has defined treaty as "a generic term covering all forms of international agreement in writing concluded between states."[13] While this definition captures the essence of international agreements, it is rather vague. Therefore the definition of treaty (also referred to in this thesis as international agreement) is extracted from the Vienna Convention on the Law of Treaties which has been ratified and signed by the majority of the major powers. That Convention defines a treaty as "an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation."[14] This definition still leaves room for flexibility about the exact nature of the agreement but is more specific about the common

[11] Stephen D. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," *International Organization* 36, no. 2 (1982): 186.
[12] Charles Lindblom, *The Intelligence of Democracy* (New York: Free Press, 1965), 227.
[13] William R. Slomanson, *Fundamental Perspectives on International Law* (St. Paul: West Pub., 1990), 351.
[14] Vienna Convention on the Law of Treaties, 1155 UNTS 311 (May 23, 1969), art. 2, s 1(a).

style of an international agreement. In the context of this thesis, international agreement is a level below ratification. The dependent variable, thus, is the existence or absence of written language regarding state behavior agreed upon at the executive level by two or more states.

Plan

The thesis proceeds as follows. The next chapter summarizes the argument and the most relevant lessons extracted from each case study. The third chapter synthesizes the existing literature on the prospects of an international agreement in cyberspace interwoven with the international relations literature on international cooperation. That chapter serves as the primary presentation of the contemporary cyberspace environment including the challenges and existing cooperative engagements. The fourth chapter presents the results from the analysis of the Reykjavik Summit. The fifth chapter analyzes the conditions that contributed to the success of CWC negotiations. Finally, the conclusion reviews the findings of this thesis and explains their implications for cyber policy in the United States and throughout the world.

Chapter 2 Roadmap to an International Agreement

There exists a wide variety of approaches to the study of international cooperation in cyberspace. This thesis employs a qualitative framework leveraged from the international relations literature on arms control and international cooperation. The chapter begins by explaining the source of the five variables that compose the core of the theoretical framework on which the analysis of this thesis rests. The chapter proceeds by summarizing the thesis's argument presented in the previous chapter. The four conditions most relevant to the successful outcome of an international agreement in cyberspace are discussed. Then, each of these four conditions and other elements of each of the five variables of this thesis - technology, geopolitical dynamics, state interests, domestic environments, and information - are developed in greater depth to provide a comprehensive overview of the findings derived from this thesis's analysis.

Variable Selection

The theoretical framework on which the analysis of this thesis rests is a grouping of five variables with explanatory value for the outcome of negotiations towards an international agreement. The dependent variable, therefore, is whether or not negotiations lead to an international agreement. These five variables were carefully chosen from a review of the international relations literature on international cooperation and arms control. They reflect common themes from the IR literature regardless of the author's theoretical basis. That is, despite a lens of realism, neorealism, liberalism, etc., discussion of these variables, with the exception of technology, informs the IR canon on international cooperation. The anomaly of technology is addressed in greater depth in the following paragraph, but given that the subject of this thesis is cyberspace, I would be remiss

not to emphasize technological characteristics of cyberspace that affect cooperation. There are certainly other variables contemplated in the IR literature, but that breadth has been paired down to the five that compose the framework of this thesis given an assessment of their anticipated relevance to negotiations in cyberspace.

Admittedly, there is limited IR theoretical work on the role of technology in international cooperation, but it would be a major oversight not to devote sufficient attention to technology when analyzing cyberspace. Cyberspace is, after all, a highly technical domain. Thomas Schelling and Morton Halperin and Robert Jervis among other IR scholars do address technology's influence on state behavior and strategic calculus but the role of the technology itself on the prospects of an agreement is insufficiently explored.[1] This dearth in the literature is likely largely a result of the technological revolution that the internet instigated where the technology that is to be regulated is much less tangible and more difficult to observe than nuclear weapons or space satellites, for example. Nonetheless, this thesis employs technology as its own variable given the technological characteristics of cyberspace.

Geopolitical dynamics is the second condition analyzed in this thesis's theoretical framework. International cooperation is intrinsically linked to the happenings of the international system and the distribution of power therein. In *Strategy and Arms Control*, one of the pioneer works on international cooperation, Schelling and Halperin allude to the difference in roles between major powers and challenging powers as well as the influence of the quantity and potency of power

[1] See Thomas Schelling and Morton Halperin, *Strategy and Arms Control* (New York: Twentieth Century Fund, 1961); Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167-214.

blocs.[2] The influence of the number of actors on arms controls is also carefully analyzed by Kenneth Oye in his renowned article "Explaining Cooperation under Anarchy: Hypotheses and Strategies." Oye's hypothesis is the prevailing one, asserting that an increase in the number of actors decreases the prospects of cooperation.[3] Questions about the influence of power asymmetries on international cooperation also informs much of the IR literature and indicates the importance of considering such elements of the international system when analyzing international cooperation.[4]

The third variable of analysis is state interests. Schelling and Halperin note that "The essential feature of arms control is the recognition of the common interest, of the possibility of reciprocation and cooperation even between potential enemies . . ."[5] This single citation alludes to two of the most important conclusions of this thesis related to the variable of state interests: the necessity of reciprocity and a collective interest in an agreement. In *Rational Theory of International Politics: The Logic of Competition and Cooperation,* Charles Glaser also emphasizes the importance of state interests. He identifies three sets of variables that he deems essential to the state's determination of the value of an agreement to them. Glaser's first variable, motives, captures what this thesis terms state interests.[6]

[2] Schelling and Halperin, *Strategy and Arms Control*, 50.
[3] Kenneth A. Oye, "Explaining Cooperation under Anarchy: Hypotheses and Strategies," *World Politics* 38, no. 01 (October 1985): 18.
[4] Helen Milner, "International Theories of Cooperation among Nations: Strengths and Weaknesses." *World Politics* 44, no. 3 (1992): 480.
[5] Schelling and Halperin, *Strategy and Arms Control*, 2.
[6] Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation,* (Princeton, NJ: Princeton University Press, 2010), 3.

Encapsulated in the variable of state interests, and alluded to by Schelling and Halperin, is the idea of reciprocity. Elizabeth Zoller contends that reciprocity "is a condition theoretically attached to every legal norm of international law."[7] According to Zoller, in an anarchic world, reciprocity is an essential condition for achieving cooperation. This position is also echoed by scholar Robert Axelrod who argues that "Under suitable conditions, cooperation based upon reciprocity can develop even between antagonists."[8] Similarly, Joseph Grieco asserts that a perceived equitable distribution of gains and losses through reciprocity contributes to the success of international cooperation.[9] Robert Keohane questions this emphasis on reciprocity in his article "Reciprocity in International Relations" by pointing out the different meanings of the word proffered by different scholars and the danger of the proliferation of use of the term.[10] He concludes that there are certain variants of reciprocity that promote, although not entirely on their own, cooperation, whereas other manifestations of reciprocity can actually be detrimental to cooperation.[11]

Keohane does, however, identify a conceptualization of reciprocity that is universal across different interpretations. This concept of reciprocity hinges on two phenomena - contingency and equivalence. Contingency indicates that a nation's actions are contingent on the actions of another entity. Equivalence suggests that the actions taken involve "at least rough equivalence of benefits."[12] This holds true even though in international relations it is especially difficult to precisely determine such equivalency. Thus, this thesis proceeds with a definition for reciprocity put forth

[7] Elizabeth Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Dobbs Ferry, N.Y.: Transnational, 1984), 15.
[8] Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984), 22.
[9] Joseph Grieco, *Cooperation among Nations* (Ithaca, N.Y.: Cornell University. Press, 1990), 47.
[10] Robert O. Keohane, "Reciprocity in International Relations," *International Organization* 40 (Winter 1986): 2-3.
[11] Ibid., 27.
[12] Ibid., 7.

by Keohane based on these two principles: "Reciprocity refers to exchanges of roughly equivalent values in which the actions of each party are contingent on the prior actions of the others in such a way that good is returned for good, and bad for bad."[13] On the whole, the growth of an emphasis on reciprocity in international relations and in instances of international cooperation elucidates the importance of evaluating reciprocity as a condition relevant to the outcome of international negotiations through the vantage point of state interests.

A more recent body of literature has emphasized the influence of domestic politics on state behavior in the international system. Increasing interdependence in the international system, John Ruggie argues, means that domestic political choices in one state no longer affect only that state but have ramifications beyond state borders.[14] In this context, according to Ruggie, the formation of international regimes is "a collective response to the collective situation of states."[15] The domestic environments of every state interact at an international level to determine international responses to collective problems. George Downs and David Rocke remark that domestic uncertainty about an executive's behavior or about the actions of democratic institutions also influences the international system, which in turn impacts instances of cooperation.[16] Additionally, James Fearon notes that between 1987 and 1996 more than one-third of the abstracts submitted to the leading IR journal, *International Organization*, made reference to domestic factors as relevant to an understanding of foreign policy decisions.[17] Demonstrably, domestic influences on state behavior in the

[13] Ibid., 8.
[14] John G. Ruggie, "International Responses to Technology: Concepts and Trends," *International Organization* 29 (Summer 1975): 565.
[15] Ibid., 574.
[16] George Downs, *Optimal Imperfection?: Domestic Uncertainty and Institutions in International Relations*, (Princeton, NJ: Princeton University Press, 1995), xiii.
[17] James Fearon, "Domestic Politics, Foreign Policy, and Theories of International Relations," *Annual Review of Political Science* 1, (1998): 290.

international system are regarded as important by IR scholars. Therefore, domestic environments cannot be excluded from an analysis of international cooperation.

Information, the final condition in the analytical framework, is a variable that is acknowledged by most IR scholars as an important determinant of the outcome of bargaining and negotiations. Conditions of insufficient information or asymmetric information are frequently cited as significant challenges to bargaining games.[18] States have incentives to withhold information and leverage private information to improve their negotiating position and the potential gains from an agreement.[19] Glaser also highlights information as one of his three sets of variables important to an assessment of international agreements.[20] He makes the case that a state's behavior in negotiations is at least partly dependent on information about motives and capabilities.[21] Particularly in the context of the cyberspace domain where secrecy and anonymity are indispensable, information and its influence on state behavior must be sufficiently examined.

With an understanding of the choice of the five variables that constitute this thesis, the following paragraphs further develop this thesis's argument in the context of these variables. As explained in the previous chapter, there are four conditions most conducive to international agreements in cyberspace. First, and most important, the negotiations should be characterized by elements of reciprocal concession. Secondly, the major players in cyberspace must be committed to arriving at an international agreement. Third, the proposed agreement should be tasked with defining acceptable and unacceptable uses of cyber weapons and not with regulating the possession

[18] See James Fearon, "Bargaining, Enforcement, and International Cooperation," *International Organization* 52, no. 2 (1998): 269-305; Oye, "Explaining Cooperation under Anarchy: Hypotheses and Strategies"; Robert Axelrod, *The Evolution of Cooperation*; James D. Morrow, "Modeling the Forms of International Cooperation: Distribution Versus Information." *International Organization* 48, no. 3 (1994): 387-423.
[19] Fearon, "Bargaining, Enforcement, and International Cooperation," 283.
[20] Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation,* 3.
[21] Ibid., 269.

of weapons themselves. Lastly, the opinions of private sector companies who would be influenced by a proposed agreement should be accounted for. The following sections expand upon these four conditions and also address other conditions derived from this thesis's analysis that have relevance, albeit limited, to the likelihood of an international agreement in cyberspace.

Technology

From a technological perspective, the negotiations for an international agreement in cyberspace will be most successful if they focus on the regulation of the use of cyber weapons rather than on the possession of weapons. The inherent dual-use nature of cyber tools, their dependence on stealth, and the difficulty of coming to a common definition as to what a cyber weapon is all argue for a regulation on use rather than a regulation on possession. An elaboration of these characteristics that lead to this conclusion is discussed in greater detail in the following chapters. Regardless, there is already some precedent for these discussions surrounding acceptable and unacceptable behavior at the UN Group of Governmental Experts (GGE) and other meetings on cyber norms.[22] The CWC provides a powerful example for this behavioral regulation of weapons as it sought to separate peaceful uses of chemicals from reprehensible uses, primarily distinguished based on intent in the form of the General Purpose Criterion (GPC). In doing so, the CWC successfully addressed the dual-use and high pace of technological development challenges of chemicals from which cyber negotiators could model their agreement.

Each case study informs the broader argument of this thesis, but only the lesson from the CWC case study helps to explain whether negotiations will be more likely to yield an agreement.

[22] See the 2015 UN GGE report that outlines four norms agreed upon by the convening body. United Nations, Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2014), available from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

The Reykjavik Summit teaches that the security dilemma arising from the technology can narrow the window of cooperation but need not nullify cooperation altogether. Therefore, one can expect that the security dilemma will influence negotiations but not be highly relevant to the outcome. As understood from the CWC case, a technological condition that does influence the outcome of negotiations is that the negotiations emphasize regulation of the use of the technology based on certain criteria, not the possession of weapons themselves. Such an approach addresses concerns about the multi-use nature of cyberspace and the high pace of development that cyber scholars argue will severely plague any attempts at international regulation.

Geopolitical Dynamics

With respect to geopolitical dynamics, there are two relevant considerations, neither of which is deterministic of the outcome of negotiations but each of which is influential nonetheless. The threat of proliferation and the number of actors party to the negotiations are the two such factors addressed here. The proliferation of cyber capabilities to non-state actors, conventionally weak nation states, and even private citizens has consequences for every nation state and shapes the conceptualization of the threat and what should be done about it. Similarly, the number of actors participating in talks and negotiations introduces a variety of perspectives that can potentially influence how the negotiations proceed. However, both of these considerations, while not insignificant, do not appear to dictate the success or failure of negotiations.

Proliferation of cyber capabilities to different actors has the potential to increase the urgency of nations to seek an international agreement to regulate the cyberspace domain. In the case of the CWC, proliferation concerns, illustrated by a weak actor like Iraq using CW, restructured the calculus of the major powers to deem it appropriate to relinquish their CW capability in order

to eliminate proliferation distress. Cyberspace is an especially asymmetric domain whereby nations that are conventionally weaker can execute a cyberattack against a strong state such as the U.S. with consequences that could not be achieved through other means. Therefore, internalization by the major powers in cyberspace that proliferation has the potential to restructure the dynamics between nations and establish a level of equivalency between weak developing nations and themselves could spark greater resolve to limit proliferation and its possible ramifications. Fear of proliferation may influence the posture of major powers in negotiations and shift the timeline of negotiations but it is not critically relevant to whether or not an international agreement is reached.

Another consideration within the scope of this variable is the number of actors party to the negotiations. An important element of cyberspace is the myriad of actors with a stake in the domain and how the domain is regulated. The differing outcomes of Reykjavik and the CWC negotiations mitigate fears that the sheer number of actors in cyberspace will limit the opportunities for cooperation. There were many actors party to the CWC negotiations, but in the end it was the U.S. and the Soviet Union that dictated the outcome and powered the negotiations. Regardless, despite the many opinions expressed at negotiations, a universally accepted outcome was reached. And at Reykjavik, with only two nations at the negotiations, an agreement to eliminate nuclear-armed ballistic missiles was not reached. Therefore, given an analysis of these particular case studies, it can be presumed that increasing the number of actors may complicate the negotiations but does not kill the prospects of an agreement entirely. However, this assessment is influenced by many other factors such as the commitment of states to an agreement and the relative involvement of the major powers, topics discussed in greater depth in the context of the two case studies.

State Interests

The variable of state interests, which encompasses two of the conditions within this thesis's argument, receives the most weight in determining the outcome of negotiations according to this thesis's analysis. Reciprocal concessions in particular are critical to the outcome of an agreement according to an analysis of the two case studies. In order to extract concessions from another party, a state must be willing to sacrifice some of its own capabilities, ambitions, or interests. At the Reykjavik Summit, there was a limit to how much each leader was willing to concede on its position on SDI, and a lack of reciprocity derailed the negotiations and the prospects for an agreement. On the other hand, during CWC negotiations the U.S. and USSR both conceded some of their positions with regards to verification and challenge inspections and the types of chemicals to be prohibited by the convention, namely riot control agents and herbicides. The concessions proved pivotal in widening the opportunities for cooperation and facilitating successful negotiations towards the CWC. Therefore, the independent variable of reciprocal concessions was a significant determinate of the dependent variable, an international agreement.

In addition to reciprocal concessions, the major players in cyberspace, specifically the United States, China, and Russia, must be committed to such an agreement and be willing to cooperate with each other to achieve the objective of an agreement. The Reykjavik Summit was conducted between the two major powers and the nations with near-monopolies on nuclear technology. Similarly, the CWC was largely influenced by the major powers with limited input from developing nations. Therefore, cooperation and elimination of hostility between the major powers in cyberspace is necessary. While this is a fairly obvious condition, the current cyberspace environment does not yet meet these criteria. In fact, the U.S. has sought a more normative approach to regulating behavior whereas Russia and China have advocated for a UN treaty. But while China has advocated for a UN treaty, it has rejected the claims that international law applies to cyber.

Therefore, there are still many disagreements that need to be addressed before the major players have cohesive interests in the pursuit of an international agreement.

Domestic Environments

There are two domestic impediments that determine a state's negotiating position and ability or willingness to compromise - the participation of the private sector and domestic politics. The fourth condition increasing the likelihood of an agreement is the inclusion of the opinions of the private sector during negotiations. Especially in cyberspace but also in the CW environment, the cooperation and participation of private sector companies who develop and own the technology that forms the basis of the weapons used by governments is valuable. The CWC negotiations illustrated the importance of allowing commercial chemical companies to express their viewpoints and have their opinions be addressed during negotiations - the private sector did not become a burden but was instead actively engaged in the pursuit of an international agreement.

At the time of the CWC negotiations, the chemical industry was suffering from reputational concerns as a result of the negative connotations of chemicals. In 1982, DuPont, a leading chemical company, even dropped the words "Through Chemistry" from its famous slogan to avoid the negative consequences of being so closely associated with the production of chemicals and to appear friendlier to public interests.[23] The chemical industry was also implicated in various uses of chemicals in war during the 1970s and 1980s, such as in Vietnam, that produced a reputation of "merchant of death" that the industry desired to break from.[24] These realities demonstrate the active

[23] Paul A. Offit, *Pandora's Lab: Seven Stories of Science Gone Wrong* (Washington, DC: National Geographic, 2016), 222.
[24] Karen Wiznowski, "Opting Out of the Iron Triangle: The US Chemical Industry and US Chemical Weapons Policy," The Nonproliferation Review 18, no. 2 (July 2011): 331.

interest by the chemical industry to support the CWC negotiations. This offers a lesson for negotiations in cyberspace where the voices of the private sector should be accounted for to strengthen the treaty and also increase the likelihood of nations determining it is in their best interest to reach agreement.

Domestic politics, a byproduct of a nation's regime type (*e.g.*, autocracy, democracy, aristocracy) also influences the likelihood of an agreement. The domestic challenges faced by the Soviets and the Americans at the time of Reykjavik were very different and functions of the pressures of an autocracy versus the pressures of a democracy. A crippled economy, a devastating nuclear accident, and political barriers faced by Gorbachev heavily shaped the Soviet position and bottom-line at Reykjavik whereas President Ronald Reagan was more concerned about the support from his political base. Domestic political pressures were much less prevalent in CWC negotiations. Regardless, regime type has great relevance to the proceedings of negotiations and is even more germane to negotiations relating to cyberspace. Regime type is a function of national experiences that shape strategic interests and state behavior; interests and behavior in turn contribute to a state's negotiating posture and therefore the prospects of an agreement. As such, the domestic pressures derived from regime type are relevant to the outcome of negotiations towards an agreement in cyberspace.

Information

There are two lessons extracted from the case studies with regards to the information variable. Neither of the two lessons is included in the four conditions listed above because while both are important to cyberspace and negotiations for an international agreement in the domain, neither one is a strong explanatory variables of the outcome of international agreements. Verification and enforcement and the ability for negotiations to generate information are the two lessons discussed.

Verification is a commonly cited barrier to an international agreement in cyberspace and an aspect of most discussions of international cooperation. The CWC provides precedent for the development of a highly intrusive verification scheme agreed to by the majority of nations to regulate a dual-use and highly secretive technology. On the other hand, The Biological and Toxin Weapons Convention (BTWC) and the Geneva Conventions, which seek to regulate behavior in armed conflict and protect innocent civilians, demonstrate that agreements lacking verification can still serve to influence state behavior and guide the international community through the codification of customary international law and revised incentives.

Verification is excluded from the core of this thesis's argument not only because of the precedent created by the BTWC and Geneva Conventions but also because cyber agreements, specifically ones predicated on the regulation of use, are inherently not verifiable.[25] You cannot verify that someone is not going to use something, so the negotiations should proceed without an insistence on a resolution of the verification question. These agreements, nonetheless, still have merit by creating international norms around use and even potentially acting as a deterrent against use. Therefore, verification may not be a relevant condition contributing to the outcome of negotiations towards an international agreement in cyberspace and is not at the center of the analysis.

Additionally, the Reykjavik Summit is an excellent example of a negotiation that itself did not produce a concrete outcome but paved the way for success in the future, namely the Strategic Arms Reduction Treaty (START) and the Intermediate-Range Nuclear Forces Treaty (INF). The outcomes generated by the Reykjavik Summit illustrate the power of negotiations to generate information that facilitates future cooperation. Therefore, an international agreement in cyberspace

[25] Herbert S. Lin, "Arms Control in Cyberspace: Challenges and Opportunities," World Politics Review (March 05, 2012). https://www.worldpoliticsreview.com/articles/11683/arms-control-in-cyberspace-challenges-and-opportunities.

is probably more likely the more time that nations spend negotiating and debating the challenges of regulation in cyberspace. However, this reality is more an intrinsic feature of negotiations than the result of actions taken or decisions made by states. Therefore, like verification, this condition is important to acknowledge but likely would not play an important role in determining the outcome of negotiations towards an international agreement in cyberspace.

Summary

The goal of this chapter has been to explicate the choice of the five variables that compose this thesis's analytical framework and summarize the key elements of this thesis's argument. The following chapters present the support for the proposed conclusions, surveying the historical record of the Reykjavik Summit and the CWC negotiations as well as the contemporary cyberspace environment. The table of variables illustrated at the end of this chapter serves as context for visualization and conceptualization of how the next three chapters interact with and build upon each other. It documents the environment during the negotiations for the two case studies and the anticipated environment during future negotiations for an international agreement in cyberspace.

The next chapter will present what has already been said about international agreements in cyberspace and illustrates how the argument presented in this chapter differs from the existing literature. Further, it is one of the first attempts to reconcile the arguments purported by cyber scholars with the international relations theoretical literature on international cooperation.

	Reykjavik 1986	CWC 1992	Future Agreement on Cyberspace
Technology			
• Offense/Defense Implications	• Offense dominates defense • Differentiation is hard	• No dominance by offense or defense • Differentiation is easy	• Disagreement as to whether offense dominates defense • Differentiation is very hard
• Pace of technological development	• Slow pace of development	• Fast pace of development	• Extremely fast pace of development
• Dual-use nature of the technology	• Very limited civilian uses of nuclear technology	• Many civilian uses of chemicals	• Extensive civilian uses of cyber technology
Geopolitical Dynamics			
• Power distribution	• Superpowers dominant	• Superpowers dominant	• Superpowers dominant and most vulnerable
• Proliferation	• Limited concerns about proliferation	• Concerns about proliferation	• Strong concerns about proliferation
• Number of actors	• Two nation-states	• Many nation states, terrorist organizations, chemical industry	• Many nation states, terrorist organizations, corporations, private citizens
State Interests			
• Alignment of interests	• Some agreement and some disagreements	• Strong agreement	• Significant, intrinsic disagreements
• Reciprocity	• Soviets concessions, no U.S. concessions	• Soviet, U.S. and developing nation concessions	• Russian, Chinese and U.S. concessions

	Reykjavik 1986	CWC 1992	Future Agreement on Cyberspace
Domestic Environments			
• Domestic politics	• Political pressures from regime type	• Limited political pressures from regime type	• Significant political pressures from regime type
• Private Sector Relevance	• Very limited private sector influence	• Extensive private sector influence	• Extensive private sector influence
Information			
• Verification/Enforcement	• High visibility of weapons capabilities • Verification/enforcement not central	• Relatively low visibility of weapons capabilities • Verification/enforcement fundamentally central	• Extremely low visibility of weapons capabilities • Verification/enforcement not very central
• Negotiations as generators of information	• Negotiations revealed previously private information	• Negotiations revealed the strength of the taboo against CW	• Negotiations could reveal shared norms or principles

Table 1: Lessons from Case Studies and Cyberspace According to Five Variables

Chapter 3 The Perils of Cooperation in Cyberspace: A Review of the Literature on Arms Control in Cyberspace and International Relations Theory

At its core, the study of cyber arms control is a study of cooperation among multiple states in an anarchic world - a collective action problem.[1] It is an analysis of how nations with potentially competing interests engage with each other without the oversight or organizing mechanisms of a governing body. Anarchy presupposes that their does not exist a higher authority which governs state behavior. Therefore, states must take the initiative to engage in dialogue and work with other nations to collectively achieve their national goals.

It is imperative to first understand what might bring states to such negotiations and subsequently what factors contribute to the success or failure of the negotiations. The exploration of these questions has been insufficiently analyzed in the cyber arms control literature. Fortunately, the IR literature on why states cooperate under a system of anarchy is extensive. Scholars have long been puzzled by states ceding sovereignty or sacrificing vital interests or some freedoms to achieve mutual gain by cooperating with other states. However, despite the breadth of literature that addresses the fundamental question of why states ever cooperate, there is no widely held view as to the conditions that are the most conducive to cooperation. This chapter details the predomi-

[1] The concept of collective action problems was popularized by Mancur Olson. Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with New Preface and Appendix*, Revised edition (Cambridge, Mass.: Harvard University Press, 1971).

nant views about international cooperation in cyberspace in dialogue with the IR literature on international cooperation to better understand the conditions that will make international agreements in cyberspace more likely.

Setting the Stage

The literature on cyber arms control is extensive. Nearly every scholar believes that some level of international cooperation in cyberspace is desirable, but there is significant disagreement about what form the cooperation should take and whether cooperation is feasible in practice. Herbert Lin, for example, observes "unilateral defensive measures alone cannot solve the cybersecurity problem," as a result, "nations would benefit from other mechanisms to reduce incoming threats."[2] Likewise, James Lewis recognizes that "The secure use of cyberspace has become a vital national interest of all states."[3] Thus, international cooperation is neither purely a fantasy nor highly speculative. Rather, there is interest in and there are incentives for international cooperation but not a clear vision for how and under what conditions such cooperation will transpire.

Scholars generally advance one of two common paradigms about the feasibility of arms control in cyberspace. The first is characterized by significant pessimism about the prospects of an international agreement given various characteristics of the contemporary cyberspace environment. Jack Goldsmith is the most vocal and adamant in asserting that the challenges to international cooperation in cyberspace are currently insurmountable. According to Goldsmith, a non-alignment of state interests, the magnitude of the concessions the U.S. would have to present, and the inability to achieve an effective verification scheme severely plague international cooperation.[4]

[2] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."
[3] James A. Lewis, "Confidence-Building and International Agreement in Cybersecurity," in *Disarmament Forum*, vol. 4 (2011): 51. https://citizenlab.org/cybernorms2012/Lewis2011.pdf.Lewis.
[4] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View," Hoover Institution, March 9, 2011, http://www.hoover.org/research/cybersecurity-treaties-skeptical-view.

The second common paradigm in the cyber arms control literature is that there are certain circumstances under which cooperation is plausible. The type of circumstances are numerous but could entail negotiations that emphasize very clearly defined issue areas or do not hinge on devising an effective scheme to verify the provisions of an agreement. Lin, Joseph Nye, Abraham Sofaer, David Clark, and Whitfield Diffie constitute the leading scholars who profess that the prospects of international cooperation in cyberspace are not as dire as Goldsmith makes them out to be. That is to say that these scholars do not state that a comprehensive international treaty that covers all disagreement in and components of cyberspace is feasible. Instead, in response to the question "Could arms control work in cyberspace?" Lin acknowledges "The answer to that question is different for different aspects of arms control and not generally definitive."[5] Similarly, Nye notes that "It is unlikely there will be a single overarching regime for cyberspace . . . Different sub-issues are likely to develop at different rates."[6] Therefore, a more reasonable approach to international cooperation, according to these scholars, is to partition avenues of cooperation into manageable pieces.

Collectively, these scholars acknowledge the benefits of international cooperation in cyberspace but approach the question of the feasibility of such cooperation with varying degrees of skepticism. Yet regardless of their conclusions, each scholar references at least one of the five explanatory variables introduced above. Therefore, in putting aside the author's conclusion, this

[5] Herbert Lin, "A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity," *Bulletin of the Atomic Scientists* 68, no. 5 (March 2012): 82.
[6] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance Paper Series, Paper No. 1. (2014): 15.

thesis emphasizes the enablers and impediments to international agreements in cyberspace by situating these variables within the international relations theoretical literature on international cooperation.

This chapter seeks to contextualize the contemporary cyberspace environment according to the five variables explained in the previous chapter. First, this chapter reveals the technological barriers to international agreements in cyberspace, namely the dual-use nature and high pace of development of the technology, and the scholarly emphasis on the uniqueness of the cyberspace domain. Next, the complexity of the untraditional geopolitical dynamics spawned by cyberspace and the large quantity of actors in the space are described. Then, this chapter illuminates the fundamental conflicts in state interests that many scholars recognize as a primary hurdle that is necessary to overcome in order to achieve an international agreement. The ensuing section highlights the role that domestic politics and the private sector play in cyberspace. Finally, the chapter concludes by underscoring the emphasis that cyber scholars have placed on verification and enforcement.

Technology

In the international relations literature, there is not a strong emphasis on the role the applicable technology plays in international cooperation. Instead, the interesting theoretical questions pertain to state dynamics and why nations cooperate with and trust each other, irrespective of what they are negotiating about. This significant gap in the literature is notable, especially when seeking to apply the theoretical framework to cyberspace - a domain that is notable chiefly for the peculiarity of the technology.

Still, two scholars address the role of technology in international cooperation. Robert Jervis focuses on the offensive and defensive characteristics of the weapon, whereas April Carter emphasizes the weapon's destructiveness and the pace of development.[7] Carter also argues that technological features can both impede and promote international cooperation.[8] While both authors provide convincing arguments for the role of technology in international cooperation, neither author's position is sufficient by itself to understand under what conditions technology will promote or impede cooperation.

Contrastingly, the nature of the technology that underlies cyberspace informs all varieties of literature on cyber arms control. The majority of scholars either implicitly or explicitly categorize cyber as a unique domain that cannot be understood or governed using traditional methods such as deterrence, which functions to encourage an opponent not to act. Gregory Koblentz and Brian Mazanec identify the multi-use nature of cyber, the possibility of anonymity, the attractiveness of the technology as an asymmetric weapon, the importance of secrecy and surprise, and the unpredictability of the technology.[9] Lin elaborates on this notion of secrecy and surprise by stating that "offensive cyber operations fundamentally depend on stealth and deception."[10] More tangibly, Nye explains that "Cyberspace is a unique combination of physical and virtual properties."[11]

The logical implication of these statements is that traditional understandings of defense and cooperation are not automatically relevant or readily applicable to cyberspace. This thesis

[7] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167-214.
[8] April Carter and Stockholm International Peace Research Institute. *Success and Failure in Arms Control Negotiations* (Oxford, UK: Oxford University Press, 1989), 23.
[9] Gregory D. Koblentz and Brian M. Mazanec, "Viral Warfare: The Security Implications of Cyber and Biological Weapons," *Comparative Strategy* 32, no. 5 (November 1, 2013): 418–34.
[10] Lin, "A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity," 85.
[11] Nye, "The Regime Complex for Managing Global Cyber Activities," 1.

seeks to challenge that notion by identifying historical lessons that can presumably be applied to cyberspace.

The pace of technological development is also acknowledged as a primary impediment to international cooperation. Given the fast-paced nature of technological development that constantly changes the employment of cyber offensively or defensively, regulations must be able to keep pace with this development.[12] Otherwise, international agreements in cyberspace will become inoperative almost instantly. Louise Arimatsu claims that "The speed at which technology is evolving means that the methods and tools of attack are constantly altering making any listing of prohibited cyber-weapons simply redundant."[13] Similarly, Nye notes "the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target."[14] Carter recognizes this impediment in an analysis that is not limited to cyber by noting that modifications of technology can nullify agreements.[15] It is certainly plausible that an agreement in cyberspace would not be able to morph with the fast pace of technological development in the domain.

If the pace of technological development is too fast for law enforcement and international regulation to keep up, then perhaps the conversation should be reoriented, as Arimatsu suggests, to focus on regulating the use of weapons rather than the technology itself. There is already some

[12] Scott J. Shackelford and Andraz Kastelic, "Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity," *NYUJ Legis. & Pub. Pol'y* 18 (2015): 895.
[13] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in *Cyber Conflict (CYCON), 2012 4th International Conference On* (IEEE, 2012): 10.
[14] Nye, "The Regime Complex for Managing Global Cyber Activities," 2.
[15] Carter and Stockholm International Peace Research Institute, *Success and Failure in Arms Control Negotiations*, 23.

acknowledgement of this reality in the discussions at the UN GGE where nations agreed, for example, upon norms that identify targets that are off limits.[16] A manifestation of a regulation on use instead of on a technology is illustrated in the CWC case study.

Beyond the inherent characteristics of the technology, there also exist influences from the security dilemma that arise from the technology. The security dilemma explains the phenomenon whereby a state takes actions to increase its own security and power but in doing so decreases the security and power of other states. This forces the others states to respond and could theoretically have devastating consequences, including by inciting an arms race that is politically and economically burdensome. A key feature of the technology that is also a function of its reliance on stealth and deception is the difficulty in differentiating between offensive and defensive operations - the first component of the security dilemma. According to Lin, "in cyberspace, intent may be the primary difference between a possibly prohibited act . . . and an allowed one."[17] To gauge intent, if at all possible, would require significant resources and an understanding of the perpetrator through attribution.[18]

Arimatsu likewise discusses the difficulty in differentiating between offense and defense. A cyber weapon, claims Arimatsu, is deemed a weapon not only by its intrinsic technological properties but also by the intended outcome it produces. She argues that "Since the same 'cyber-weapon' deployed in a different manner may result in an effect that is simply disruptive, regulating the use of the weapon, rather than the weapon per se may present a more viable option."[19]

---

[16] See United Nations, Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.
[17] Lin, "A Virtual Necessity," 84.
[18] Attribution seeks to answer the question "who is responsible?" For a detailed discussion of attribution, see Herbert S. Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," Journal of International Affairs (Winter 2016).
[19] Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," 8.

Arimatsu's argument echoes that of Jervis who acknowledges that the determination of whether a weapon is offensive or defensive is highly situational. Jervis concludes that "the most propitious conditions for regime formation, then, are the cases in which offensive and defensive weapons and policies are distinguishable but the former are cheaper and more effective than the latter, or in which they cannot be told apart but it is easier to defend than attack."[20] However, Jervis's emphasis on territorial expansion in order to reach this conclusion has limited applicability to cyberspace. Nevertheless, Jervis's work on the security dilemma helps to situate the reality of cyberspace in the context of IR theory conveyed by a widely-respected scholar.

The second element of the security dilemma described by Jervis, the offense-defense balance, is also relevant to cyberspace. Until very recently, the consensus has been that cyberspace is a domain where the offense has an advantage over the defense. This consensus implies that cyber fits into the "doubly dangerous" category, as illustrated in Figure 1, that Jervis presents and is the world which is the most unstable and the least conducive to cooperation.

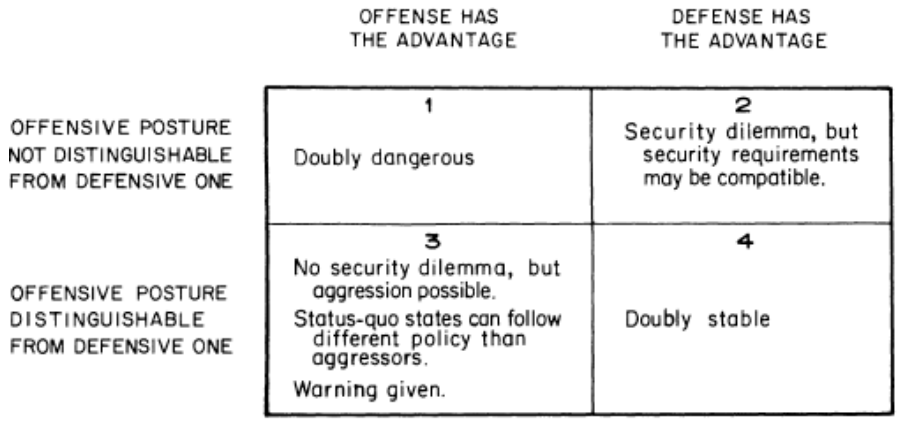

Figure 1. Robert Jervis's Four Worlds of Offense/Defense

[20] Robert Jervis, "Security Regimes," *International Organization* 36, no. 2 (1982): 362.

Rebecca Slayton disputes this general assumption of offense dominance in her article *What is the Cyber Offense-Defense Balance?* She argues that there is a critical failure in the discourse about the offense-defense balance because it does not account for organizational behavior.[21] If technology and behavior are assessed in kind, Slayton presents a convincing argument that the offense is more handicapped by organizations, advantaging the defense. Slayton's argument, however, does not sufficiently acknowledge that different organizations have different priorities and varying degrees of flexibility in structure that lead their offensive capabilities to be unequally burdened by organization.

Regardless, in assuming Slayton's perspective of slight defense dominance, Jervis's categorization implies that the security dilemma still exists but that there is room for security restrictions (see Figure 1). The challenge of differentiating between offensive and defensive uses of the technology ensures that regardless of the results of the offense-defense balance, the security dilemma endures. In bringing new life into the debate, Slayton illustrates that an assessment of the offense-defense balance is not as simple as scholars believed it to be. But no matter which perspective is taken, offense dominance or defense dominance, the security dilemma still exists and can influence negotiations.

Despite the conclusions about the offense-defense balance in cyberspace, Jervis's analysis has shortcomings when applied to the context of cyber. First, Jervis's argument assumes that states can effectively predict the length and frequency of conflict and quickly react to the changing status of the opponent's level of arms. In cyber, both of these assumptions are incorrect. Cyber is a highly secretive domain, making it very difficult to predict and assess another state's capabilities without

[21] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," International Security, Vol. 41, No. 3 (2017): 82.

engaging in cyber operations (i.e. cyber espionage). A main reason why the domain is so secretive is because cyber weapons are primarily single use weapons, so states must either use the weapon themselves or become the victim of the weapon by an adversary without the possibility of reusing the weapon in the future.

Further, it is incredibly difficult to accurately predict exactly how an offensive cyber weapon will operate upon execution. Taking Stuxnet as a clear example, the perpetrators of the Stuxnet worm sought the Iran nuclear reactors as their target. However, the worm continued to promulgate beyond its intended target, an evolution unbeknownst to the attackers until the moment it happened.[22] This example illustrates that many of the assumptions upon which Jervis's statements about the implications of offense having the advantage during war are based may not easily be translated to cyberspace. There is, however, still great value in analyzing cyberspace through the lens of Jervis's security dilemma paradigm to extract important areas of analysis and lingering questions.

Geopolitical dynamics

In addition to characteristics of the technology, the geopolitics of the international system have the potential to influence the probability of cooperation. Technological interdependence, which feeds geopolitical interdependence, is one of the phenomena in the scope of this variable that is important to understand. The existence of interdependence however is, for the most part, relevant only to cyberspace as nations at the time of the Reykjavik and CWC negotiations operated relatively autonomously in the international system and with their weapons programs. Interdependence is, nonetheless, explored in this section because of its importance to understanding the

[22] See Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2014).

contemporary cyberspace domain. This section also stresses the uniqueness of the power dynamics generated by cyberspace and the influence of the number of actors in cyberspace on the prospects of an international agreement.

In the IR literature, Robert Keohane contends that geopolitical interdependence has created more potential for friction and helps to explain an increased prevalence of discord relative to cooperation.[23] Conversely, Thomas Bernauer argues that interdependence has led to greater cooperation.[24] Similarly, Ernst Haas and Donald Puchula and Raymond Hopkins argue that interconnectedness is highly correlated with cooperation. Haas notes that a primary motivation for regimes is to resolve complicated issues that cannot be resolved unilaterally. And, the quantity and frequency of complications that arise that are not conducive to unilateral action increases with interconnectedness.[25] Puchula and Hopkins "maintain that regimes are more likely to arise under conditions of complex interdependence."[26] Even though the same variable, interdependence, is employed by different scholars in different ways to explain cooperation, or its absence, its prevalence in the literature underscores its importance to the analysis.

While interdependence is rarely explicitly mentioned by scholars of cyber arms control, interdependence by way of connectivity in particular is a key feature of cyberspace. As the definition of cyberspace suggests, the domain is composed of a set of interconnected systems. The complexity and interwoven nature of cyberspace creates an environment in which data is routed through various destinations that are not necessarily constrained to one state. An email one sends

[23] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton University Press, 1984), http://www.jstor.org/stable/j.ctt7sq9s.
[24] Thomas Bernauer, *The Chemistry of Regime Formation: Explaining International Cooperation for a Comprehensive Ban on Chemical Weapons* (Ashgate Publishing Company, 1993).
[25] Ernst B. Haas, "Words Can Hurt You; Or, Who Said What to Whom about Regimes," *International Organization* 36, no. 2 (1982): 207–43.
[26] Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," 196.

could potentially pass through multiple routers in multiple states before arriving at its final destination. Inherent in how the technology works is a high level of connectivity, with very few systems within cyberspace being isolated from others. Connectivity then feeds geopolitical interdependence because of the coordination necessary to ensure unfettered access to these interconnected systems.

Beyond interdependence, scholars of cyber arms control also note the uniqueness of power dynamics and the interaction between states in the international system as a result of unprecedented characteristics of cyberspace. James Forsyth, however, contends that the problems posed by cyberspace are nothing new. Forsyth argues that cyberspace is, and will be, what great powers make it, implying that any international agreement or international regime generated will be reflective of geopolitics and the interests of the great powers.[27]

However, Forsyth's argument assumes that great powers have a sufficient monopoly on the operations in cyberspace under its authority. This assumption logically flows from the history of arms control agreements that have presumed a state monopoly on the arms being regulated. Yet, Lin acknowledges that this is not necessarily the reality. He writes that the proliferation of actors and easy accessibility to the technology used in cyberspace runs counter to this historical record.[28]

Additionally, Matthew Waxman emphasizes the changing nature of power in cyberspace that may influence the prospects of an international agreement. He writes that "The distribution of emerging cyber-capabilities and vulnerabilities . . . is unlikely to correspond to the status quo

[27] James W. Forsyth Jr, "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace" (AIR UNIV MAXWELL AFB AL SCHOOL OF ADVANCED AIR AND SPACE STUDIES, 2013), http://www.dtic.mil/docs/citations/ADA595562. 94.
[28] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."

distribution of power built on traditional measures like military and economic might."[29] Conventional understandings of power and the distribution of power according to tangible metrics are not so easily applied to cyberspace where traditionally weak states can exact a disproportionate impact on powerful states. Iran, for example, does not have the military capability to directly challenge the United States through conventional means. But, it can exploit vulnerabilities in United States infrastructure to send a message and theoretically induce damage.[30] There is very little in the international relations literature that helps to situate Waxman's argument in theory.

IR and cyber scholarship also note the influence of the number of actors on the prospects of international cooperation. Bernauer and Dieter Ruloff and Kenneth Oye discuss this factor but surprisingly do not contend that the increase in the number of actors necessarily prohibits cooperation.[31] However, there is significant discussion around how to counter the detrimental force of an increased number of actors to still achieve cooperation.[32] The majority of the analysis done by these scholars assumes unitary actors. Yet, cyberspace is a multi-stakeholder domain wherein many individuals and groups within each state have a vested interest in the outcome of international cooperation. Nye, among other scholars of cyber, notes that the quantity and diversity of actors in cyberspace can further complicate international cooperation.[33] Nye does not assess the optimal conditions for the number and diversity of actors conducive to successful international

[29] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)," *Yale Journal of International Law* 36 (2011): 450.
[30] Danny Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," *Wall Street Journal*, December 21, 2015, sec. US, http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559.
[31] See Thomas Bernauer and Dieter Ruloff, *The Politics of Positive Incentives in Arms Control* (Univ of South Carolina Press, 1999); and Oye, "Explaining Cooperation under Anarchy: Hypotheses and Strategies."
[32] See Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy;* John Conybeare "International Organization and the Theory of Property Rights," *International Organization* 34 (1980), 307–34; and Kenneth Akito Oye, *Bargaining, Belief Systems, and Breakdown: International Political Economy, 1929-1936* (Harvard University, 1983).
[33] Nye, "The Regime Complex for Managing Global Cyber Activities," 9.

cooperation nor does he leverage the arguments presented by Bernauer and Ruloff or Nye to supplement his analysis. Nonetheless, the number and diversity of actors certainly presents a logistical burden to negotiations and also widens the possible number of competing interests.

State Interests

State interests function both to embolden states to pursue cooperative measures and to constrain the chances of cooperation. The predominant scholarship that emphasizes the role of state interests in determining the outcome of international cooperation is advanced by realist theorists.[34] Realists espouse the theory that power is the primary explanation for state behavior as states act in their own self-interest to achieve their goals. Hans Morgenthau, considered one of the leading realist theorists, has written that states "are always anxious to shake off the restraining influence that international law might have upon their foreign policies, to use international law instead for the promotion of their national interests."[35] Similarly, realists argue that legal obligations and other multilateral constraints actually have little import on a state's behavior. However, realist theory fails to fully account for the empirics of significant international cooperation on issues of mutual concern in the contemporary international system. Realists do acknowledge that states have and do tie their own hands by adhering to the principles of international regimes in some circumstances. But, the post-World War II international system has witnessed a systematic increase in international negotiations and a desire for international agreements to regulate matters in a vast range of issue-areas.

Keohane and Joseph Nye, Beth Simmons, and Arthur Stein advance arguments in the vein of the contention that international cooperation surfaces when states seek to address issues that are

[34] The prominent realist theorists are John Mearsheimer, Kenneth Waltz, and Stephen Walt.
[35] Hans J. Morgenthau, Kenneth W. Thompson, and David Clinton, *Politics Among Nations*, 7 edition (Boston: McGraw-Hill Education, 2005), 259.

very much in their self-interest but that they cannot address unilaterally. Keohane and Nye argue that international regimes are reflections of state interests rather than a replacement of those fundamental interests.[36] Simmons writes that "governments are more prone to make agreements that comport with the kinds of activities they were willing to engage in anyway, and from which they foresee little incentive to defect."[37] Finally, Stein acknowledges that "there are times when rational self-interested calculation leads actors to abandon independent decision making in favor of joint decision making."[38] These authors indicate that international cooperation, at least in certain circumstances, is actually in the self-interest of nations.

However, joint decision making is predicated on the existence of shared interests that are favorable for international cooperation. The fundamental disconnect in interests and perceptions among states is regularly cited as a critical barrier to international cooperation in cyberspace. In cyber, the most prominent argument purported by scholars that supposedly diminishes the prospects of international cooperation is that state interests conflict despite the commercial benefits of a free and open internet. The common assessment is that this conflict of interest is arduous to overcome and is the first and most important barrier to surpass on the way to international cooperation. Therefore, a reconciliation of state interests is arguably the decisive condition for cooperation when cyberspace is considered in isolation.

The discord resulting from conflicting state interests primarily pertains to disagreements over what should be regulated rather than how the domain should be regulated. Situated at the core

[36] Robert O. Keohane and Joseph S. Nye, "Two Cheers for Multilateralism," *Foreign Policy*, no. 60 (1985): 152.
[37] Beth A. Simmons, "Compliance with International Agreements." *Annual Review of Political Science* 1, no. 1 (1998): 89.
[38] Arthur A. Stein, "Coordination and Collaboration: Regimes in an Anarchic World," *International Organization* 36, no. 2 (1982): 316.

of Goldsmith's argument is an acknowledgement of definitional issues of two varieties that severely weaken the outcome of cooperation or fully destroy the prospects of cooperation itself. The two varieties of definitional challenges that Goldsmith addresses relate to "the nature of the activity itself" and "the matter to be regulated."[39]

Given the multiuse nature of cyber capabilities and despite many occurrences of negotiations among the most capable states in cyberspace, the states have failed to come to agreement on definitions in these two categories. Goldsmith attributes this failure to the secrecy around offensive weapons and "the fundamental clash of interests."[40] Lin, while belonging to the other group of scholars who argue that international cooperation is situational, also recognizes the critical disagreements that arise. Lin argues that "it surely behooves all nations concerned with the problems of international cyber conflict to find a common ground of understanding and a common language with which to describe the issues."[41] Additionally, Arimatsu stresses that definitional disagreements are a reason to sign an agreement as much as they function as a barrier to agreements.[42]

The disagreements and conflicting interests that exist among the major powers are serious and intrinsic. With respect to how to proceed with the regulation of cyberspace, the Russians and Chinese advocate enhanced international cooperation and the establishment of a code of conduct to democratically govern the domain.[43] The Western nations have instead concluded that international law as it is written today does apply to cyberspace and the first attempts at regulation should

[39] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 6.
[40] Ibid., 7.
[41] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."
[42] Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," 18-19.
[43] James A. Lewis, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms," *Strategic Technologies Program,* Center for Strategic and International Studies (February 2014): 6.

be normative in nature.[44] As a result, the UN GGE, convened to discuss issues of information technology, agreed upon norms largely developed by the U.S.[45] Yet, beyond producing a consensus report on norms of behavior that reflect common interests, little progress has been made to guide state behavior more broadly in cyberspace.

Apart from disagreements about the way forward in cyberspace, Western nations and non-Western nations have taken distinctly different approaches towards conceptualizing cyberspace and assessing what should be protected. These different approaches are in part because the survival of authoritarian leaders and closed regimes is threatened by societal openness and the exchange of information in a way that democratic regimes are not.[46]

Given the interests of authoritarian regimes, Russia and China advocate for what they term "information security" -- the protection of information and information systems from threats to individuals, society and nations. These nations are concerned with the internet's ability to jeopardize their political survival and the stability of their nation.[47] The Chinese in particular articulate this fear in their national strategy on securing cyberspace by noting the necessity to prevent the use of information technology to incite rebellion or an overthrow of the government for the sake of national security.[48]

---

[44] Ibid., 14.
[45] Henry Rõigas and Tomáš Minárik, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," NATO Cooperative Cyber Defence Centre of Excellence, 31 August 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.
[46] Lewis, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms," 7.
[47] International Code of Conduct for Information Security, transmitted by "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," UN Doc. A/69/723, January 13, 2015.
[48] A goal of information security strategies is to "Prevent, curb and lawfully punish any act of using the network to engage in treason, separatism, incite rebellion or subversion, or incite the overthrow of the people's democratic dictatorship regime; prevent, curb and lawfully punish acts of using the network to steal or leak State secrets and other such

The Americans, Europeans and their allies, on the other hand, promote "cybersecurity" which separates the society and technology.[49] Cybersecurity emphasizes solely the regulation of technology, allowing for information, including speech, which may offer opposing views to their regimes. These nations staunchly defend democratic values and view a free and open internet instrumental to that end. For example, the United Kingdom denounces the use of the term "information security," "since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed to in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[50]

Another element of the disagreement between the Western nations and the non-Western allies, to include Russia and China, pertains to the concept of sovereignty. The Russians advocate the protection of the "information sovereignty of the Russian Federation."[51] Similarly, the Chinese stress that "no infringement of sovereignty in cyberspace will be tolerated, the rights of all countries to independently choose their development path, network management method and Internet public policy, as well as to equally participate in international cyberspace governance will be respected."[52]

---

acts harming national security; prevent, curb and lawfully punish foreign powers using the network to conduct infiltration, destruction, subversion and separatist activities." *National Cybersecurity Strategy*, released by the Cyberspace Administration of China on December 27, 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

[49] Lewis, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms," 2.

[50] United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General," U.N. Doc. A/68/156 (2013), 15. https://undocs.org/A/68/156.

[51] Doctrine of Information Security of the Russian Federation, approved by the President of the Russian Federation Vladimir Putin on December 5, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

[52] *National Cybersecurity Strategy.*

The U.S. and Western nations have countered this position, contending that it authorizes nations to "undermine human rights and the free flow of information but also the interoperability of the network."[53] Unless the nations can agree on an understanding of what is sovereign, they likely may not be able to agree on what should be protected and how. As a result, many scholars conclude that there is not a basis for nations to come to an agreement at the moment.[54]

In this context of intrinsic disagreements about the regulation of cyberspace, Sofaer et al. contend that "international agreements will . . . be impossible where irreconcilable differences in policies exist among states."[55] Yet, unlike Goldsmith, these authors do not view this challenge as preventing all forms of cooperation. Instead, they optimistically assert, "while these factors limit the potential scope and utility of international cyber-security agreements, they do allow for international cooperation on many issues that could prove beneficial."[56] Therefore, differences in state interests are not existential threats to international cooperation in cyberspace as Goldsmith would maintain. Sofaer et al. and Lewis argue that it is unreasonable to assume that the states will come to agreement on all conflicting definitions.[57] But, there is still space for cooperation on the matters where definitional challenges do not exist or can be overcome through increased communication and negotiation.

Under conditions where state interests are not aligned, the international relations literature cites the principle of reciprocity as a way to propel states to reach an international agreement.

---

[53] Hillary Rodham Clinton, "Remarks." Conference on Internet Freedom, The Hague, Netherlands, December 8, 2011.
[54] See Goldsmith, "Cybersecurity Treaties: A Skeptical View"; Sean Kanuck, "Deterrence and Arms Control in Cyberspace." The Berkman Klein Center for Internet & Society, March 30, 2016; and Chelsea Slack, "Wired yet Disconnected: The Governance of International Cyber Relations," *Global Policy* 7, no. 1 (2016): 69-78.
[55] Abraham Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in National Research Council, Proceedings of a Workshop on Deterring Cyberattacks, 2009: 180, http://sites.nationalacademies.org/CSTB/cs/groups/cstbsite/documents/webpage/cstb_059440.pdf.
[56] Ibid., 180.
[57] See Lewis, "Confidence-Building and International Agreement in Cybersecurity," 58.

Intuitively, the prospects of cooperation can significantly be increased if a state agrees to sacrifice a certain behavior for a reciprocal action by another state or multiple states. Thomas Schelling and H. Peyton Young both acknowledge that when the preferences of states conflict, the discord can be mediated by reciprocal sacrifice.[58] Similarly, Bernauer and Ruloff state that under these circumstances "Each party agrees to take specific action in exchange for some action by other parties."[59]

For many formulations of international cooperation in cyberspace, sacrifice may be decisive. Goldsmith illuminates this problem of mutual concession: "For our government to receive the concessions and relief that it thinks international cooperation by treaty can bring, it must be willing to clamp down on some, probably many, aspects of its many public and private cyber activities."[60]

Consider, for example, a regulation or ban on offensive weapons in cyberspace. The United States would need to balance a desire to mitigate the quantity and destructiveness of attacks that it is the target of while sacrificing the ability to conduct offensive operations against others. In this vein, Henry Farrell notes that "If the United States is serious about promoting a normative approach to interactions in cyberspace, it will have to undertake some difficult reforms."[61] Discerning at what threshold the United States or other states would be willing to sacrifice their capabilities in exchange for a mutually beneficial international agreement will be highly informative as to the degree of influence reciprocal concessions has on the explanatory variable of state interests.

---

[58] See Thomas C. Schelling, *The Strategy of Conflict*, Reprint edition (Cambridge, Mass.: Harvard University Press, 1981); and H. Peyton Young, *Equity: In Theory and Practice* (Princeton University Press, 1995).
[59] Bernauer and Ruloff, *The Politics of Positive Incentives in Arms Control*, 17.
[60] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 8.
[61] Henry Farrell, "Promoting Norms for Cyberspace," *Council on Foreign Relations Cyber-Brief*, 2015: 2.

Domestic Environments

Various characteristics of a state's domestic environment can affect its interests and ability to forge international agreements about cyberspace. Bernauer and Ruloff allege that capabilities emanating from a state's domestic situation may preclude a state from satisfying the proposed criteria that results from international cooperation. Therefore, states may choose not to pursue international cooperation considering the domestic conditions that significantly restrict their behavior once an agreement becomes reality.[62]

This argument is especially germane to cyberspace where the majority of the infrastructure is privately owned and operated. An international agreement targeted at state behavior raises critical questions about state responsibility and what institutions and individuals are under the authority of the state.[63] It is reasonable to envision a world in which states fail to agree on the concept of state responsibility as states recognize their inability to regulate the domestic environment to successfully adhere to a potential international regime.

Conversely, Simmons observes that characteristics of the domestic environment may incite a state to seek international cooperation. "[A]ctors may not only have incentives to make international agreements," she notes "but also to comply with them in order to solve an intractable domestic problem."[64] Domestic interests and international state interests are independent catalysts towards international cooperation from the perspective of Simmons.

---

[62] Bernauer and Ruloff, *The Politics of Positive Incentives in Arms Control*, 17.

[63] For more on state responsibility and state responsibility in cyberspace, see International Law Commission, *Draft Articles of Responsibility of States for Internationally Wrongful Acts*, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1; Nicholas Tsagourias, "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts," *Journal of Conflict and Security Law* 21, no. 3 (2016): 455–474; William Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0," 95 TEXAS L. REv. 1487, 1501 (2017); and Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

[64] Simmons, "Compliance with International Agreements," 82.

In the context of cyber, Simmons would plausibly argue that the United States may pursue an international agreement in order to resolve disagreements and conflicts with multinational corporations headquartered in the United States. These corporations are generally opposed to regulation, thus an international agreement might be one of the only avenues by which the United States could control these corporations. However, it is difficult to see how most domestic disputes, even those pertaining to multinational corporations, can be resolved internationally and generate enough collective international attention so as to lead to a codified agreement.

Surprisingly, there is little discussion of the influence of domestic environments on the prospects of international cooperation in cyberspace beyond analysis of relationships between the private (companies like Google and Facebook) and public (government) sectors. However, Lin does suggest that because the private sector "owns and operates much of the infrastructure through which cyberattacks might be conducted" and the government does not control the majority of the technology used to execute cyberattacks, domestic law may be the most viable method by which to regulate the behavior of non-state actors.[65] He does qualify his contention by noting that "the effectiveness of domestic laws depends on the availability of some enforcement mechanism."[66] Domestic regulation is not included in this paper's analysis, but Lin's assertion illustrates the intertwined nature of domestic and international regulation. The effectiveness of domestic law to regulate non-state actors has consequences for the ability of a state to adhere to and comply with an international agreement in cyberspace.

It is also important to note that the at least in the United States, the private sector does not necessarily want to work with or be controlled by the government. Specifically, during his keynote

[65] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."
[66] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."

speech at the RSA Conference in April 2018, Microsoft President Brad Smith argued "We need governments to stop targeting the public sector, hospitals, and power grids… we need to make the world a safer place. This requires that we not only do more [to address security risks] but do more together."[67] Smith is explicitly calling out the actions of the government and noting the importance of separating the coordination of the private sector from the government. This is in direct contrast to the behavior of the chemical industry during the CWC negotiations where the chemical industry was actively and cooperatively engaging with governments, as will be seen in chapter five. Therefore, a better understanding of the motives of the private sector and their appetite for engagement with the public sector can inform the likely nature of private sector participation in potential international negotiations to regulate cyberspace.

Beyond domestic law and private sector participation, regime type and domestic politics also shape state behavior and state interests, each of which affects the likelihood of cooperation. One of the key differentiators between the U.S. on the one hand and Russia and China on the other is regime type.

The U.S. is a democracy constrained by the Constitution and democratic values whereas Russia and China are autocracies whose survival is grounded in censorship and constraints on discourse. These regime differences help to explain the key disagreements between Western nations and Russia and China in cyberspace presented in the previous section.

[67] Brad Smith, "The Price of Cyber-Warfare," (speech, RSA Conference, San Francisco, CA, April 17, 2018), in Lindsey O'Donnell, "RSA 2018: Tech Giants form Cybersecurity Tech Accord," ThreatPost, April 17, 2018 https://threatpost.com/rsac-2018-tech-giants-form-cybersecurity-tech-accord/131253/.

Regime type also leads to different approaches to international cooperation. A recent body of literature has sought to understand how autocracies of various sorts pursue international cooperation. Erdmann et al. explain that autocracies tend to use instances of international cooperation to reinforce their rule and legitimacy.[68] Michaela Mattes and Mariana Rodriguez break apart the different manifestations of authoritarian regimes and argue that single-party regimes are more likely to pursue and are better equipped to succeed at international cooperation.[69] They also find that dictatorships may have little incentive to engage with and strengthen relations with other nations, closing off avenues of cooperation.[70] Evidently, regime type matters and it influences whether or not a nation chooses to negotiate in the first place and what it seeks to gain from the cooperation. Additionally, characteristics of a nation's domestic environment more broadly cannot be overlooked when analyzing international cooperation in cyberspace.

Information

One of the most commonly cited challenges to international cooperation and collective action problems more broadly is the availability of information. Secrecy and anonymity are the nucleus of cyber operations, with capabilities, intentions, and actions of actors in cyberspace all regularly concealed. Therefore, the uncertainty that arises due to a lack of information about another actor in cyberspace is central to the cooperation problem being explored and warrants an independent assessment. Verification and enforcement are also largely influenced by informational challenges.

---

[68] Gero Erdmann et al., "International Cooperation of Authoritarian Regimes: Toward a Conceptual Framework," GIGA Working Paper 229, (Hamburg: GIGA German Institute of Global and Area Studies, 2013). Available online at: www.giga-hamburg.de/de/publication/international-cooperation-of-authoritarian-regimes-toward-a-conceptual-framework. 5.

[69] Michaela Mattes and Mariana Rodríguez, "Autocracies and International Cooperation," *International Studies Quarterly* 58, no. 3 (2014): 536.

[70] Ibid., 536.

Uncertainty regarding information derives from two cases - lack of information about a state's capabilities and intentions that may impact its bargaining position in negotiations and lack of information about a state's compliance with an agreed upon cooperation framework. In a seminal work in this field, Jervis argues that international relations scholars must assume that state leaders make decisions "armed with uncertain knowledge and ambiguous information."[71] A deficiency in information about another side can negatively impact the outcome of cooperation. Conversely, an increase in the availability of information can improve the likelihood of cooperation. According to the perspectives of Jervis and Keohane, increased transparency and decreased levels of secrecy may positively impact the prospects of cooperation.

Similarly, Bernauer and Ruloff remark that "With insufficient information on the future preferences and behaviors of other actors . . . each actor is likely to make worst-case assumptions and fail to cooperate."[72] Their assertion implies that under the conditions in which incomplete information about another state exists, states are likely unable to achieve an optimal outcome through cooperation. Stephen Krasner likewise acknowledges the benefits of increased communication which inherently connotes an increase in the availability of information on the prospects of international cooperation.[73]

It is precisely these characteristics -- lack of information, asymmetry of information and uncertainty -- that characterize the cyberspace domain.[74] Due to these characteristics, attribution

[71] Robert Jervis, *Perception and Misperception in International Politics*, 1st edition (Princeton, N.J: Princeton University Press, 1976), 5.
[72] Bernauer and Ruloff, *The Politics of Positive Incentives in Arms Control*, 16.
[73] Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," 196.
[74] Asymmetry of information refers to circumstances under which one side has better information about a particular issue than another. Such circumstances result in an imbalance in the power distribution among negotiating parties.

and verification, which both rely on sufficient information about the technology and adversary, become very burdensome.

Goldsmith recognizes the challenges to attribution and verification as insurmountable barriers he does not believe the international system will adequately overcome. He summarizes his skepticism in this way: "in the absence of decent verification, we cannot be confident that transparency measures are in fact transparent, or that revealed doctrine is actual doctrine . . . anonymity is a norm destroyer."[75]

From a theoretical perspective, Simmons notes that "one function of international agreements is to enhance the reputational consequences of noncompliant behavior by providing mechanisms that increase transparency and therefore improve information regarding other states' behavior."[76] However, these potential benefits of an agreement are nullified if there is insufficient information about another state and a lack of transparency. Under these conditions, exploitation can occur, discord can persist, and states cannot verify adherence to an international agreement.

Goldsmith is not alone in his recognition of the challenges posed by attribution and verification. Grant Hodgson devotes an entire article to evaluating the efficacy of various methods of verification as applied to cyber operations to conclude that many of the methods traditionally used for verification are not so easily translated into cyberspace. Hodgson elevates the importance of his analysis by arguing that a UN General Assembly resolution has agreed that "adequate and effective verification is an essential element of all arms limitation and disarmament agreements."[77] Essentially, without verification, arms control is neither effective nor feasible.

---

[75] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 12.
[76] Simmons, "Compliance with International Agreements," 81.
[77] Grant Hodgson, "Cyber Attack Treaty Verification," *ISJLP* 12 (2015): 231.

This judgment about the necessity of verification is reiterated by Lin who states that "Many analysts argue that arms control agreements without adequate verification provisions are fatally flawed."[78] However, is this emphasis on verification as big a concern as scholars make it out to be? In looking at the Biological and Toxin Weapons Convention (BTWC) and even the Geneva Conventions, there are consistently arguments made that these agreements are not verifiable and thus ineffective. Yet, the agreements still hold weight in the international system and have not been revoked. Surely these agreements are not as effective as they would be with verification measures that states trusted and obeyed, but nevertheless the agreements still guide state behavior and codify norms. Additionally, if an agreement is tasked with regulating use instead of regulating the possession of technology, verification is inherently implausible. Therefore, verification may have to be an element of negotiations that is actively pushed aside and not regarded as fundamental to an international agreement in cyberspace.

The BTWC and Geneva Conventions also reflect other international relations arguments about the characteristics of information. For example, Haas argues that regimes generate and distribute information that can reveal new and valuable information which shapes the cause and effect of future relationships.[79] Even without effective verification, regimes can perform as generators and distributors of information that can have future effects on a state's calculations about international cooperation. The information extracted from negotiations can help to resolve conceptual disagreements and bring state interests into alignment. A critical shortcoming of this analysis, however, is the assumption that there was enough information and transparency for states to initially establish an agreement or regime in the particular issue-area. Given this assumption holds,

[78] Lin, "Arms Control in Cyberspace: Challenges and Opportunities."
[79] Haas, "Words Can Hurt You; Or, Who Said What to Whom about Regimes," referenced in Oye, "Explaining Cooperation under Anarchy," 11.

the question then becomes whether the new information or perceptions have a significant enough effect to shape future international cooperation.

Summary

Cyberspace is plagued by a variety of disagreements between states and unstable conditions due to the nature of the technology. However, there is an opportunity for international cooperation. This chapter presented an overview of the contemporary cyberspace environment and the barriers to an international agreement. The analytical framework of explanatory variables discussed in the previous chapter was employed to assess both the international relations literature on international cooperation and the literature on cyber arms control. This chapter also identified shortcomings of both bodies of literature in effectively and strategically assessing international cooperation in cyberspace. A judgement about the conditions most likely to contribute to international agreements in cyberspace will require linking the two bodies of literature and situating the diverse and commonly conflicting arguments about optimal conditions in historical case studies with opposing outcomes but similar underlying characteristics to cyberspace. The next two chapters will apply this same analytical framework to the two case studies - the Reykjavik Summit and the CWC - to better understand the conditions most conducive to international agreements in cyberspace.

Chapter 4 The Reykjavik Summit and the Failure of Nuclear Missiles Elimination

At first glance, the Reykjavik Summit does not appear to resemble what one might envision negotiations in cyberspace to be like. Yet, the role that the Strategic Defense Initiative (SDI) played in the negotiations and the fact that the Soviets and U.S. were engaging in critical dialogue about relatively new and revolutionary technology can and should help shape an understanding of the prospects of international agreements in cyberspace. This chapter seeks to assess what conditions most prominently determined the outcome of the negotiations at Reykjavik according to the five variables at the core of this thesis: technology, geopolitical dynamics, state interests, domestic environments and information. In the case of Reykjavik, the challenges posed by the security dilemma of the technology, the diversion of state interests and relative lack of reciprocal concessions, and significant domestic constraints on the leaders were the most influential determinants of the outcome of the negotiations.

First, this chapter argues that the implications of the security dilemma derived from nuclear technology shaped negotiating positions which in turn limited the window of overlap for cooperation. Second, the introduction of SDI threatened to upend the existing strategic balance between the U.S. and the Soviet Union as established by the proceedings of the Cold War even though this did not influence the outcome of the negotiations. Third, Reykjavik illustrates the importance of reciprocal concessions and the necessity for core state interests to be aligned to facilitate agreement. Fourth, this chapter demonstrates that domestic politics can sway negotiating postures and

limit the capacity for cooperation. Lastly, the Reykjavik Summit confirms the importance of negotiations, regardless of their outcome, in generating information that makes possible future cooperation.

Setting the Stage

Between the years 1945 and 1989, the United States and the Soviet Union were embattled in a war absent combat: the Cold War. The two superpowers that emerged following the end of World War II consistently challenged each other's ideologies, economic and political preferences, and engaged in a dangerous arms race for nuclear weapons. As tensions rose, the nations periodically pursued negotiations to address many of their disagreements. Throughout the nearly 50 years of hostilities, the U.S. and the Soviet Union never fought each other directly. They did, however, sign numerous treaties spanning topics from nuclear arms reductions to outer space security to defense and cooperative agreements. Yet to nuclear abolitionists, the momentous agreements that arose during times on the brink of full-blown nuclear war are of little import compared to what could have been at Reykjavik in October 1986.

October 11 and 12, 1986 are forever remembered as the days when the Soviet Union and the United States almost eliminated nuclear-armed ballistic missiles and the threat they posed. But, in 2018 at the time of the writing of this thesis, the United States and Russia combined still own approximately 14,000 nuclear warheads.[1] The Reykjavik Summit of October 1986 evidently did not result in the elimination of these missiles. This chapter seeks to assess the conditions that allowed for possible elimination and those that contributed to the ultimate failure of the U.S. and the Soviets to eliminate ballistic missiles. It is important to acknowledge that the summit itself was

[1] "Nuclear Weapons: Who Has What at a Glance | Arms Control Association." Arms Control Association. Accessed January 31, 2018. https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

not a failure. There were many important discussions at the summit that laid the groundwork for the INF Treaty and for START.

Of critical relevance to the Reykjavik Summit and the time period being analyzed is the U.S. SDI program.[2] SDI was announced by U.S. President Ronald Reagan in a public speech in March 1983 and was presented as a program to render nuclear weapons obsolete and keep the American people safe.[3] In the words of U.S. Secretary of State George Shultz, "the SDI program ambitiously said we would know that [a missile] was fired and we could knock it down before it hits us."[4] The Soviets, however, viewed the announcement of SDI in a very different light - an idea that is explored in greater depth in the following sections. In the 1983 speech, Reagan continually asserted that the U.S. program was going to be conducted in adherence to the Anti-Ballistic Missile (ABM) Treaty and all other obligations the U.S. held to the Soviet Union.[5] Yet, due to the ambiguity of the text of the treaty and the variety of possible interpretations, the dispute about SDI's alignment with the provisions of the treaty shaped the outcome of the summit and continued many years beyond Reykjavik.[6]

---

[2] The SDI program was a research program announced by President Reagan with the hopes of rendering nuclear weapons obsolete. The intentions were to "develop a space-based missile defense program that could protect the country from a large-scale nuclear attack. The proposal involved many layers of technology that would enable the United States to identify and destroy automatically a large number of incoming ballistic missiles as they were launched, as they flew, and as they approached their targets." Department Of State. The Office of Electronic Information, Bureau of Public Affairs. "Strategic Defense Initiative (SDI), 1983," May 1, 2008. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm.

[3] Ronald Reagan, "Address to the Nation on Defense and National Security," Speech, The White House, Washington, D.C., March 23, 1983, Ronald Reagan Presidential Library, *Public Papers,* Reagan Library.

[4] Secretary George Shultz, interviewed by Rachel Hirshman, Stanford, CA, February 2018.

[5] Treaty on the Limitation of Anti-Ballistic Missile Systems, May 26, 1972, United States-U.S.S.R., 23 U.S.T. 3435, T.I.A.S. No. 7503. The ABM Treaty, signed and ratified in 1972, helped govern the development of nuclear-based missile defense systems. The general guiding principle of the treaty was that both the U.S. and U.S.S.R. agreed not to deploy ABM systems in defense of its nation with the exception of a permitted "development area" and test regions.

[6] See, for example Frances V. Harbour, "The ABM Treaty, New Technology and the Strategic Defense Initiative." *J. Legis* 15 (1988): 119; Malvina Halberstam, "The Use of Legislative History in Treaty Interpretation: The Dial Treaty Approach," *Cardozo Law Review* 12 (1991 1990): 1645–52; Kenneth C. Randall, "The Treaty Power." *Ohio State Law Journal* 51 (1990): 1089–1126.

In 1985, two years after the SDI speech, Mikhail Gorbachev came to power as the General Secretary of the Communist Party of the Soviet Union. Gorbachev viewed the relationship with the U.S. differently from his predecessor, Konstantin Chernenko. By virtue of the development of a cordial relationship with Reagan and seeking a departure from Chernenko's policies, Gorbachev desired the reopening of negotiations with the U.S. to resolve important disputes.[7] The first round of resumed negotiations took place in Geneva in March 1985. These negotiations followed a joint declaration by Secretary Shultz of the U.S. and Foreign Minister Andrey Gromyko of the Soviet Union that outlined the impetus for the restart of negotiations. Shultz and Gromyko's statement highlighted strategic nuclear arms, intermediate-range nuclear forces, and space arms as the topics of gravest importance.[8]

The March negotiations, however, made little progress in drafting terms of agreements on these three issues. Thus, Gorbachev and Reagan's paths met again in November 1985 in the familiar location of Geneva. The agenda in November differed slightly from that in March as Reagan and Gorbachev agreed to discuss human rights, regional issues, bilateral matters, and arms control.[9] Yet, once again November did not produce substantial agreements.

Hence, while on vacation in Crimea in August 1986, Gorbachev phoned his principal advisor Anatoly Chernyaev, instructing him to draft a letter to Reagan requesting a meeting.[10] In his letter to Reagan, Gorbachev proposed a meeting at Reykjavik in preparation for Gorbachev's visit to the U.S. later that year. He communicated that "I am convinced that we shall be able to find

[7] William Taubman. *Gorbachev His Life and Times* (Simon & Schuster, 2017), 277.
[8] Jack F. Matlock Jr., *Reagan and Gorbachev* (New York: Random House, 2004), 66-69.
[9] To the Geneva Summit: Perestroika and the Transformation of U.S.-Soviet Relations, in National Security Archive Electronic Briefing Book No. 172.
[10] Taubman. *Gorbachev His Life and Times*, 294.

solutions, and I am prepared to discuss with you in a substantive way all possible approaches to them. . .”[11] The leaders were desperate for resolution and hopeful that new talks would be fruitful.

In chilly Reykjavik, Iceland, Gorbachev and Reagan convened at Hofdi House along the water to address the same four points on the agenda in the November 1985 negotiations - human rights, regional issues, bilateral matters, and arms control. This time, though, the media was excluded from the talks and there was an emphasis on the informality of the meeting.[12] These factors opened up the doors for more frank and direct engagement between the leaders. Under these circumstances, the two leaders nearly agreed to progressively eliminate ballistic missiles to zero. They also even discussed future efforts to eliminate all categories of nuclear weapons to zero.

Such a feat was unimaginable until the news of Reykjavik broke. Not only were nuclear warheads, and the ballistic missiles that carried them, the cornerstone of post-WWII security and strategic doctrine, they were also a means of demonstrating military prowess and maintaining superpower status. It was unfathomable at the time to envision the two greatest powers giving up the very weapons that other nations were positioning to get. In Secretary Shultz’s words, “it was radical” for the Soviets to propose the skeleton of the deal to eliminate ballistic missiles at the outset of Reykjavik.[13] For the U.S. delegation, Shultz acknowledges that “the first session was so surprising because Gorbachev laid on the table all our positions.”[14] But, Shultz continues, “[Gorbachev] conditioned everything . . . on what amounted to killing SDI.”[15] Regardless of the outcome,

[11] Mikhail Gorbachev letter to Ronald Reagan, 15 September 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 1.
[12] George P. Shultz. *Turmoil and Triumph: My Years as Secretary of State* (New York: Charles Scribner's Sons, 1993), 752.
[13] Secretary George Shultz, interviewed by Rachel Hirshman.
[14] Ibid.
[15] Ibid.

it truly was revolutionary just how close Gorbachev and Reagan came to agreeing to eliminate nuclear-armed ballistic missiles.

The reason why these missiles were not eliminated is most succinctly articulated by William Taubman in a biography of Gorbachev: "For Reagan, it was SDI that rendered nuclear weapons obsolete. For Gorbachev, SDI rendered an agreement to abolish them impossible."[16] However, Reykjavik is not regarded as a complete failure. Important progress was made to address incompatibilities between the two superpowers over nuclear testing, human rights, and nuclear reductions. Reykjavik planted the seeds for the success of future negotiations that resulted in critical treaties to tame the tensions of the Cold War.[17] The following sections analyze the various intricacies of Reykjavik in greater detail and link the lessons learned at Reykjavik back to cyberspace.

Technology

Many scholars may contend that technological comparisons between cyber and nuclear are impractical and unreasonable. But, that is not the goal of this section nor this case study. Instead, the focus here is on how the characteristics of a technology, regardless of what the technology is, influences the outcome of the negotiations. Practically, it may be difficult to completely separate these types of analysis, but this section attempts to isolate the technology itself from the technology's geopolitical influence.

The following paragraphs outline how the security dilemma resulting from nuclear technology shaped the negotiations at Reykjavik and limited the window of cooperation. The discussion is separated according to Robert Jervis's conceptualization of offense-defense theory. First,

[16] Taubman. *Gorbachev His Life and Times*, 295.
[17] The Intermediate-range Nuclear Forces Treaty (INF Treaty) and the Strategic Arms Reduction Talks (START) both heavily benefitted from discussions at and agreements reached at Reykjavik. See Shultz. *Turmoil and Triumph: My Years as Secretary of State*.

the differentiation between the offensive and defensive natures of the SDI technology is assessed. Secondly, the relative balance of offensive and defensive weapons at the time is studied. The implications of offense-defense theory are even more severe in cyberspace. So, the challenges experienced at Reykjavik argue for even more pronounced challenges to agreements in cyberspace, although there are ways to mitigate those challenges.

Before proceeding to this analysis, it is important to acknowledge a fundamental paradox about SDI. Some members of the Soviet scientific and military community and much of the U.S. defense-industrial complex felt it was very difficult to produce such a system. But Reagan, and some of his close allies, fundamentally believed that SDI was a real possibility in the near future. Yet regardless of the supposed feasibility of SDI, the threat of the technology at some point in the future opened the door for transformational debates along the lines of Jervis's offense-defense theory.

Whether a ballistic missile defense (BMD) system such as SDI is offensive or defensive oriented is a matter of perception but of critical importance. Ballistic missile defense comprises "All active and passive measures designed to detect, identify, track, and defeat attacking ballistic missiles (and entities), in both strategic and theater tactical roles, during any portion of their flight trajectory (boost, post-boost, midcourse, or terminal) or to nullify or reduce the effectiveness of such attacks."[18] Evidenced by the name, ballistic missile defense systems are advertised as defensive.

[18] "Ballistic Missile Defense (BMD)." Ballistic Missile Defense Glossary Version 3.0. Accessed January 31, 2018. http://www.dtic.mil/dtic/tr/fulltext/u2/a338544.pdf.

But in many circumstances, the country whose missiles the BMD is intended to intercept regards the system as offensive-oriented. The Soviet Union, for example, accused the U.S. of developing SDI to facilitate a first-strike.[19] The idea behind the contention that SDI gives the U.S. a first strike capability is that with a defensive system in space, the U.S. could much of the Soviet Union's nuclear capability, reducing the potential force for a counterattack. The U.S. would also have in place a system to destroy or stymie a counterattack if it does occur.[20]

SDI can also be viewed as a means of tying the hands of the Soviets by forcing them either to develop offensive missiles to render the defense useless or to build analogous defenses.[21] At the time, the Soviets did not have the economic resources or the technological knowhow to develop offensive or defensive programs to effectively challenge SDI. They did, however, have the capacity to develop numerous decoys that would make the development of a comprehensive and effective SDI program more complicated and demanding.

In internal discussions, the Soviets clearly articulated their view that SDI was not only offensive or defensive in nature; it was both. They asserted that its two purposes could not be differentiated from each other. Preparatory documents for Gorbachev's meeting with Reagan at

[19] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament, October, Box 4, Folder 13, Vitalli Leonidovich Kataev Collection, Hoover Institution Archives, Stanford, California.
First-strike in the nuclear domain refers to an attack with nuclear weapons that paralyzes the other side and reduces their capability to use their nuclear forces.
[20] Hobart Rowen, "Soviets See SDI as Economic First Strike," The Washington Post, 19 October 1986. https://www.washingtonpost.com/archive/business/1986/10/19/soviets-see-sdi-as-economic-first-strike/36fddf24-5dba-4137-a65c-3af999381250/?utm_term=.4abd7dd56f5b.
[21] Sidney D. Drell, Philip J. Farley, and David Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative," *International Security* 9, no. 2 (1984): 72.

Reykjavik suggest the Soviet belief that "[t]here is no basis for separating space-based strike weapons into offensive and purely defensive categories. This distinction is useful to the U.S. to mask the true goals of creating a multi-echelon missile defense system."[22]

The offensive nature of the system can be understood from how BMDs operate by actively shooting down missiles. To the Soviets, "[SDI] is a strategic offensive system designed to destroy the warhead of our missiles and also other objects in space, on earth, and in the air."[23] The Soviets' actions demonstrated a fear of being both physically and strategically threatened by SDI and they were unable to trust U.S. rhetoric that there were no intentions to use the system for anything beyond missile interception in protection of the American people.

In the face of these accusations, Reagan and the U.S. maintained their stance that SDI was strictly defensive. Replying to Gorbachev's allegation of the U.S. wanting a first strike, Reagan contended "We are accused of wanting a first-strike capability, but we are proposing a treaty that would require the elimination of ballistic missiles before a defense can be deployed; so a first strike would be impossible."[24] Reagan's assertion illustrates his desire to shift from a system of deterrence based on offensive nuclear programs to a system of deterrence based on defensive systems. His argument is that in the latter environment, if there is no existing defense, there is nothing preventing either side from rebuilding offensive nuclear-armed missiles. Effectively, if there is a defense after the elimination of offensive missiles as Reagan proposes, building offenses is futile. Regardless of whether or not it would or could be fully realized, Reagan's contention illuminates a critical argument that is often missed in discussions of the heated exchanges at Reykjavik.

[22] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament.
[23] Ibid.
[24] Shultz. *Turmoil and Triumph: My Years as Secretary of State*, 760.

There are three possible explanations for Gorbachev's rejection of this rationale. First, Gorbachev fundamentally distrusted Reagan and was not willing to risk Reagan deploying SDI before offensive ballistic missiles were completely eliminated. This is a perfect example of a credible commitment problem. Shultz acknowledges this reality: "[Gorbachev] worried that if SDI research proved successful in the near term, the United States would simply not wait for the ten years to expire before deploying."[25] The ten years referred to pertain to the restricted period during which the states agreed not to circumvent the ABM Treaty.

The second possibility is that both Reagan and Gorbachev feared breakout from a treaty to eliminate ballistic missiles. This is highly realistic because both sides knew how to make ballistic missiles even if they eliminated some and neither side doubted the other's capability to do so.

A third interpretation is that regardless of what Reagan said, Gorbachev was not willing to let the SDI program continue and would employ any reasonable argument against it to convince Reagan of its destabilizing effects.

All three interpretations are convincing and likely in combination explain the impenetrable barrier that SDI was at Reykjavik.

The second consideration from the offense-defense theory and relevant to both SDI and cyber is the offense-defense balance. As mentioned in the previous chapter, the offense-defense balance seeks to address whether the offense or defense has an advantage over the other. The foreign policy community, defense specialists, and academics all characterized the strategic environment at the time of the Reykjavik Summit as offense dominated.[26] That is, in a reasonable

[25] Ibid., 770.
[26] Drell, Farley, and Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative," 67.

amount of time the offense could develop the capability to penetrate the defense and make it ineffective.

There are many reasons that SDI and BMDs more broadly are characterized in this way. Most prominently, a defense like SDI encourages a buildup of offensive forces by the opposing power that can penetrate the defense. In this vain, the defense always has to keep up with the development of offensive systems.[27] The defense is always behind because it cannot realistically predict all the ways in which offenses can be developed to counter it.

The security dilemma resulting from SDI at Reykjavik has implications for international agreements in cyberspace but is of limited relevance primarily because the security dilemma is incomparably more pronounced in cyberspace. The operational preparation of the environment is critical to both offensive and defensive operations in cyberspace. Nations will intrude the information systems of other nations for reconnaissance and also to allow for the option to attack at some point in the future. If a nation discovers another nation in its system, it is nearly impossible to determine whether the other nation has intruded for offensive or defensive purposes given this operational preparation. Therefore, the way to distinguish between offensive and defensive attacks is to understand a nation's intent in conducting those operations which ironically might involve espionage operations by the victim state.

This reality suggests that it is difficult to differentiate between offensive and defensive operations purely based on the technology. A similar situation arose at Reykjavik where the deployment of the system can be analogized to the operational preparation of the environment at which point the system can be defensive in intercepting missiles or offensive by allowing for a

[27] Ibid., 60.

first strike. However, a critical distinction between BMDs and cyberspace is that cyberspace is inherently private and secretive whereas BMDs are visible and publicly known. This lack of visibility heightens the significance of the security dilemma in cyberspace.

The discussion of the offense-defense balance in cyberspace is much more nuanced. For a long time much of the cyber community was in consensus that offense had an advantage over defense because defense had to be perfect one hundred percent of the time whereas the offense only had to be right once. However, Rebecca Slayton's *What is the Cyber Offense-Defense Balance?* article led many to reconsider. Slayton argues that information technology defense is based on the technology and organizational behavior; technology and behavior cannot be separated.[28] In this context, Slayton argues that the conceptualization of offense dominating defense is misguided based on a cost-benefit analysis so long as organizational behavior and skills are accounted for. Regardless, the contemporary debate about the offense-defense balance illustrates its importance to policy making and an understanding of how to protect ourselves and our systems from malicious cyber incidents.

Nonetheless, the overall lessons about how the nations navigated SDI's influence on international relations elucidates the types of challenges that may arise in cyberspace. The CWC case study is more informative of how nations can circumvent the complications of the security dilemma by regulating intent and behavior rather than the possession of technology as Reykjavik sought to do. It is likely that the implications of the security dilemma will be influential during cyberspace negotiations, but they will not be highly indicative of the prospects of an agreement.

Geopolitical Dynamics

[28] Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," 82.

The conditions associated with power dynamics and how the nations involved in the negotiations perceived and interacted with each other in the context of Reykjavik are more salient to the nuclear domain than anything else and were not particularly relevant to the outcome of the negotiations. That is not to say that lessons cannot be gleaned from this variable and extrapolated to cyber. However, ultimately little weight will be placed on the conclusions of the analysis of this variable because of distinct differences between nuclear and cyber.[29]

The bilateral nature of the Reykjavik negotiations helped to simplify the negotiations by limiting the number of interests being considered. However, while the summit is commonly viewed through this bilateral lens, other nations had a stake in the negotiations and the negotiating nations had to actively consider how others would react. For example, in discussing the Reykjavik negotiations and the deployment of intermediate range nuclear weapons by the U.S., Secretary Shultz states "we knew we were bargaining not just with the Soviet Union but we were bargaining with European publics because if a nuclear weapon is stationed near you, it's a target and you're nervous."[30] Other nations, including China, also publicly expressed opinions about SDI and the importance of maintaining the ABM Treaty because of the standard it sets for the entire world.[31] Therefore, while not directly party to the negotiations, world powers beyond the U.S. and Soviet

[29] For discussion of the shortcomings of the analogy between nuclear and cyber see: Patrick Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence." Bulletin of the Atomic Scientists, February 22, 2016. http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179; Herbert Lin, "A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity"; and Patrick Cirenza, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence.* Center for International Security and Cooperation Honors Thesis, Stanford University, 2015.
For a more nuanced discussion of the relationship between the nuclear domain and the cyber domain see: Joseph S. Nye Jr., "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?," *Bulletin of the Atomic Scientists* 69, no. 5 (September 2013): 8–14, https://doi.org/10.1177/0096340213501338; Joseph S. Nye Jr, "Nuclear Lessons for Cyber Security" (AIR UNIV PRESS MAXWELL AFB AL, 2011), http://www.dtic.mil/docs/citations/ADA553620; and Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, April 28, 2009), https://papers.ssrn.com/abstract=1396375.

[30] Secretary George Shultz, interviewed by Rachel Hirshman.

[31] Ronald E. Dolan, Russell R. Ross, and Robert L. Worden. "East Asia/Pacific Reactions to the Strategic Defense Initiative." *Federal Research Division of the Library of Congress,* January-December 1986: 1.

Union had a strategic interest in the negotiations. Cyberspace, on the other hand, consists of myriad actors who each have a substantial stake in the outcome of negotiations. The cyberspace domain thus embodies multilateralism rather than bilateralism with other relevant interests.

Another element of the power dynamics variable as it pertains to the Reykjavik Summit was the importance of the strategic balance between the two superpowers. The widely recognized result of the development of a defensive system such as SDI, as explored with regards to the technology variable, was a destabilizing arms race with the Soviets seeking to modernize their offensive capabilities to counter the U.S. defense. It is more likely that the resulting arms race would involve the development of offensive missiles to counter defensive systems than for both sides to compete in defensive systems. A Report of the Committee of Soviet Scientists in Defence of Peace and Against the Threat of Nuclear War concluded that "it would be much cheaper to develop effective means of destroying space-based systems than to develop the systems themselves."[32]

The resulting strategic balance is much less stable and no longer grounded in the governing principles of deterrence and mutually assured destruction.[33] Without an alternative mechanism to prevent the superpowers from using their nuclear warheads, the strength of deterrence on which the peace and stability of the international system rests becomes precarious. "If then it turns out

[32] *Prospects for the Creation of a U.S. Space Ballistic Missile Defense System and the Likely Impact on the World Military Political Situation*, Report of the Committee of Soviet Scientists in Defence of Peace and Against the Threat of Nuclear War, Moscow, 1983, mimeo.

[33] Drell, Farley, and Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative," 56.

Deterrence is defined as "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits." "Deterrence." Department of Defense Dictionary of Military and Associated Terms. Accessed January 31, 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

Mutually Assured Destruction refers to the doctrine that the U.S. and the Soviet Union are capable of exacting unacceptable damage on each other at all times, which provides a deterrent against the use of nuclear weapons in the first place. Edward S. Boylan, Donald G. Brennan, and Herman Kahn. "An Analysis of "Assured Destruction."" *Hudson Institute* (1972): 1.

all of a sudden one party can defend itself," Shultz notes, "then all of a sudden that deterrence equality disappears."[34] This argument is supported by Sidney Drell et al.'s analysis of the Soviet Scientific report: "the net effect of deploying such a system would not be to provide an escape from mutual deterrence, but to make that relationship less stable."[35]

From the U.S. perspective, the introduction of SDI and the way it shaped Soviet responses and approaches to the U.S. was "a revolution in [U.S.] strategic doctrine."[36] The program, effective or not, was viewed as a shock to the existing strategic balance in the international system by the Soviets and leading thinkers in the U.S. administration.

In a contemporaneous argument, Drell argued that the new program, SDI, "is at odds with the premises on which Soviet-American strategic relations have been conducted, and arms control negotiations based, for the last fifteen years."[37] Such a unilateral change, Drell contends, compels the Soviet Union to respond according to its own calculations of how the strategic balance shifts. This shift in power also has implications for international stability and deterrence more broadly because of the resulting security calculations that the superpowers would make.

The link between strategic calculations because of SDI and the technological factors of SDI shaping viewpoints is intrinsic. The technical feasibility and quality of a defensive system shape the balance of power in the international system. Should the system be ineffective in fending off all possible ballistic missile threats, the result is destabilizing because it feeds fears of a first

[34] Secretary George Shultz, interviewed by Rachel Hirshman.
[35] Drell, Farley, and Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative," 63.
[36] Shultz. *Turmoil and Triumph: My Years as Secretary of State*, 250.
[37] Drell, Farley, and Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative," 53.

strike. If a perfect, impenetrable defense is developed and deployed, the U.S. has a significant strategic advantage by being able to effectively combat the Soviet threat.

The resulting U.S. military and strategic dominance would be a revolution in the power dynamics in the international system as it would diminish the Soviet Union's superpower status and transform the balance of power to be unipolar instead of bipolar. Surely, these are hypothetical scenarios derived from educated presumptions. However, even though the SDI program was in its infancy at the time of the Reykjavik Summit, the two superpowers evidently pondered the scenarios presented above. The possible shifts in power dynamics resulting from SDI, although never realized, helped shape the negotiating postures and fears of the two leaders during the Reykjavik Summit.

This section illuminates how unpredictability drives fear which in turn shapes negotiating postures. But, the analysis presented here does not serve this thesis's broader argument because elements of geopolitics at Reykjavik were not deterministic of the outcome of negotiations and because of the difficulty in comparing the circumstances in 1986 to the present.

State Interests

There are two primary takeaways from the Reykjavik Summit with respect to state interests. First, the fundamental misalignment of state interests impeded the potential for cooperation in a significant way. This misalignment of interests manifested in many ways but perhaps most prominently in the disagreement over the appropriate interpretation of the ABM Treaty. The two prominent interpretations of the treaty discussed at Reykjavik are the broad interpretation and the

narrow interpretation.[38] The broad interpretation says that research and development on technologies not covered explicitly by the treaty is acceptable.[39] The narrow interpretation argues that such R&D is not allowed under the treaty.[40] Both interpretations, however, agree that the deployment of BMD technologies is prohibited under the treaty.

The differing interpretations are viewed less as disagreements over the text of the treaty and more as conceptual disagreements over how the nuclear domain should be allowed to evolve. These disagreements are rooted in national experiences that have shaped understandings and negotiating positions. Second, and most importantly, the leaders failed to reach an acceptable level of reciprocal concessions to facilitate cooperation and the arrival at an agreement.

While the U.S. and Soviet interests were generally in alignment, they were not perfectly cohesive. The U.S. and Soviets were mutually interested in restraint on nuclear-armed ballistic missiles. However, the reduction of offensive forces was a secondary concern to the Soviets. The Soviet's primary goal as communicated by Gorbachev in preparation for the summit was to "to prevent the next round of arms race . . ."[41] Unquestionably, the Soviets and especially Gorbachev sought reductions in offensive missiles. Yet, Gorbachev was unwilling to accept a reduction in

[38] The disagreement over interpretations of the ABM Treaty hinged on Agreed Statement D which reads:
"In order to insure fulfillment of the obligation not to deploy ABM systems and their components except as provided in Article III of the Treaty, the Parties agree that in the event ABM systems based on other physical principles and including components capable of substituting for ABM interceptor missiles, ABM launchers, or ABM radars are created in the future, specific limitations on such systems and their components would be subject to discussion in accordance with Article XIII and agreement in accordance with Article XIV of the Treaty." Treaty on the Limitation of Anti-Ballistic Missile Systems, Agreed Statement D.
[39] Abraham D. Sofaer, "The ABM Treaty and the Strategic Defense Initiative," *Harvard Law Review* 99, no. 8 (1986): 1972–85, https://doi.org/10.2307/1341216. 1973.
[40] Ibid., 1973.
[41] Gorbachev's instructions for the group preparing for Reykjavik, 4 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 5.

offensive forces without mutual restraint on defensive forces.[42] The Soviets were concerned about U.S. superiority in defensive systems and the inability to match the U.S. development if an arms race were to occur. In order to preserve their fundamental interests, they could not accept a deal that still allowed for an arms race they were unprepared for. Thus, the Soviets likely viewed the negotiations, as they did with the ABM Treaty, as a way of limiting the technologically superior U.S.[43]

In addition to constraining the technologically superior U.S., there are a variety of other reasons why Gorbachev was so frightened by the SDI program and linked it to reductions in offensive forces. The Soviet Union's status, and Gorbachev's political leverage, rested heavily on having superpower status and being a military dominant nation. SDI threatened the very heart of the Soviet's superpower status - its military prowess.[44]

The importance of the elimination of SDI for the preservation of the Soviet reputation as a superpower and a variety of other Soviet interests was evident in public discourse. The sheer magnitude of discussions about SDI in private and public domestic circles demonstrated the strong possibility for the program to influence Soviet interests and actions.[45] The Soviets liberally employed propaganda and public relations campaigns to dispel fears within the domestic public about

[42] Abraham Sofaer, "A Legacy of Reykjavik: Negotiating with Enemies," in Implications of the Reykjavik Summit on its Twentieth Anniversary, eds. S. Drell & G. P. Shultz, (Stanford: Hoover Institution, 2007): 61.
[43] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament.
[44] Benjamin S. Lambeth and Kevin Lewis, "The Kremlin and SDI," Foreign Affairs, March 1, 1988, https://www.foreignaffairs.com/articles/russian-federation/1988-03-01/kremlin-and-sdi.
[45] Lambeth and Lewis, "The Kremlin and SDI.

a shift in the strategic balance away from the Soviet Union. Although the Soviets pursued an intensive propaganda agenda to try to downplay the threat of SDI to the Soviet Union, internal documents suggest a real fear of the program among the leading Soviet government officials.[46]

As the previous sections indicate, the Soviets knew that SDI would not be possible with contemporary technology. However, the critical paradox is that SDI could still work in the future and there were reputational costs to allowing the U.S. to pursue a program that could threaten the Soviet's military capabilities and superpower status. Therefore, combative public measures directed at SDI were not simply empty statements; the Soviets could not ignore the SDI program and the threat it posed even if that threat was not immediate. As such, SDI altered the Soviet's calculus of how best to pursue its interests.

The composition of the Soviet delegation at Reykjavik also reflected an emphasis on propaganda. The Soviet delegations historically were composed of primarily KGB agents, the Soviet intelligence service. However, Shultz recognized a striking departure from this historical composition at Reykjavik. Not only were the Soviets "conducting a full-scale media blitz in the days before the summit," according to Shultz, but "the Soviet team was packed with officials associated with the media and propaganda."[47] Evidently, the resolute interest in reputation protection shaped the Soviet position and the summit as a whole.

An important dynamic that these Soviet interests and concerns explain is the use of negotiations to seek parity. According to Joseph Kruzel, "every arms control negotiation must deal with

[46] Dmitry Mikheyev, *The Soviet Perspective on the Strategic Defense Initiative* (Washington: Brassey's Inc, 1987), 2.
[47] Shultz. *Turmoil and Triumph: My Years as Secretary of State*, 756.

some asymmetries between negotiating states."[48] The Soviets were conscious of their technological inferiority. As such, the vast majority of the Soviet position was grounded in the ABM Treaty because that treaty ensured constraints on U.S. development that over time would have allowed the Soviets to "conduct analogous work in [their] country."[49]

Soviet interests could have been met at Reykjavik had there been agreement to constrain development and testing of missile defense systems, as the Soviets were the inferior power hoping to curb U.S. development. This disagreement is at the core of the difference between the broad and narrow interpretations of the ABM Treaty. Continued investment by the U.S. in SDI would widen the capability gap and threaten the core of Soviet interests. Therefore, negotiations and a hopeful agreement were the avenues through which the Soviets could actively shape U.S. actions and satisfy their interests.

While the Soviets were concerned that their reputation and superpower status were at stake, the U.S. and Reagan principally emphasized reductions in offensive forces. In U.S. documents, the administration noted that "deep reductions in ballistic missiles is the heart of the matter . . . main theme: it's time to move on to reductions."[50]

At the same time, it would be misguided not to recognize secondary concerns the U.S. delegation had. The matter of human rights was not to go unmentioned. In correspondence with Reagan before Reykjavik, Shultz emphasized "Gorbachev must go home with a clear sense that Moscow's continuing insensitivity to the humanitarian dimension of the relationship will assume

[48] Joseph Kruzel, "From Rush-Bagot to START: The Lessons of Arms Control," *Orbis* 30, no. 1 (1986): 210.
[49] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament.
[50] "The President's Trip to Reykjavik, Iceland, October 9-12, 1986 - Issues Checklist for the Secretary," U.S. Department of State, 7 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 7.

greater significance as prospects open up in areas of mutual concern."[51] The U.S. intently wanted to advance human rights in the Soviet Union, even devoting an entire working group at the summit to the topic.[52] Nonetheless, while it is important to acknowledge this active U.S. interest, it was not particularly controversial. Agreement on human rights was one of the important successes of Reykjavik.[53]

The ABM Treaty operated at the core of the dispute that destroyed the prospects of agreement on missile reductions.[54] President Reagan advanced a broad interpretation of the treaty that he believed permitted the U.S. to pursue the SDI program without violating any terms of the treaty.[55] Gorbachev, however, advocated a narrower interpretation of the treaty that implied that the development and testing of SDI must be constrained to the laboratory.[56] The two leaders and their respective aides held discordant opinions about what or what was not permitted according to the word of the treaty. Shultz even argues that the Soviets pursued an interpretation of the ABM Treaty that was even narrower than what the negotiators and experts on the treaty would contend.[57]

The interpretation challenges with the ABM Treaty more broadly reflect the national objectives at the negotiations. These types of interpretation challenges are especially pertinent to

[51] Memorandum to the President, Secretary of State George Shultz, "Subject: Reykjavik," 2 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 4.
[52] Thomas Blanton and Svetlana Savranskaya, "Reykjavik: When Abolition Was Within Reach," *Arms Control Today; Washington* 41, no. 8 (October 2011): 48.
[53] Shultz. *Turmoil and Triumph: My Years as Secretary of State,* 775.
[54] Sofaer, "The ABM Treaty and the Strategic Defense Initiative," 1972.
[55] Shultz. *Turmoil and Triumph: My Years as Secretary of State,* 753.
[56] For discussion of the differing interpretations of the ABM Treaty see Sofaer, "The ABM Treaty and the Strategic Defense Initiative"; and Strategic Defense Initiative, Box 20, Folder 18, Joan Beecher Eichrodt Collection, Hoover Institution Archives, Stanford, California.
There were indeed American analysts who also believed in the narrow interpretation of the treaty. But those involved in the negotiations at Reykjavik did not acquiesce to this perspective and sought to use the broad interpretation to justify the continued pursuit of the SDI program.
[57] Shultz. *Turmoil and Triumph: My Years as Secretary of State,* 773.

cyberspace where nations advance definitions of key terms, including about what is to be protected, as a means of promoting what is best for their own domestic and international security and politics. The Chinese and Russian insistence on "information security" as opposed to the Western advancement of "cybersecurity" precisely illustrates this dynamic. China and Russia are seemingly more concerned about restricting the transmission of information in their countries that can threaten their hold on power. Their shared experiences of liberal freedoms inciting revolutions and threatening their regimes leads them to this position. The U.S. and Western values of freedom of expression run counter to this emphasis on information security. Therefore, Western nations promote cybersecurity which advocates the protection of technology, while still allowing for the spread of information that may be in opposition to the government.

Beyond a mélange of conflicting and aligning interests at Reykjavik, another aspect of state interests to consider is a willingness to sacrifice on elements of one's negotiating posture. This factor fundamentally influenced Reykjavik and also plays a significant role in cyberspace. Discussion of concessions that were and were not made at Reykjavik feature prominently in the negotiating record. There were clear limits to how much each leader was willing to sacrifice in order to uphold its interests. Reagan's insistence on the preservation of the SDI program and Gorbachev's reluctance to reach any agreement that did not confine SDI to the laboratory illustrated the obstacle of mutual concession.

Reagan and Gorbachev bickered back and forth towards the end of the last day of the summit, each accusing the other of an unwillingness to make the necessary concessions to achieve their objectives. Gorbachev brashly contended "The American side has essentially not made any

concessions, not a single major step to meet us halfway. It's hard to do business on that basis."[58] Reagan also criticized Gorbachev on many occasions, at one point saying "But now, when I have asked you a personal favor which would have enormous influence on our future relations, you have refused me."[59] Late in the negotiations, the two leaders reached an impasse. Neither side was willing to change its posture beyond the limits already established.

The boundaries of the concessions the two leaders were willing to make are evident in preparatory documents. On the Soviet side, "Gorbachev informed the Politburo that he was prepared to make concessions on intermediate-range missiles and deep cuts in strategic weapons but would not compromise on Reagan's missile defense scheme."[60] Similarly, Reagan was not willing to compromise on any contingencies regarding his SDI program. Philip Taubman, former Moscow Bureau Chief for the New York Times, notes that "Reagan was willing to consider compromises that might lead to an agreement on intermediate-range missiles. He was also open to sharing missile defense technologies with the Soviet Union, but he was not prepared to abandon research and development work on a missile shield."[61]

Importantly, the negotiating record suggests that Reagan approached Reykjavik with a vision that was all or nothing. He supported either complete reductions on nuclear-armed ballistic missiles or nothing at all. There was not a middle ground where steps could be taken to complete reductions without the agreement hinging on full commitment. This approach is significant because such an all or nothing position obviously threatens the success of negotiations. Perhaps it is

[58] Russian transcript of Reagan-Gorbachev Summit in Reykjavik, 12 October 1982, in National Security Archive Electronic Briefing Book No. 203, document no. 16.
[59] Ibid.
[60] Philip Taubman, *The Partnership: Five Cold Warriors and Their Quest to Ban the Bomb* (New York: HarperCollins, 2012), 250.
[61] Ibid., 252.

more reasonable and practical to have an ultimate goal of complete reductions with the acceptance of steps taken towards that end and a promise of continued negotiations.

The outcome of Reykjavik thus implies that negotiations on international agreements in cyberspace may be most likely if topics are tackled in stages rather than all at once. Breaking down the topics of negotiations into manageable pieces can increase success and also maintain positive morale that progress is being made even if the ultimate objective is far off. And as Reykjavik suggests, even in the presence of an unwillingness to compromise, there are still issues that can effectively be addressed. At this point in time it is difficult to assess exactly what subjects in cyberspace would result in an impasse and what subjects might have overlapping interests. Nonetheless, without some compromise by one or many states, plenty of issues in cyberspace may remain unresolved like the reduction of nuclear-armed ballistic missiles while others can be agreed upon.

Conflicting state interests and an unwillingness to seek mutual concessions proved pivotal at the Reykjavik Summit. The Soviet Union's desire for parity and the U.S. eagerness for Soviet promise of acting in accordance with fundamental human rights clouded the nations' ability to cooperate on the issue of ballistic missile elimination. And most significantly, the leaders of the two countries maintained hard lines on positions they were against compromising on for the sake of nuclear arms reductions. Mutual concessions and state interests more broadly thus were critically relevant to the outcome of the negotiations and illustrate the importance of reciprocity in future negotiations over international agreements in cyberspace.

Domestic Environments

Given the different governmental regime structure of the two nations, the domestic environments influenced the leaders in different ways. Gorbachev, a leader of an authoritarian regime was constrained by domestic pressures to maintain the strong reputation of the Soviet Union as a

militarily dominant superpower and to preserve the Soviet Union as it existed in 1986.[62] A crippled economy threatened Gorbachev's rule and the future of the Soviet Union. President Reagan, a leader of a democratic nation, was limited in his proposals due to the desires of his domestic constituents and his political base. These elements of domestic politics in both nations were critically relevant to the outcome of the negotiations at Reykjavik.

The ways in which governmental structure - democracy, autocracy, etc. - influenced negotiations and potential agreements is especially applicable to cyberspace. Noticeably absent from the discussion of the domestic environment variable is the private sector. Given the limited relevance of the private sector to the nuclear domain and the negotiations at Reykjavik, the emphasis of this section is instead on the domestic politics that shaped the outcome. The section proceeds by highlighting the domestic conditions influencing the Soviet negotiating posture and concludes with a discussion of the domestic conditions determining the U.S. position.

The Soviet negotiating posture at Reykjavik was constructed in response to pressures from a crippled economy, a desire to maintain Soviet military superiority which was harmed by the Chernoybl accident, and a necessity to preserve the Soviet leadership's power.[63] Arguably, the most proximate factor shaping the Soviet negotiating posture was the Soviet Union's weak economy. The economy had been experiencing effectively zero growth for nearly twenty years.[64] With a lack of economic growth, the Soviets feared, they were not capable of competing with the United States. Specifically, Philip Taubman contends that "If a defensive arms race began, there was no

[62] Lambeth and Lewis, "The Kremlin and SDI."
[63] For more on the Chernobyl accident, see "Chernobyl Accident 1986," World Nuclear Association, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx.
[64] Writings 2 of 2, Box 69, Henry Rowen Collection, Hoover Institution Archives, Stanford, California.

guarantee that the Soviet Union could keep pace with American technology."[65] The paradox existed such that in order for the Soviet Union to subsist, it must pursue parallel technological developments to the U.S. However, technological and scientific development required economic support that, in this time of economic peril, would then threaten the stability and very existence of the Soviet Union.[66]

Thus, Gorbachev realized, the Soviets must present the Americans with compromises in order to pressure them to eliminate SDI and to mutually agree to reductions in nuclear arms. Arms control negotiations were the only ways that Gorbachev believed the Soviets could constrain U.S. development and maintain relative equality in military power. The alternative, Gorbachev and his close advisors internalized, was the ultimate defeat of the Soviet Union.

The gravity of these concerns seems astronomical compared to the potential concerns emanating from cyber power. However, the Russian and Chinese insistence on information security as opposed to cybersecurity reflects a real fear that freedom of information can threaten the regime and the leadership's survival. This analogous concern about regime stability illuminates that judgments about survivability of the regime are critical to the assessment of the favorable conditions for an agreement.

Unquestionably, economic struggles figured prominently in Soviet thinking leading to Reykjavik. Yet, there was a secondary concern that also propelled Gorbachev to introduce far-reaching concessions and to be so adamant about reducing nuclear arms. Only six months before

[65] Taubman, *The Partnership: Five Cold Warriors and Their Quest to Ban the Bomb*, 250.
[66] Mikheyev, *The Soviet Perspective on the Strategic Defense Initiative,* 3. See also Benjamin S. Lambeth and Kevin Lewis, "The Strategic Defense Initiative in Soviet Planning and Policy," Santa Monica: RAND Corporation (1988): vi.

Reykjavik, the Soviet Union experienced the world's most devastating nuclear accident at Chernobyl. While the accident demonstrated inadequate safety procedures at commercial nuclear plants within the Soviet Union, it also exposed a flawed design.[67] The public revelations of this information did not help Gorbachev or the Soviet's superpower position. As such, the destructive nuclear accident coupled with a deteriorating economic situation pressed Gorbachev to seek successful negotiations on nuclear arms.[68]

Contrary to constraints on Gorbachev, Reagan's primary domestic constraints derived from political promises he had made to the American people through public speeches about SDI and the conflict with the Soviets. In the heated discussions with Gorbachev at Reykjavik, Reagan admitted: "Let me say frankly that if I give you what you ask it will definitely hurt me badly at home."[69] Reagan was aware of the potential political consequences facing him if he returned home admitting the concession of confining SDI to a laboratory. Reagan's strong political base was very supportive of SDI, making it hard for him to renege on his promise to the American people. Similarly, public opinion polls at the time demonstrated significant public support for the missile defense program.[70]

Reagan recognized that this domestic constraint imposed upon him by the U.S. populace was a challenge uniquely faced by him due to the different governmental structure of the two nations. It is impossible to assess what the political consequences of succumbing to the Soviets in confining SDI to the laboratory would have been. However, the inability to analyze the counterfactual does not preclude judgements about Reagan's perceptions of the ramifications.

---

[67] "NRC: Backgrounder on Chernobyl Nuclear Power Plant Accident." Accessed January 31, 2018. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html.
[68] Mikheyev, *The Soviet Perspective on the Strategic Defense Initiative*, 3.
[69] Russian transcript of Reagan-Gorbachev Summit in Reykjavik.
[70] Arms Control Unchained, Box 20, Charles Hill Papers, Hoover Institution Archives, Stanford, California.

This perspective is best illustrated by Reagan's response to Gorbachev's assertion that SDI research and development be constrained to the laboratory.

> "I can't go along with that. You and I have different positions, different problems. In your country, nobody can criticize you without winding up in prison. In my country the situation is different. I have a lot of critics who wield great influence. And if I agree to such a formulation, they will launch a campaign against me; they will accuse me of breaking my promise to the people of the United States regarding SDI."[71]

Gorbachev countered Reagan's accusation that every critic of the Kremlin ends up in prison. Nonetheless, the two countries indisputably had different governmental structures that yielded divergent constraints on their leaders.

While domestic politics played a critical role at Reykjavik, the involvement of the private sector was not a factor. This lack of involvement is a shortcoming of the Reykjavik case study given the role of the private sector in cyberspace where private companies own and operate the majority of the infrastructure in the domain. Therefore, unlike in the nuclear domain, the government does not have a monopoly on the technology or weapons.

The absence of a state monopoly on the proprietary technology in cyber further exacerbates domestic constraints, especially in democracies such as the U.S. At Reykjavik, Reagan was not concerned about cooperation with the private sector to develop SDI or implement the terms of a potential agreement and neither leader required assistance from the private sector to conduct nuclear policy. Regardless, the analysis of the significance of domestic politics on the outcome of the negotiations at Reykjavik illustrates that the domestic dimension of negotiations cannot be overlooked.

Information

[71] Russian transcript of Reagan-Gorbachev Summit in Reykjavik.

The Reykjavik Summit case study does little to inform the cyber domain what the most precipitous conditions are for the development of an effectively verifiable and enforceable agreement. However, this section does demonstrate the value of negotiations in generating information about the other side's interests and capabilities to inform future negotiations and agreements. Further, the analysis of the information variable at Reykjavik confirms that incomplete information at negotiations can impede negotiations. Given that incomplete information imposes constraints on every negotiation, the emphasis here is on the role of negotiations in generating information. With high levels of skepticism about the prospect of an international agreement in cyberspace, one can envision multiple rounds of negotiations without an agreement. However, those negotiations, like Reykjavik, are still valuable and should not be regarded as failures.

Negotiations themselves can be fruitful in revealing previously private information. As the U.S. delegation reflected upon the negotiations at Reykjavik, it understood the immense progress that was made in a variety of domains. The U.S. participants also realized the consequence of the concessions the Soviets presented: the Soviets had revealed their bottom-line and would be unable to retreat from that position now that the U.S. was made aware. Specifically, the Soviets agreed to cut strategic weapons in half, accepted the U.S. definition of strategic weapons, approved the elimination of missiles grounded in Europe, and agreed to a deployment freeze on short-range INF systems.[72] The Soviets also clearly demonstrated that they would not accept anything less than a "ten-year period of nonwithdrawal and strict adherence to the terms of the ABM Treaty during that period."[73] The Reykjavik Summit succeeded, from a U.S. perspective, in bringing out Soviet positions that had otherwise been concealed.[74]

[72] Shultz. *Turmoil and Triumph: My Years as Secretary of State*, 759.
[73] Ibid., 768.
[74] Ibid., 775.

The negotiations at Reykjavik therefore served to lay the groundwork for future progress. Secretary Shultz recognizes the significance of this reality: "all the things that were worked out there eventually came to pass, so it was a very important meeting in this sense."[75] "In the Nitze negotiations," Shultz continues, "they basically identified all the key things that became eventually the INF Treaty and the START Treaty. And Roz's negotiations, for the first time, she got Soviet agreement that human rights would be a recognized, regular item on our agenda. That was a real breakthrough."[76]

Paul Nitze and Roz Ridgway, U.S. diplomats, led breakout sessions on arms control and on all other topics, respectively, during the Reykjavik Summit where these breakthroughs were made. Therefore, even though Reykjavik did not lead to an agreement on the reduction of ballistic missiles, it did serve many other critical purposes. This concept is especially relevant to cyber as it demonstrates the value of the negotiating process irrespective of the outcome. Bringing nations together to debate regulations in cyberspace can help to reveal where state interests align or may be brought into alignment.

In addition to revealing information, one of the relevant elements at Reykjavik was the incomplete nature of information. The U.S. delegation arrived at Reykjavik with inaccurate information about the Soviet intentions and anticipated negotiating position. The information the Central Intelligence Agency (CIA) provided to Reagan and his close advisors was of little import. Shultz acknowledges in his memoir that poor intelligence about the Soviet Union, a closed and highly illusive regime, was relatively common. Yet, in the case of Reykjavik, the intelligence was

[75] Secretary George Shultz, interviewed by Rachel Hirshman.
[76] Ibid.

particularly meager. He candidly notes that "the message we received from the CIA about what to expect in Reykjavik was exactly contrary to what transpired."[77] As a result, the U.S. was initially ill-prepared to react and respond to Gorbachev's sweeping concessions.

The Soviets similarly did not have perfectly reliable information about the U.S., but they were well-endowed with accurate intelligence about the U.S. posture at Reykjavik. In materials presented to Gorbachev in preparation for the Reykjavik Summit, the briefers acknowledge that "Given the lack of reliable information about the opponent, it is not to be excluded that the information about certain types of weapons might be somewhat exaggerated."[78] Nevertheless, the documents illustrate precise estimates of the technical capabilities and timelines for U.S. programs in a variety of disciplines.

Another factor influencing incomplete information was the unpredictability of the ways in which SDI could develop.[79] This unpredictability meant that the Soviets were forced to develop a large variety of contingency plans in case the U.S. successfully developed and deployed a missile defense system. Similarly, while the Soviet scientists communicated their skepticism about the technical feasibility of such a system at the time, they did not have perfect knowledge of U.S. capabilities.[80] Therefore, in this world of imperfect information, the Soviets had to act based on the assumption of the worst possible case of a successful SDI program. In this vein, Gorbachev's insistence that reductions in offensive missiles were intrinsically linked to constraints on defensive

[77] Shultz. *Turmoil and Triumph: My Years as Secretary of State*, 780.
[78] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament.
[79] Lambeth and Lewis. "The Kremlin and SDI."
[80] David Holloway, "The Strategic Defense Initiative and the Soviet Union," *Daedalus* 114, no. 3 (1985): 267.

programs becomes clear.[81] The Soviets were forced to pursue a negotiating position at Reykjavik that rested on incomplete information and unpredictability about the future of the SDI program.

The reality of incomplete information is even more extreme in cyberspace. State operations, capabilities, and intentions are clouded in secrecy. It is very difficult to have a general understanding of another state's cyber activities without performing covert espionage which itself generally involves cyber operations. In negotiations, the participating states have bargaining incentives to withhold information about their own capabilities or intentions. In cyberspace, these incentives are derived from desires well beyond negotiations. Revealing sources of information about another state's cyber operations or even the information necessary to credibly communicate attribution of an attack has severe implications for a state's own capabilities and ability to conduct cyber operations in the future.

Additionally, the incentives to guard vulnerabilities and exploits are immense. Unlike in the nuclear domain where nuclear weapons and ballistic missiles can be reproduced, once a vulnerability is exploited in cyberspace, patches can be created to invalidate the exploit on all systems that deploy the patch. Certainly there are circumstances where organizations for a variety of reasons do not implement patches and are still vulnerable. But, for the most part, cyber tools are a single use instrument. This characteristic of cyber tools heightens the need for secrecy and exacerbates the challenge of incomplete information during negotiations and for a verification scheme.

The most important lessons drawn from the Reykjavik Summit in the context of information pertain to negotiations as generators of information and the challenges posed by incomplete information. These characteristics of the negotiations both have the potential to be influential in

[81] Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament.

negotiations, but are not necessarily deterministic of the outcome of negotiations. Therefore, while it is important not to overlook the role that they played at Reykjavik, they are less relevant in explaining the conditions most likely to lead to an international agreement in cyberspace.

Summary

This chapter analyzed the relevant conditions that impeded and strengthened the prospects of an agreement to eliminate ballistic missiles at Reykjavik. The variable of greatest significance for the outcome of the negotiations was state interests. Specifically, at Reykjavik neither side was willing to move beyond its bottom line and compromise in any way on its position on SDI and the ABM Treaty. The misalignment of state interests with the U.S. seeking Soviet recognition of human rights and the Soviet demanding that the U.S. cease SDI research and development at all costs also constrained the window of cooperation. In addition to state interests, domestic politics also greatly influenced the outcome of the negotiations. Soviet domestic pressures from a crippled economy and a desire to preserve Soviet superpower status and U.S. democratic pressures contributed to the leaders' unwillingness to compromise on their bottom line. Finally, the analysis of the role of information during the negotiations exposes the benefits and importance of negotiations regardless of their outcome in generating information for future progress.

The analysis of this chapter also illustrates shortcomings of the Reykjavik Summit case study as the role of the private sector, elements of the international system, and verification and enforcement were of limited relevance to the negotiations. This chapter further argues that the challenges posed by the security dilemma in the nuclear domain imply that the security dilemma in cyberspace will play a prominent, likely adverse, role in the negotiations for an international agreement in cyberspace. However, the security dilemma itself was not deterministic of the outcome at Reykjavik. Nonetheless, the synergy of the variables discussed illustrates the conditions

that are likely to be most influential in cyberspace if nations are brought to the negotiating table. The significant barrier of the lack of reciprocal concessions, domestic pressures, and negotiations as generators of information are the most important lessons derived from the Reykjavik Summit case study.

Chapter 5 The Chemical Weapons Convention: An Effective Ban on a Weapon of Mass Destruction

The Chemical Weapons Convention (CWC) and the negotiations that produced it can inform the prospects of international agreements in cyberspace in many ways. This chapter addresses the most significant determinants of the outcomes of negotiations and their potential applicability for cyberspace. The CWC negotiations are, as with previous chapters, assessed according to five variables: technology, geopolitical dynamics, state interests, domestic environments and information. Lessons extracted from the treatment of the technology, from the cohesion of state interests, and from geopolitical developments are the most salient in supporting this thesis' argument. Each variable is analyzed in kind with its relative weight to the outcome of the negotiations also assessed.

First, this chapter maintains that the efforts of the negotiators of CWC to ensure the treaty accounted for the dual-use nature of chemicals and the fast pace of technological development led to widespread support and the success of negotiations. Second, the commitment by the U.S. and the Soviet Union to bilateral negotiations and reductions facilitated agreement on CWC. Third, when it became critical to the outcome of the negotiations, nations were willing to make the necessary concessions on their positions to arrive at a mutually beneficial agreement. Fourth, the cooperation and advocacy of the chemical industry played an important role in facilitating negotiations that preserved its interests and ensured its cooperation in implementing the agreement. Last, the CWC demonstrates the political will of nations to engage in complex negotiations to achieve acceptably intrusive verification measures.

Setting the Stage

The history of the use of chemical weapons (CW) spans centuries. Toxins have long been used in warfare to incapacitate the opponent. In 1675, 1874, and 1899, various nations agreed to limit if not strictly prohibit the use of chemical weapons.[1] Yet, these regulatory attempts proved ineffective during World War I. By the end of the war, around 124,200 tons of chemical agents had been deployed and over a million soldiers were wounded or died as a result of these chemicals.[2] The use of CW on a massive scale, combined with a pervasive understanding of the cruelty of CW, prompted the international community to negotiate the 1925 Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, also known as the 1925 Geneva Protocol.[3]

The 1925 Geneva Protocol, while an important step towards the elimination of chemical weapons, had significant shortcomings that precluded it from substantially shaping international behavior on CW. Importantly, the U.S. did not ratify the protocol until 1975 during negotiations for the CWC.[4] The absence of the U.S., a large producer of CW, hindered the efficacy of the Protocol.

Additionally, some countries that did sign the Protocol did so with reservations. The two common reservations communicated by states were that they did not consider themselves to be

[1] "Origins of the Chemical Weapons Convention and the OPCW," September 12, 2014. https://www.acs.org/content/dam/acsorg/events/program-in-a-box/documents/2016-global-security/cw-history.pdf; and Geneva Protocol, "Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare," *Signed at Geneva, June* 17 (1925).
[2] United States, and Harry Lorenzo Gilchrist. *A comparative study of World War casualties from gas and other weapons* (Washington, D.C.: Govt. Printing Office, 1928).
[3] Bernauer, *The Chemistry of Regime Formation: Explaining International Cooperation for a Comprehensive Ban on Chemical Weapons*, 18.
[4] David A. Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," *Yale Journal of International Law* 15 (1990): 17.

bound by its provisions if they were involved in an armed conflict against a state that was not party to the protocol, or if chemical weapons were used they maintained the right to respond in kind.[5] Further, the Geneva Protocol banned the use of CW and biological weapons (BW) only in war but did not prohibit their development or stockpiling. As a result, the Geneva Protocol was widely regarded as a no first-use agreement.[6]

The strength of the international norm created by the Geneva Protocol was eroded as violations occurred and nations did not experience consequences for their actions.[7] The use of riot control agents (RCAs) and herbicides by the U.S. was also widely seen as undermining the norm against CW and BW embodied by the 1925 Geneva Protocol. Nevertheless, the CWC explicitly refers to the Protocol in its preamble.

Both during the period between World War I and World War II and during World War II, nations continued to develop and innovate their CW programs. However, despite the high anticipation of their use, CW were not used in the European theater during WWII.[8] The reason for their non-use in WWII is passionately debated but such theories are beyond the scope of this thesis.[9] Throughout the Cold War, the U.S. and the Soviet Union maintained large stockpiles of CW and the commercial chemical industry grew rapidly.

---

[5] "Genesis and Historical Development," *Organisation for the Prohibition of Chemical Weapons,* https://www.opcw.org/chemical-weapons-convention/genesis-and-historical-development/.

[6] This was especially true after the use of CW by Italy in the Ethiopian War and the use of both CW and biological weapons by Japan in China. Thomas Bernauer. "Warfare: Nuclear, Biological, and Chemical Weapons," in *Managing Global Issues: Lessons Learned,* edited by Chantal de Jonge Oudraat, P.J. Simmons, and Jessica Tuchman Mathews, Carnegie Endowment (2001), 16.

[7] Patricia Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," Doctoral diss., Universität Wien, (2011): 41.

[8] "Origins of the Chemical Weapons Convention and the OPCW."

[9] See Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Organization* 49, no. 1 (1995): 73–103; Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention."; and Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success."

In this environment of non-use but with the persistence of CW programs in various nations, the international community discussed avenues of international coordination to address the threats posed by CW and BW. Noticeably, the Warsaw Treaty member states noted that "One of the main objectives of their foreign policy is the speediest completion of talks on a full and universal ban on chemical weapons."[10] Similarly, official U.S. government correspondence at the time illustrates "The United States is formally committed to eliminating chemical warfare."[11]

Arms control negotiators concluded that it was most efficient and effective to first negotiate an agreement on BW with no standing verification provisions because such an agreement attracted broad international consensus, concerned a weapon with less military value, and did not hinge on verification measures, and then deal with CW afterwards.[12] Thus, the Biological and Toxins Weapons Convention (BTWC) signed in 1972 explicitly required that the signatories continue negotiations on CW, which were easier to verify. The preamble of the BTWC reads:

> "Recognising that an agreement on the prohibition of bacteriological (biological) and toxin weapons represents a first possible step towards the achievement of agreement on effective measures also for the prohibition of the development, production and stockpiling of chemical weapons, and determined to continue negotiations to that end."[13]

[10] Soviet Embassy, Information Department, Statement on a Ban on Chemical Weapons, News and Views from the USSR (Mar. 26, 1987): 1.

[11] *Memorandum for Zbigniew Brzezinski from Jessica Tuchman regarding U.S. approach to a chemical weapons treaty with the Soviet Union*. National Security Council, 7 June 1977. *U.S. Declassified Documents Online*, http://tinyurl.galegroup.com/tinyurl/5wj8E0. Accessed 15 Mar. 2018.

[12] There were also discussions that finalizing a prohibition on BW would help to prevent states from realizing how effective BW could be. Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," 18.

[13] *Convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction*, Washington, 10 April 1972, *United Nations Treaty Series*, vol. 1015, p. 163, available from https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280101653.

Comprehensive negotiations towards a CWC that aligned with the above obligation did not seriously begin until 1980 in the forum of the UN Conference on Disarmament. Various geopolitical and strategic factors shaped the negotiations for the next twelve years. Progress towards an agreement was supported by multilateral efforts at the Conference on Disarmament, bilateral negotiations between the U.S. and Soviet Union, and contributions by many nations. The Conference on Disarmament adopted a "rolling text" that was modified iteratively and reflected principles and text not formally agreed to.[14] The critical disagreements reflected in the "rolling text" were ultimately resolved or discarded and the text of the CWC was finalized under the chairmanship of Ambassador Adolph von Wagner of Germany.

The negotiations on CWC were concluded in 1992 and the agreement opened for signature in January 1993. The CWC entered into force on April 29, 1997 and currently has 192 signatories.[15] Egypt, North Korea and South Sudan are the only nations in the world not to sign or ratify the treaty, while Israel has signed but not acceded to the treaty.[16] The CWC prohibits the development, production, acquisition, retention, stockpiling, transfer, and use of chemical weapons.

While there is a consistent debate in the literature about the effectiveness of the CWC, especially in light of the continued use of CW in the Syrian Civil War, the CWC is an important achievement that has significantly reduced the number of CW in the world and reaffirmed the

[14] Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," 4.
[15] Daryl G Kimball, "The Chemical Weapons Convention (CWC) at a Glance." January 2018. https://www.armscontrol.org/factsheets/cwcglance.
[16] Ibid.

international norm against the use of such weapons.[17] As of March 2018, the vast majority of nations possessing CW had completed the destruction of their Schedule 1 chemicals with only the U.S. and Syria with stockpiles remaining.[18] As with the previous chapter, the following sections analyze the details of the CWC negotiations and connect the lessons learned during the negotiations back to cyberspace.

Technology

Unlike nuclear-armed ballistic missiles in the Reykjavik Summit case study, chemical weapons have some similar technological properties to cyberspace tools. Chemical weapons and cyber weapons are both relatively easy to use, are dual-use, can be acquired cheaply, are subject to fast-paced technological development and innovation, and perhaps most interestingly are regarded as instrumental tools in conflict at a tactical level but not as decisive weapons.[19] These characteristics have extensive implications for the regulation of their use or purpose. As such, an understanding of how the nations addressed the challenges that arose due to these characteristics in the CWC negotiations can help to inform negotiators in cyberspace how to address analogous obstacles (*e.g.*, with regard to the intent of a given activity or program). While all of these defining traits are important and relevant to the ensuing discussion, this section emphasizes the dual-use issue and the pace of technological development as those proved to be the most controversial in CWC negotiations and are even more acute in cyberspace. The question of the security dilemma

[17] David P. Fidler, "The Chemical Weapons Convention After Ten Years: Successes and Future Challenges," *ASIL Insights* 11, no. 12 (2007), https://www.asil.org/insights/volume/11/issue/12/chemical-weapons-convention-after-ten-years-successes-and-future.
[18] Kimball, "The Chemical Weapons Convention (CWC) at a Glance."
[19] Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," 8. Some scholars do regard cyber weapons as decisive. For this opposing perspective, see "The Military Balance 2010," The International Institute for Strategic Studies, 2010. https://www.iiss.org/en/publications/military-s-balance.

is not elaborated upon in this section because there existed effective defenses against chemical weapons that made the security dilemma inconsequential.

The CWC deals with the dual-use issues and pace of technological development through a General Purpose Criterion (GPC).[20] This clause is meant to encapsulate the acknowledgement by the signatories of the treaty that there are both prohibited and acceptable uses of chemical weapons. In defining chemical weapons, Article II of the CWC reads: "Toxic chemicals and their precursors, **except where intended for purposes not prohibited under this Convention, as long as the types and quantities are consistent with such purposes.**"[21] The bolded portion of the clause is what is commonly referred to as the GPC, whose ambiguity allows the treaty to still provide such restrictions even in the event of technological development and innovations in chemicals. And given that the convention completely prohibits CW, this phrase ensures that toxic chemicals as defined by the convention can be used only for permitted purposes regardless of when and where they are developed.

The dual-use challenge was widely recognized at the time and in retrospect as decisive in the negotiations. Negotiators and scholars alike argued that a CWC was only to be deemed acceptable by nation states if the provisions of the treaty did not put an undue burden on the commercial sector of the chemical industry.

Managed access provisions and principles are derived from this necessity. David Koplow, a lawyer who specializes in international law, noted that "the challenge for CW arms control . . .

[20] See Thomas Bernauer. *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*, New York, United Nations, 35.
[21] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction*, Geneva, 3 September 1992, *United Nations Treaty Series*, vol. 1974, p. 45, available from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-3&chapter=26&clang=_en.

will be to develop a system for the effective regulation of the weapons capability of the chemical industry in a fashion that does not unduly inhibit the commercial operations of this important, dynamic segment of the international economy."[22] Koplow's assessment further illuminates the transnational nature of the chemical industry which only heightens the challenge.

U.S. Vice President George H. W. Bush likewise stressed the dual-use issue: "some chemicals with peaceful utility are structurally similar to some chemicals used in warfare."[23] Bush declared the U.S. position at the time that "the principal criterion for distinguishing between permitted and banned activities would be the purpose for which an activity is being conducted."[24] Ultimately the language contained in the treaty to distinguish between the two activities was not as explicit but was of a similar premise.

Given the similarity between civilian chemicals and chemicals used in warfare, it was not possible just to ban and destroy categories of chemicals themselves. The solution, therefore, was to categorize CW "based on the properties of a given chemical (toxicity or precursor to a toxic chemical), purpose of use, and consistency of types and quantities of chemicals with such purposes."[25] The GPC encapsulates this conceptualization of how to distinguish between acceptable and unacceptable uses of chemicals.

The CWC also details scheduled and non-scheduled chemicals that are each subject to specified provisions. Schedule 1 chemicals, for example, pose the highest risk to the objectives of the convention and have very limited accepted peaceful uses. Schedule 2 and Schedule 3 chemicals

[22] Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," 35.
[23] Vice President Bush, "U.S. Proposes Banning Chemical Weapons," *Current Policy No. 566*, U.S. Department of State, Bureau of Public Affairs, Washington, D.C.
[24] Ibid.
[25] Mohamed Daoudi and Ralf Trapp. "Verification under the Chemical Weapons Convention." In *Verifying Treaty Compliance* (Springer, Berlin, Heidelberg, 2006): 78.

have more commercial/peaceful purposes and are subject to less stringent declaration and verification requirements than Schedule 1 chemicals. Further, the declaration and verification regime surrounding non-scheduled chemicals, predominantly discrete organic chemicals (DOCs) or chemicals containing phosphorus, sulfur or fluorine (PSF), is more focused on the chemical plants than the chemicals themselves. The GPC and the requirements surrounding scheduled and non-scheduled chemicals compose the core of the CWC's efforts to delineate between acceptable and unacceptable uses of chemicals.

Through these provisions, the CWC regulates the intent of use rather than the toxicity of the chemical or the particular chemical being used.[26] A caveat to this claim is that the Schedules contained within the treaty do explicitly detail classes of chemicals, as well as toxins regarded as most threatening to national security, imposing more stringent restrictions on those chemicals than others with predominantly peaceful uses.

An important distinction between the CWC and cyberspace in this context of regulation on use is how the restrictions are framed. In the case of cyber, an analogous international agreement would likely start by assuming that all activities are allowed and then proceed to explain what specific activities are prohibited as an exception to that rule. The CWC is the opposite as it begins by assuming that all chemicals are inherently harmful and then elaborates on the type and quantity of chemicals that are accepted under the provisions of the agreement. Specifically in Article II, Section 9, the CWC explicitly outlines the uses of chemicals that are permitted under the terms of

[26] Alexander Kelle, "Developing Control Regimes for Chemical and Biological Weapons," *The International Spectator* 32, no. 3–4 (July 1, 1997): 138, https://doi.org/10.1080/03932729708456788.

the treaty, to include "industrial, agricultural, research, medical, pharmaceutical," and law enforcement uses.[27] Therefore, the restriction on use in the CWC can also be understood as an allowance of particular uses with the understanding that everything else is prohibited. The significance of this distinction is that it is practically much more difficult to regulate use when the assumption is that everything is acceptable. Creative individuals could conceive activities that circumvent those enumerated in an international agreement. This distinction, however, does not contradict the conclusions made but instead illustrates that the approach to regulation in cyberspace based on use will be different and likely more difficult to implement than in the case of CWC given the differences in the technology.

Nonetheless, this resolution of the dual-use challenge in the CWC case has significant implications for cyberspace. It not only indicates that classifications based on intent or purpose can be accepted by the international community, but it also may mitigate concerns that the inherent dual-use nature of cyberspace is a treaty killer. As such, arguably one of the most significant lessons extracted from the negotiating history of the CWC is that an international treaty can carefully be constructed so as to safeguard peaceful uses of CW while still banning inadmissible uses.

Additionally, the negotiations for international agreements in cyberspace must take seriously the question of how the resulting agreement will be able to adapt to new technological developments. The CWC similarly addressed this challenge. The GPC, in addition to helping distinguish acceptable uses of chemicals from unacceptable uses of chemicals, also maintains a level of flexibility to allow the treaty to account for changes in science and technology. In addition to the

[27] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction,* Article II.9.

GPC, the CWC explicitly bans any future development of CW. There was and still is the theoretical possibility that countries would cheat and continue to develop weapons.[28] Yet, it is feasible and in the interest of many nations to discontinue development of weapons due to high costs, declining use of the technology, and reputational concerns.[29]

Importantly, however, the environment of cyberspace makes such a blanket elimination of development activities complicated. First, the very same tools, processes, and infrastructure used to develop cyber weapons are used by corporations themselves to assess the security of their own products and systems. The same exploit built by the National Security Agency (NSA) may also be built by a private corporation to test that its systems cannot be penetrated or affected by such an exploit. As a result, an international treaty to ban future technological development by nation states would fail to account for the development within the private sector that results in the same technology outcomes as the public sector. Second, cyber weapons are notoriously clouded in secrecy and it is very difficult to positively confirm that development is not taking place until the results of the development are made public.

Secrecy was certainly an issue with CW programs, but nations were willing to sacrifice CW for a variety of other reasons, diminishing the relative importance of secrecy.[30] For example, Brad Roberts, director of the Center for Global Security Research at Lawrence Livermore National

[28] Jean Pascal Zanders, "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications," *Revue Belge de Droit International / Belgian Review of International Law* 26 (1993): 275.
[29] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 119.
[30] William H. Webster (1989). Testimony. U.S. Senate, Committee on Governmental Affairs, *Global Spread of Chemical and Biological Weapons: Assessing Challenges and Responses.* 101st Congress, 1st sess., February 9. Washington, DC: U.S. Government Printing Office: 11.

Laboratory, acknowledges that after the Cold War, there was less political and military support for secret programs in the US.[31]

But with cyber weapons, secrecy is regarded as of paramount necessity. Nations do not want to reveal their cyberspace capabilities nor any of their offensive cyber activities. In this environment, it is hard to envision any provision on development that would be both acceptable to nation states in cyber and feasible. Therefore, the CWC demonstrates that concerns about technological development in a domain with high levels of innovation can be addressed in principle. But the feasibility of such measures is contingent on there being other reasons for nations to cease development.

A plausible explanation for nations agreeing to cease CW development was the declining military value of CW.[32] Specifically, there existed strong defenses against CW despite the operational difficulties the defenses imposed on troops.[33] This meant that the military value of CW was significantly decreased and CW were even regarded as the "poor nation's atomic bomb."[34]

But the military value of cyber weapons today is markedly different from the military value of chemical weapons at the time of CWC negotiations. Cyber weapons do not face as effective defenses and have significant military value. Cyber tools can be employed to take out an enemy's command and control system or shut off its radar system, paralyzing it and shaping its operational behavior drastically.

---

[31] Brad Roberts, "The Chemical Weapons Convention and World Order." *Shadows and Substance: The Chemical Weapons Convention*, edited by Benoit Morel and Kyle Olson, Westview Press, 1993, 5.
[32] Bernauer, *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*, 13-14.
[33] Matthew Meselson, Keynote Address to the Sixth Annual Scientific Conference on Chemical Defense Research, U.S. Army Chemical Research, Development and Engineering Center, Edgewood Area, Aberdeen Proving Ground, Maryland, 13-16 November 1990.
[34] Neil C. Livingstone, and Joseph D Douglass. *CBW, the Poor Man's Atomic Bomb (*Cambridge, Mass.: Institute for Foreign Policy Analysis, 1984).

The military value of the applicable technology is a key difference between the two domains, helping to facilitate cooperation towards the CWC but likely imperiling negotiations in cyberspace. There were defenses against CW (*i.e.,* one could wear personal protective equipment against CW) that contributed to a strategic calculus which ushered in the acceptability of sacrificing CW whereas the same conditions do not necessarily exist in cyberspace.

Ultimately, the case of the CWC illustrates how a domain with similar technological challenges to those in cyberspace adopted an innovative strategy - a General Purpose Criterion - to retain flexibility in the face of technological development and innovation. The GPC also establishes how acceptable uses of chemicals are distinguished from prohibited uses. As such, these characteristics were relevant to the outcome of the negotiations. The CWC likely would not have been feasible had the dual-use issue and technological innovation not been addressed sufficiently.

Geopolitical Dynamics

There are three primary takeaways from the CWC negotiations with respect to geopolitical dynamics. First, the commitment and urgency of the major powers was critical in driving negotiations towards a CWC. Second, concerns about the growing universality and proliferation of the weapons to the developing world motivated the developed world to value CWC negotiations. Third, and related to the second point, is that the use of CW during the Iran-Iraq War increased the stakes of reaching an agreement and further motivated nations to eliminate CW as soon as they could. Each of these elements will be addressed in turn.

Perhaps of greatest consequence to the outcome of CWC negotiations was the successful cooperation of the U.S. and the Soviet Union on the issue of CW disarmament. Not only did both

nations prioritize CW on their agendas, but the nations devoted substantial time each year to bilateral negotiations.[35] As early as 1974 the two nations jointly acknowledged the intention of working together to foster a universal CW ban.[36] Subsequently, the U.S. and the Soviet Union engaged in at least eleven rounds of bilateral talks. 1989 and 1990 were the pivotal years of negotiations to ban chemical weapons because they were also the most productive years of bilateral talks.[37] The 1989 negotiations resulted in the Wyoming Memorandum of Understanding which provided a framework for the exchange of information between the two nations and for bilateral verification measures.[38] Similarly, the 1990 bilateral talks resulted in an agreement between the two nations to destroy twenty percent of their chemical weapons stocks beginning in 1992.[39]

These significant steps taken by the U.S. and Soviet Union provided other nations with a model of action and sent a clear message that the countries with the largest stockpiles of CW were committed to an international ban. The U.S. State Department acknowledged the importance of these bilateral actions at the time. In a background memo and in reference to the 1990 bilateral agreement signed with the Soviet Union, the agency stated "the bilateral destruction agreement also is important as a demonstration of the superpowers' tangible commitment to eliminate chemical weapons completely and should help accelerate completion of the Geneva negotiations on a

---

[35] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 46.
[36] Julian Perry Robinson, "The Negotiations on the Chemical Weapons Convention: A Historical Overview." *The New Chemical Weapons Convention: Implementation and Prospects,* edited by Michael Bothe et al., Martinus Nijhoff Publishers, 1998, 24.
[37] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 50.
[38] *Text of a memorandum of understanding between the U.S. and the U.S.S.R. with respect to a bilateral verification experiment and a data exchange program to deal with the prohibition of chemical weapons*. White House, 23 Sept. 1989. *U.S. Declassified Documents Online,* http://tinyurl.galegroup.com/tinyurl/5wj9R9. Accessed 17 Mar. 2018.
[39] *Agreement between the United States of America and the Union of Soviet Socialist Republics on Destruction and Non-production of Chemical Weapons on Measures to Facilitate the Multilateral Convention on Banning Chemical Weapons,* 1 June 1990, 29 ILM 934 (1990).

chemical weapons convention (CWC)."[40] The Provisional Technical Secretariat Executive Secretary Ian Kenyon likewise acknowledged the contributions of the U.S. and Soviet Union: "It is clear that the international community owes a great debt to the USA and the USSR/Russia as the CWC could not have been concluded without their joint commitment to be bound by its provisions."[41] Kenyon stresses just how consequential the U.S. and Soviet commitment to the treaty was on allowing for the CWC to come into force. The decreased importance of Cold War tensions and great power conflict in the late 80s and 90s also cultivated expanded opportunities for cooperation and engagement on the issue of CW.[42]

Beyond the demonstrated commitment of the major powers, the increased proliferation and universality of chemical weapons also played a significant role in advancing the objective of a multilateral agreement on CW. The U.S., Soviet Union, and other developed nations recognized that only if the vast majority of nations capable of or with the intention of producing chemical weapons became signatories to the treaty would chemical weapons be eliminated. They needed the cooperation of nations with CW programs and nations without CW programs alike. Specifically, Nikita Smidovich, a Soviet diplomat and Senior Political Affairs Officer at the UN Office for Disarmament Affairs (UNODA), writes "it became obvious that even if the Soviet Union and the United States were to destroy all their chemical weapons . . . such destruction would not automatically lead to a CW-free world or eliminate the possibility of these weapons being used in

[40] *Background Paper on the Following Arms Control Issues Which Are Likely to Arise in the Course of Upcoming U.S.-Soviet Summit Discussions: Nuclear Testing; Chemical Weapons; Open Skies Proposal; Conventional Armed Forces in Europe (CFE) Treaty; Strategic Arms Reduction Talks (START)*. United States: Department Of State, 1990. http://tinyurl.galegroup.com/tinyurl/5wjA65.
[41] Ian Kenyon, "The USA/USSR Arms Control Relationship and Its Impact on the CWC," *CBW Conventions Bulletin* (2006): 2.
[42] Roberts, "The Chemical Weapons Convention and World Order," 9.

current or foreseeable conflicts."[43] Therefore, despite the negotiating proceedings being dominated by the superpowers, the accession to the treaty of the rest of the world was paramount. Acquiescing to at least some of the demands of these other nations fostered their cooperation.

Proliferation also served a second purpose in augmenting the concern of the developed world and increasing their motivation to ban CW promptly. As of the writing of this thesis, six nations still possess stockpiles of CW.[44] However, the horizontal proliferation of weapons to new countries has been overtaken by modernizing CW programs within these six countries.[45] In the 20th century and still today, chemical weapons are very attractive to developing nations. Chemical weapons, they believe, could be used to counter the technologically superior nations with various weapons of mass destruction (WMD) arsenals, including nuclear weapons.[46]

In addition to the real fear of developing nations acquiring CW, the developed world also envisioned the spread of CW to terrorist organizations and non-state actors that would be much more difficult to control and influence. Koplow contends "The alarming possibility of readily available chemical arms, distributed to numerous small countries, and possibly to terrorist organizations as well, generates some of the most intractable security nightmares for the United States and the rest of the world."[47] Therefore, given the developed world's ability to dictate how much of the international system operates, the fear of proliferation gave them more impetus to seek a CWC. And this fear, coupled with the asymmetric nature of the weapon, was deemed an acute

[43] Nikita Smidovich, "The Russian and Other Perspectives." *Shadows and Substance: The Chemical Weapons Convention,* edited by Benoit Morel and Kyle Olson, Westview Press, 1993, 58.
[44] This statistic does not account for dumped munitions, old CW, and abandoned CW that are not covered by the provisions of the CWC.
[45] Jonathan B. Tucker, "The Future of Chemical Weapons," *The New Atlantis*, Number 26, Fall 2009/Winter 2010: 12. https://www.thenewatlantis.com/publications/the-future-of-chemical-weapons.
[46] Zanders, "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications," 264.
[47] Koplow, "Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention," 14-15.

threat to the security of the U.S. and other developed nations. With a stronger commitment to the objective of a ban, the likelihood of the CWC increased.

The Iraqi use of CW during the 1980-1988 Iran-Iraq War demonstrated the proliferation concerns of the major powers and was a momentous event in the course of the CWC negotiations.[48] The revelations of the Iraqi program and the use of CW against Iran was a strong catalyst to follow through on the negotiations and greatly increased the urgency of the major powers.[49] Notably, the most successful rounds of bilateral negotiations between the U.S. and the Soviet Union came in the two years immediately following the end of the Iran-Iraq War.

Additionally, the Iraqi use of CW motivated the creation of the Australia Group to harmonize the transfer of chemicals agents and precursors to CW to ensure they were not misused for chemical or biological warfare as a first step towards regulation of CW.[50] Export controls were critical because intelligence reports quickly revealed that Western chemical industries trading with Iraq contributed considerably to the development of the Iraqi CW program.[51] The West's implication in the Iraqi use struck chords in the U.S. and other nations, convincing them further of the

[48] As a result of the Iraqi use of CW, the UN established the UN Special Commission to oversee the inspection of Iraq's biological and chemical weapons facilities and to facilitate the destruction of these weapons by Iraq. Importantly, however, Iraq was not thoroughly compliant with the practices established by the commission. See United Nations Security Council Resolution 687, S/Res/687 (3 April 1991) p. 13, http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/687(1991); United Nations Report, *Report of the Executive Chairman on the activities of the Special Commission established by the Secretary-General pursuant to paragraph 9 (b) (i) of resolution 687 (1991),* S/1999/401, 9 April 1999, http://www.un.org/Depts/unscom/sres401eng.htm.

[49] Zanders, "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications," 265.

[50] Ibid., 265.

[51] See Zanders, "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications," 267; United Nations Special Commission, *Letter dated 25 January 1999 from the Executive Chairman of the Special Commission established by the Secretary-General pursuant to paragraph 9 (b) (i) of Security Council resolution 687 (1991) addressed to the President of the Security Council,* S/1999/94, 29 January 1999, http://www.un.org/Depts/unscom/s99-94.htm.

necessity of a universal ban. It especially illustrated the ineffectiveness of the current regime to govern CW and provided an indication of what could occur if a ban were not agreed to.

The consequences of the Iraqi CW program imply that with the use of cyber capabilities by nations where cyber capabilities have proliferated and whose conventional militaries are relatively weak, nation states would take international cooperation more seriously and be more likely to seek and accept an international agreement. However, an important distinction must be made; the superpowers and international community were opposed to the use of CW and in pursuit of a global ban even before the manifestation of proliferation concerns with the Iraqi use. The use of CW during the Iran-Iraq War provided the impetus for concluding the negotiations.[52] The same general taboo or principle of non-use does not exist in cyberspace. So, one could only speculate as to the level and nature of proliferation or even the circumstances of use of cyber weapons that would have to ensue for multiple states to all independently conclude that the security protections of an international agreement exceed the benefits of maintaining clandestine cyber programs.

The cooperation between the U.S. and USSR, proliferation concerns, and the Iraqi use of CW all increased the likelihood of an international agreement to eliminate chemical weapons. These factors, like their technological counterparts, were of extreme relevance to the outcome of the negotiations. Their interaction served to increase the longing for an agreement and, in the case of the Iraqi CW program and proliferation, elevate the importance of agreeing to and signing a comprehensive ban promptly.

State Interests

[52] Ian R. Kenyon and Daniel Feakes, eds. *The Creation of the Organisation for the Prohibition of Chemical Weapons: A Case Study in the Birth of an Intergovernmental Organisation*. 1st edition (The Hague : West Nyack, NY: T.M.C. Asser Press, 2007), 6.

One of the clearest differentiators between the successful CWC negotiations and the inability to reach an agreement on the elimination of nuclear-armed ballistic missiles at Reykjavik was the willingness of the states involved to sacrifice elements of their positions to advance the proposed agreement. The lack of reciprocal concessions at Reykjavik was decisive whereas nation states frequently conceded demands during CWC negotiations. As such, the presence of reciprocal concessions is the most salient element of the negotiations to the conclusions of this thesis.

This section presents the concessions made during CWC negotiations. The relative alignment of interest among the major powers and their commitment to an agreement also impacted the success of the negotiations. However, the core of this section's analysis is devoted to the existence of concessions because there is not much more to be said regarding the alignment of state interests.

There were four primary incidences of concessions. First, developing nations gave up their ability to acquire CW altogether. Second, the U.S. conceded on its insistence that riot control agents (RCAs) and herbicides be excluded from the CWC by permitting the treaty to disallow their use in warfare. Third, the U.S. retreated on its desire to maintain two percent of its arsenal for retaliatory purposes. Last, the Soviets and the Socialist bloc accepted intrusive verification measures after insisting that verification should be conducted at a national level not an international level.

Developing nations were initially opposed to the concept of a CWC because it unfairly discriminated against them. A successful CWC would ensure that they would never have an opportunity to pursue their own CW program.[53] However, other security and economic benefits of

[53] Zanders, "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications," 267.

the proposed treaty and the limited value of CW programs led most of the developing world to value the prospect of a treaty over a national CW program.

Particularly, only in joining the treaty could nations reap the benefits of chemical trading. Otherwise, nations would be sidelined from this sharing of knowledge and technology.[54] Thus, the calculus was that the security and economic benefits of signing the treaty would exceed those of remaining outside. Most of the world's nations had peaceful chemical sectors at the time that would be hindered by refusing to the sign the treaty. The existence of key advantages to the treaty illustrates that concessions are more likely under conditions where there are acceptable alternatives to what is being sacrificed. That is, reciprocal concessions are more achievable when trade-offs can be made and the circumstances are not all or nothing.

Another controversial element of the negotiations was the U.S. insistence that RCAs and herbicides be excluded from the regulated chemicals in the CWC. The U.S. sought to maintain the flexibility to produce and store these chemicals because of their widespread domestic uses and thus viewed their inclusion in the treaty as detrimental to that end.[55] The U.S. also demonstrated the military utility of herbicides by using the chemical in large quantities during its war in Indochina in the 1960s.[56]

Likely in response to the U.S. use of herbicides, eighty nations adopted a formal definition of chemical weapons at the UN General Assembly (UNGA) that included RCAs and herbicides.[57]

---

[54] Bernauer, "Warfare: Nuclear, Biological, and Chemical Weapons," 33.
[55] Bernauer, *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*, 74.
[56] Ibid., 15.
[57] United Nations General Assembly Resolution 2603, *Question of Chemical and Bacteriological (Biological) Weapons*, A/RES/2603(XXIV)A (16 December 1969), available from https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/257/37/IMG/NR025737.pdf?OpenElement.

Predictably the U.S. opposed the resolution and many Western nations abstained. A memorandum to U.S. President Lyndon B. Johnson from Secretary Nicholas deB Katzenbach in 1967 also explicitly illuminates the U.S. reservations about RCAs and herbicides. Secretary Katzenbach recommended that Johnson publicly announce a "no first use" policy "with regard to chemical and biological warfare, with the exception of riot gases and herbicides."[58] Throughout debates within the U.S. about ratifying the Geneva Protocol, a ubiquitous argument was exactly this - the U.S. could accept a no first-use policy so long as RCAs and herbicides were excluded.

However, despite U.S. reservations, the administration accepted a final draft of CWC that explicitly prohibits the first use of RCAs and herbicides as a "method of warfare."[59] The CWC does however permit the use of RCAs and herbicides for specified purposes such as research or for "law enforcement including domestic riot control purposes" [60] - the primary method of use the U.S. was concerned with.[61] In a correspondence to Henry Kissinger, Matthew Meselson and Paul Doty illustrate this shift in the U.S. position as early as 1972. In addressing the desired Senate ratification of the 1925 Geneva Protocol, the authors communicate the marginal value of such RCAs and herbicides and propose a statement by the U.S. that conveys an understanding that "the applicability of the Protocol to riot control agents and herbicides should not be allowed to stand in

[58] Nicholas deB Katzenbach to Mr. Walt W. Rostow, "Policy on Chemical and Biological Weapons," February 20, 1967, Department of State, Washington, D.C.
[59] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction,* Article I.5.
[60] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction,* Article II.9.
[61] There is an ongoing debate as to the exact interpretation of "law enforcement" purposes as the United States tends to view law enforcement differently than the rest of the world. Most states agree that the use of RCAs is prohibited in international conflict zones altogether. The U.S., on the other hand, regards the use of RCAs for very specific purposes in armed conflict zones to be acceptable and in accordance with the CWC. Executive Order 11850, signed by President Gerald Ford, outlines the U.S. position on the use of herbicides and RCAs during armed conflict. Gerald Ford, "Executive Order 11850 -- Renunciation of certain uses in war of chemical herbicides and riot control agents," National Archives, 1975.

the way of United States ratification of the treaty or of progress toward further constraints on chemical and biological warfare."[62]

The U.S., throughout negotiations of the CWC, similarly conceded on its position to maintain a small retaliatory force. Immediately following the release of the Wyoming Memorandum of Understanding, President George H. W. Bush presented a U.S. proposal for the elimination of CW that included a provision for the U.S. to retain two percent of its CW arsenal until all other states also took measures to reduce their stockpiles.[63] The common interpretation of this proposal was that the U.S. would refuse to destroy all of its CW until all other states did so as well. Concerns about proliferation, especially as a result of the Gulf War of 1991, led the U.S. to sacrifice insistence on maintaining two percent of its stockpile to provide more precipitous conditions for a multilateral agreement on CW.[64] President H.W. Bush publicly announced "we are formally forswearing the use of chemical weapons for any reason, including retaliation, against any state, effective when the convention enters into force, and will propose that all states follow suit."[65]

The last concession that was made and that contributed to the success of CWC negotiations was the Soviet Union and the Socialist bloc agreeing to intrusive verification measures, including challenge inspections. Specifically, "The Socialist countries . . . regarded national means of verification as the principal tool to ensure compliance with the treaty."[66] National means are by their nature non-intrusive and do not necessitate cooperation. The U.S., on the other hand, regarded

---

[62] Paul Doty and Matthew Meselson to Dr. Henry A. Kissinger, May 16, 1972, Department of Chemistry, Harvard University.
[63] Daily Bulletin of the US Mission to the UN in Geneva, 26 September 1989.
[64] Robinson, "The Negotiations on the Chemical Weapons Convention: A Historical Overview," 29.
[65] George H. W. Bush, "Statement on Chemical Weapons," May 13, 1991. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=19575.
[66] The Socialist Countries at the Conference on Disarmament were Bulgaria, Czechoslovakia, German Democratic Republic, Hungary, Mongolia, Poland, Romania, and the Union of Soviet Socialist Republics. Bernauer. *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*, 21.

international means of verification as "a prerequisite for the conclusion of a comprehensive treaty."[67] The international means proposed by the U.S., such as on-site inspections, were inherently intrusive.

In the 1980s, the Soviet position began to shift, and it molded its position to be more accepting of international verification measures and less insistent on national measures being the way forward. 1986 and 1987 proved to be pivotal years in resolving the verification dispute. The Soviets explicitly acknowledged their acceptance of on-site inspections, including challenge inspections, and verification of adherence to the treaty: "the Warsaw Treaty member-states stand for imposing the toughest system of verification, including international verification, to monitor the compliance of the signatory states with their commitments under the convention."[68] Prior to these years, the Soviets and Socialist countries had contended that these verification measures were too intrusive.[69]

Thomas Bernauer, a former researcher at UNODA, attributes this shift in position to internal changes within the Socialist countries.[70] In a speech at the Conference on Disarmament in 1987, Soviet Foreign Minister Eduard Shevardnadze confirmed the Soviet willingness to accept more intrusive, on-site inspections but stressed reciprocity. Shevardnadze communicated "As you can see, we are expanding the area of confidence to the maximum by opening up the territory of the Soviet Union to inspections. However, complete confidence naturally presupposes complete

[67] Ibid., 21.
[68] Soviet Embassy, Information Department, Statement on a Ban on Chemical Weapons, News and Views from the USSR, 2.
[69] Bernauer, *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*, 49.
[70] Ibid., 52.

reciprocity."[71] He also reiterated throughout his speech that the shift in the Soviet position was a result of "new political thinking," supporting Bernauer's conclusions.[72] Ultimately, the differing positions of nations on verification measures was largely resolved by concessions made on the part of the Socialist countries to accept intrusive and mandatory inspections they were previously opposed to.

U.S. and Soviet concessions proved pivotal in making possible a comprehensive ban on CW. Had sacrifices not been made and been met by concessions from other parties, a stalemate could have prevailed on various fronts. Specifically, the Soviets were adamant in public speeches at the Conference on Disarmament and in correspondence with the U.S. administration that they would not accept a U.S. proposal to maintain two percent of their stockpile. Had the U.S. not conceded on this point, it is entirely possible that the result would have closely resembled that of Reykjavik. Therefore, this variable of reciprocal concessions was of critical relevance to the outcome of the negotiations. Its presence in the CWC case study where the outcome was a successful treaty and its absence at Reykjavik where negotiations faltered demonstrates, in the context of this thesis, its considerable predictive weight.

Domestic Environments

There was widespread international support for a chemical weapons ban and specifically strong domestic support in the U.S. for a ban. Therefore, the concept of public support is not particularly interesting to the analysis of the CWC. Instead, this section emphasizes the involvement of the private sector in the negotiations and the domestic impediments faced by the U.S. and Soviet governments to confidently commit to a universal ban.

---

[71] United Nations, Conference on Disarmament, *Final record of the 428th plenary meeting, held at the Palais des Nations, Geneva*, CD/PV.428 (6 August 1987), available from https://digitallibrary.un.org/record/143615/.
[72] Ibid.

An analysis of the participation of the private sector in the outcome of the CWC negotiations is highly informative for cyberspace. In fact, the stake that the private sector has in an international agreement is higher in cyberspace than it was for CW. The private sector owns and operates the majority of infrastructure that makes up cyberspace. The government also leverages the private sector for its operations. Therefore, if an agreement does not have the nod of approval or explicit cooperation from the private sector, it is unlikely that nation states would regard the treaty as desirable. Notably, this is true only in nations where there really does exit an independent private sector. In the CW domain, the governments and the private sector were able to successfully devise and negotiate a solution to the CW problem that was deemed acceptable by all parties involved.

Importantly, the chemical industry was allowed to contribute its viewpoints to the negotiations.[73] It was the nation states who argued for the consideration of the industry in negotiations. The governments acknowledged the importance of its cooperation. After all, with a dual-use technology, it was hard to explicitly separate peaceful uses from prohibited uses.

Secretary Shultz even stated "achieving effective control, while avoiding unworkable measures that place an unfair burden on our industry, is a serious and difficult challenge."[74] The chemical industry could not and would not be overlooked. According to Patricia Kröll, "The regime came into existence only because representatives of the chemical industry support it. They also influenced the states' negotiating position."[75]

---

[73] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 50.

[74] *Letter to Senator William Cohen (R-Maine) from Secretary of State George Shultz Concerning Measures to Prevent the World-Wide Spread of Chemical Weapons*. United States: Department Of State, 1988. http://tinyurl.galegroup.com/tinyurl/5wj7o3. 1.

[75] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 10.

The industry was highly active and publicly vocal. In fact, the industry likely viewed the CWC as an opportunity to rebound from the negative perceptions of companies who produce and sell chemicals. After the use of CWs in Vietnam, the industry acquired the reputation of "merchant of death,"[76] and DuPont, a leading chemical company, even changed its famous slogan to remove the word "chemistry."[77] It was not only the governments who sought the participation of the chemical industry; the commercial companies themselves wanted to cooperate and be seen as supportive of a comprehensive ban.

The U.S. Chemical Manufacturers Association, the European Chemical Industry Council, and the Japan Chemical Industry Association all publicly announced their support for the CWC. Yet, in doing so, the industry sought to ensure that the verification measures agreed upon would not place an undue burden on its innovation and development. The industry and governmental officials were concerned that intrusive verification measures would lead to the espionage of or unwanted release of proprietary information that is threatening to business and operations.[78]

This concern about the espionage of "confidential business information" (CBI) was mitigated by the nature of the inspections regime agreed upon.[79] An international forum of the commercial sector was created after the Canberra Conference to help shape the language of the treaty on inspections to protect CBI.[80] And given the nature of the CWC inspections regime, the only

[76] Wiznowski, "Opting Out of the Iron Triangle: The US Chemical Industry and US Chemical Weapons Policy," 331.
[77] Offit, *Pandora's Lab: Seven Stories of Science Gone Wrong*, 222.
[78] Kathleen C. Bailey, "Problems with the Chemical Weapons Convention." *Shadows and Substance: The Chemical Weapons Convention*, edited by Benoit Morel and Kyle Olson, Westview Press, 1993, 31.
[79] United States Congress, Office of Technology Assessment, The Chemical Weapons Convention: Effects on the U.S. Chemical Industry, OTA-BP-ISC-1O6 (Washington, DC: U.S. Government Printing Office, August 1993): 43.
[80] Ibid., 11.

circumstance under which a commercial plant would be inspected is through a challenge inspection.

However, no challenge inspections have taken place as of the writing of this thesis, and the restrictions for bringing on and conducting a challenge inspection are complex.[81] There are many criteria that have to be met in order to levy a challenge inspection, and there are various authorities that have the power to monitor and even prevent the use of challenge inspections.[82] In this context, it would be very unlikely for the chemical industry to be subject to intrusive inspections that would jeopardize CBI, suppressing the concern of industrial espionage. Another motivation of the chemical industry, especially in the Western world, was to recover from being implicated in the Iraqi CW program, "to get rid of its reputation as a dirty business."[83] Overall, the commercial chemical sector was very pleased with the outcome of the negotiations and the final draft of the CWC.

Beyond the importance of private sector involvement, the domestic environment of the various nations involved also shaped the CWC negotiations. The emphasis here is on the U.S. and Soviet Union only because of their critical role in shaping the negotiations and potential for the domestic factors to be consequential. The economic and political challenges influencing the Soviet Union were more severe and consequential than those faced by the U.S. The Soviet Union and subsequently Russia experienced economic recessions in the final years of the CWC negotiations

[81] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction,* Article IX.
[82] Tatsuya Abe, "Challenge inspections under the Chemical Weapons Convention: between ideal and reality," *The Nonproliferation Review* 24, no. 1-2 (2017): 167-184.
[83] Kröll, "The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success," 136.

that precluded the nation from independently being able to credibly commit resources to a treaty that obliges the destruction of CW.[84]

Specifically, Smidovich acknowledges that "The lack of required financial resources due to the lingering economic crisis in Russia makes foreign help a necessary factor in enabling Russia to proceed expeditiously toward destruction of chemical weapons."[85] Yet, the economic reality preventing Russia from abiding by the terms of an agreement did not impede the countries from reaching an agreement. Notably, the U.S. agreed to assist in the construction of destruction facilities. With a strong desire for an agreement and an economic barrier in the way, the system was capable of adjusting. Therefore, this domestic consideration is important in illustrating the challenges faced by Russia but not particularly relevant to the outcome of the agreement.

The most severe domestic challenges faced by the U.S. during negotiations were political in nature. The U.S. bureaucracy did not make it easy for the American negotiators to credibly commit to the agreement, especially given the diversity of actors throughout the government who participate in arms control negotiations. Ratification power of international treaties in the democratic structure of the U.S. bureaucracy resides with the Senate. Previously, the Senate refused to ratify the Geneva Protocol of 1925 and ratified it only fifty years later. Therefore, decisions about the benefits from the agreement would be driven "by bureaucratic and domestic politics."[86] Even if the primary U.S. negotiators believed that they had reached a reasonable and mutually beneficial agreement, there was still unpredictability about the preferences of the Senate and whether its

[84] Smidovich, "The Russian and Other Perspectives," 63.
[85] Ibid., 63.
[86] Julian Perry Robinson, "Difficulties Facing the Chemical Weapons Convention," *International Affairs* 84, no. 2 (March 1, 2008): 225, https://doi.org/10.1111/j.1468-2346.2008.00701.x.

members would officially ratify the final text. Keeping in mind the voting patterns of Senators and domestic constituent concerns about CW while negotiating the text of the treaty were paramount.

On the whole, though, domestic considerations had little relevance in determining the success of CWC negotiations compared to other factors such as reciprocal concessions and resolution of the dual-use challenge. What did help tip the balance of the negotiations in a positive direction was the involvement of the private sector. Its support and public commitment to cooperate was significantly relevant to the negotiations.

Information

Informational challenges related to the inherent secrecy involved with CW programs and the little public knowledge disseminated about CW in general were collectively reflected in debates about verification. This section emphasizes the critical relevance of verification to the negotiations on a CW ban and the solutions that the negotiators formulated.

As with CW, verification is a commonly cited barrier to an international agreement in cyberspace. The CWC provides precedent for the development of an intrusive verification scheme agreed to by the majority of nations to regulate a dual-use and sensitive technology. However, there is also evidence that even an agreement lacking verification, such as the BTWC and the Geneva Conventions, still serves to influence state behavior and guide the international community.

Given that verification was a sticking point in the CWC negotiations, an agreement in cyberspace will be more likely if the major powers can agree on a verification scheme that can effectively monitor state capability and adherence to the agreement while at the same time preserving confidential and proprietary information safeguarded by private corporations. Yet, as noted in chapter two, regulation on use is inherently difficult, so an international agreement may also be

more likely if the entire verification question is sidelined. This section seeks to detail the discussions surrounding and elements of the CWC verification scheme to illustrate its many challenges and provide context for a potential verification scheme in cyberspace if nations decide to pursue one.

As addressed in the introduction, this thesis does not attempt to assess the efficacy of an agreement. It only seeks understand the conditions that make an agreement most likely. Therefore, this chapter will similarly not engage in an analysis of the effectiveness of the CWC verification scheme. Instead, what is more interesting and pertinent to this thesis's analysis is the importance given to verification in the CWC negotiations.

In the early years of negotiations for BW and CW regulation, the international community recognized the significant challenge of verification for CW and decided to separate BW and CW. It was concluded that a CWC could not be agreed upon unless the issue of verification was sufficiently scrutinized.

As a result, verification became a central tenet of subsequent negotiations on a CWC. In a Memorandum of Conversation in 1985, delegates of the U.S. and the Soviet Union acknowledged "We would like to do away with chemical weapons, but here again a major problem is verification. This is a very hard problem to solve."[87] As discussed in the context of reciprocal concessions, in the early years of CWC negotiations the two superpowers and the nations aligned with them disagreed on the issue of verification until around 1987. At this point, the Soviets changed their position on intrusive international verification and the positions of the East and West converged.

[87] Record of Conversation between George Shultz and Eduard Shevardnadze in Helsinki, July 31, 1985, in National Security Archive Electronic Briefing Book No. 481, document no. 3.

The core of the CWC verification regime seeks to ensure the accuracy of the obligatory declaration of various components related to the use and development of CW made by states party to the agreement.[88] The regime also involves on-site inspections of facilities and a verification scheme grounded in the monitoring of the "schedules" of chemicals identified as being developed with varying degrees of military utility. Therefore, a primary goal of verification is to ensure that operations related to the chemicals listed in any of the schedules are appropriately being dealt with.

Another element of the verification regime that generated controversy during the negotiations is the concept of challenge inspections. Article XI gives states the right to request an on-demand inspection without the right of refusal of another nation's facilities to clarify actions "which may be considered ambiguous or which gives rise to a concern about the possible non-compliance of another State Party with this Convention."[89] Additionally, the principle of managed access permits states to restrict the inspector's access to protect information not relevant to the treaty.[90] The combination of these measures fortified the verification regime to ostensibly cover all potential pathways towards violation. This particular verification scheme works well with chemical weapons because it takes a long time to clean up a chemical site once it has been identified via a challenge inspection. In cyber, evidence can be eliminated quickly or may not be able to be found at all, so such a scheme would not be as powerful.

---

[88] The required declarations are "information on chemical weapons, chemical weapons storage facilities (CWSFs), chemical weapons destruction facilities (CWDFs), chemical weapons production facilities (CWPFs), and facilities used in the past for the development of chemical weapons. Similarly, all States Parties are required to make chemical industry declarations related to toxic chemicals and precursors that are mentioned in the three schedules of chemicals, as well as to other chemical production facilities (OCPFs) producing discrete organic chemicals (DOCs)." Peter Boehme. "The Verification Regime of the Chemical Weapons Convention: An Overview." November 28, 2008. https://www.opcw.org/news/article/the-verification-regime-of-the-chemical-weapons-convention-an-overview/.

[89] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction.*

[90] Randall Forsberg, William Driscoll, Gregory Webb, and Jonathan Dean. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons* (MIT Press, 1995), 68.

The expansiveness of the verification regime is largely a consequence of one of the marked challenges of CW verification -- low visibility of weapons capability. This challenge is compounded by the overwhelming incentives for nations to keep their programs secret. CW programs and cyber programs that devise weapons are frequently clouded in secrecy and rarely acknowledged publicly. And even if the programs themselves are public knowledge, it is difficult to go the step further to determine the intent of the programs and whether there is an objective to use the developments for malicious purposes.[91]

A more complicated paradox then emerges. If national intelligence operations are able to identify foreign programs or capabilities, they seldom make such revelations public. Outing another nation's secret programs risks disclosing information about one's own program. Specifically, Elisa Harris, former Director for Nonproliferation and Export Controls on the National Security Council staff, argued that "Governments may fear that if they are more forthcoming with information on chemical warfare activities of specific states, the sources of this information and the methods by which it was acquired might be compromised."[92] Therefore, verification measures in highly secretive domains such as CW or cyberspace are not only feared by nations because they might reveal trade secrets or proprietary information but because they might also require the disclosure of sensitive information about their intelligence operations.

This concern is particularly germane to cyberspace and has been illustrated in practice. In 1971, Jack Anderson, a columnist at the *Washington Post,* wrote an article detailing a sensitive CIA operation in Moscow to eavesdrop on the telephone conversations of Soviet leaders as they

[91] Koblentz and Mazanec, "Viral Warfare: The Security Implications of Cyber and Biological Weapons," 426.
[92] Elisa D. Harris (1989). Testimony. U.S. Senate, Committee on Governmental Affairs, *Global Spread of Chemical and Biological Weapons: Assessing Challenges and Responses.* 101st Congress, 1st sess., February 9. Washington, DC: U.S. Government Printing Office, 56.

drove in limousines throughout the Kremlin.[93] The operation, code named "Gamma Guppy," became inoperable after Anderson's disclosure. The Soviets employed encryption techniques to prevent the U.S. from continuing to extract valuable information from these phone conversations.[94] Thus, once the program was revealed, the U.S. lost the capability that came with it. The Jack Anderson case illustrates the information paradox present in the case of the CWC and omnipresent in cyberspace: when you reveal a capability, you often lose it. Verification and inspection regimes threaten to uncover capabilities that nations try, for evident reasons, to keep secret.

The CW regime circumvented this information paradox by introducing third-party organizations tasked with overseeing verification and a confidentiality clause to prevent the disclosure of national capabilities. The confidentiality clause acts to ensure that inspection authorities are not unduly intrusive and that they take all measures necessary to ensure the protection of confidential information. [95] The OPCW, along with National Authorities which help to enforce the treaty provisions at the national level, are the third-party groups tasked with oversight and implementation of inspections. These groups serve to instill in the signatories a sense of security that the treaty will be appropriately enforced and that the security benefits of terminating their own CW program will be achieved.[96] Therefore, a nation's fear that others will surreptitiously maintain a CW arsenal or that their intelligence capabilities will be compromised is lessened.

---

[93] Unauthorized Disclosures of Classified Information, September 2011, in National Security Archive Electronic Briefing Book No. 506, document no. 42.
[94] Jeffrey T. Richelson, "The CIA and Signals Intelligence," 20 March 2015, in National Security Archive Electronic Briefing Book No. 506.
[95] The "Confidentiality Annex" also ensures that "only the minimum amount of information and data necessary for the timely and efficient carrying out of its responsibilities under this Convention . . ." is adhered to by the Organization for the Prohibition of Chemical Weapons (OPCW). *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction,* Annex on the Protection of Confidential Information. A.1.
[96] "National Authorities," Organisation for the Prohibition of Chemical Weapons, https://www.opcw.org/about-opcw/member-states/national-authorities/.

The CWC regime also acts as a platform for consultation among nations to overcome some of these informational challenges that would otherwise be exacerbated without the CWC. Questions certainly still remain as to why nations would trust the third party not to divulge sensitive capabilities or conduct espionage. Regardless, nations instilled greater trust in such a third party than in other nations, and this preference is a historical precedent that could be addressed in negotiations in cyberspace if verification were to be a fundamental consideration.[97] However, in cyberspace, an agreement founded on the regulation of the use of cyber weapons is inherently not verifiable.

Summary

This chapter has provided a comprehensive overview of the conditions that contributed to the success of negotiations towards a comprehensive ban on chemical weapons. Of greatest relevance to the outcome of the negotiations was the existence of reciprocity in the concessions made to reach a mutually agreeable resolution. Reflected in the capacity for reciprocal concessions to be decisive in the negotiations is the importance of concessions in resolving the difficult yet indispensable question of verification. The commitment and cooperation of the major powers - the U.S. and the Soviet Union - also helped lead the negotiations to success. Additionally, this chapter highlighted the universality of the desire for the elimination of chemical weapons that was strengthened by fears of proliferation and the Iraqi use of CW during the Iran-Iraq War. It likewise

[97] This very concept of third party involvement in monitoring in cyberspace has already been proposed by various organizations. The International Cyberattack Attribution Organization proposed by Microsoft as part of their push for a Digital Geneva Convention is advertised as an organization to increase trust and accountability in cyberspace. It recommends an independent attribution organization "that could receive and analyze the evidence related to a suspected state-backed cyberattack, and that could then credibly and publicly identify perpetrators, would make a major difference to the trust in the digital world." This organization resembles those of various arms control regimes, including that of the CWC, and emphasizes the role of third-party organizations. "An attribution organization to strengthen trust online." Microsoft. https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online.

demonstrated that the negotiators of the CWC devised an acceptable solution to the dual-use challenge and the high pace of technological development in the chemical industry. The analysis of this chapter further contends that the domestic environments of the nations negotiating the treaty, beyond the importance of their respective commercial chemical industries, were of only little relevance to the outcome of the negotiations.

The combination and interaction of these various characteristics of the CW domain and CWC negotiations illustrate the conditions that are likely the most relevant to the success of negotiations towards a cyber international agreement. Specifically, the lessons extracted from the CWC case study are the criticality of reciprocal concessions and the capacity of the international community to derive reasonable solutions to the issues of dual-use, technological development and verification. What did not prove particularly consequential during CWC negotiations was the security dilemma of the technology, the presence of conflicting state interests, and the number of actors party to the negotiations. Given the myriad similarities between the CW environment and cyberspace, the history of the fact that the CWC was eventually successful suggests that it is not completely hopeless that something similar can happen in cyberspace.

Chapter 6 Conclusion

Under what conditions will international agreements in cyberspace be more likely? This thesis has argued that there are four primary conditions that increase the likelihood of international agreements in cyberspace. The condition most conducive to an international agreement in cyberspace is the prevalence of reciprocal concessions during negotiations. This thesis further finds that the existence of the following conditions increase the likelihood of an agreement: the major players in cyberspace are committed to the objective of an agreement, the use of cyber tools not the possession of the tools themselves are being regulated, and private sector concerns are included in negotiations. The more of these conditions that are present, the greater the likelihood an agreement will be reached.

Regardless of whether or not the contemporary cyberspace environment indicates the potential existence of these conditions in the near future, this thesis provides potential avenues of engagement for policy makers to pursue to make international agreements in cyberspace more likely. It also yields a more nuanced view on why international agreements, in writing and governed by international law, have not yet succeeded to this day.

The introduction outlined the theoretical framework on which this thesis's analysis rests and elucidated the scope and assumptions of the analysis. Chapter two explained the choice of the five variables that compose the theoretical framework - technology, state interests, geopolitical dynamics, domestic environments, and information - and presented the preliminary findings. Chapter three provided a comprehensive overview of the existing literature on cyber arms control interwoven with the IR theoretical literature on international cooperation. Chapters four and five examined in detail the negotiations at Reykjavik and towards the CWC, respectively, in the context

of the five key variables. These two case study chapters formed the core of the analysis and consist of reasoning that feeds this thesis's argument, elaborated upon in the next few paragraphs.

The first and most important condition that has the greatest potential to increase the likelihood of an agreement is the existence of reciprocal concessions of a rough equivalence of value made by nations during negotiations. The same variable, reciprocal concessions led to opposing outcomes in the two case studies. The presence of concessions helped facilitate an agreement during CWC negotiations whereas the absence of reciprocal concessions at Reykjavik derailed the negotiations. For this reason, reciprocal concessions is considered the most important condition. Therefore, it is reasonable to assume that reciprocal concessions will also be influential, if not decisive, in negotiations towards an international agreement in cyberspace.

At Reykjavik in 1986, Gorbachev and the Soviet delegation presented significant and unexpected concessions to the U.S. on a variety of issues ranging from ballistic missiles to human rights. In exchange, they demanded that the U.S. halt its SDI program. The Soviets expected that by giving the U.S. a lot of what they sought from the Soviets with respect to restraints on nuclear weapons programs, the U.S. would reciprocate with concessions of similar value. However, Reagan's insistence on the persistence of the SDI program basically nullified any potential agreement on the reduction of nuclear-armed ballistic missiles. Therefore, the outcome of the negotiations was at least somewhat dependent on the ability of nations to commit to reciprocal concessions.

The CWC case study, on the other hand, illustrates the power of reciprocity to propel negotiations to an effective agreement. The U.S. and Soviets, in addition to developing nations, conceded on previously staunch positions to widen the window of cooperation and support the continuation of negotiations. The Soviet concession to accept intrusive, international inspections and

the U.S. acceptance of restrictions on the use of RCAs and herbicides in wartime proved significant in facilitating agreement. Accordingly, the presence of reciprocal concessions in the case of CWC demonstrates the explanatory power of the condition for the outcome of negotiations towards an international agreement.

The second condition this thesis concludes is relevant to the likelihood of international agreements in cyberspace is also an element of the variable state interests. Specifically, the major nations using and engaging in cyberspace should be dedicated to the pursuit of an international agreement and amenable to listening to and engaging in a cooperative manner with each other.

The current reality of cyberspace is plagued by intrinsic differences in perspectives and outlooks among the major powers. The U.S. has pursued an international position grounded in the desire for international norms whereas Russia and China have argued for the establishment of an international code of conduct to democratically govern activity in cyberspace. This conceptual difference is compounded by conflicting views about what should be protected by an agreement and what authority nations have to dictate behavior in the domain. The case studies suggest that resolving many of these conflicts will increase the probability of an international agreement. At Reykjavik and in CWC negotiations, the major powers dominated the discussions and their agreement or inability to agree was decisive. Therefore, resolution of at least some disagreements between the major powers in cyberspace is relevant to the outcome of negotiations toward an international agreement.

The third condition that increases the likelihood of international agreements in cyberspace derived from this thesis's analysis is that such an agreement should regulate the use of cyber weapons rather than the weapon itself. Cyberspace is a highly dual-use domain whereby the same capabilities used to execute cyber weapons have legitimate civilian uses. Additionally, given the

crossover of technology between military and civilian uses, the distinction between such uses is more a result of human behavior than the technology itself.

An agreement meant to regulate possession of cyber weapons is also nearly impossible to verify as a result of the high degree of secrecy surrounding cyber programs and the ambiguity between military and civilian capabilities. Therefore, although an agreement to regulate based on use is also not easily verifiable, a regulation on use is more sustainable than a regulation on the possession of cyber weapons in the face of a high pace of technological development, a dual-use technology, and operations that depend on stealth and deception.

The CWC, which itself dealt with a dual-use technology in chemicals, provides a solid example of negotiations and a resulting effective agreement that emphasizes restrictions based on use instead of the chemicals themselves. Certainly the CWC contains schedules of classes of chemicals in its annexes, but the core of the agreement centers on a General Purpose Criterion that guides state behavior according to acceptable and unacceptable uses and is adaptable with technological development.

There have also been steps already taken by states to agree upon norms that reflect an understanding that use rather than possession of technology should be the subject of discussion. The UN GGE agreed upon norms not to target the critical infrastructure or the computer emergency response team of another state.[1] The Convention on Cybercrime, established by the Council of Europe, also predicates its provisions on defining actions in cyberspace that should be punishable by law rather than attempting to ban classes of weapons commonly used in cybercrime.[2] These examples illustrate the existing efforts to focus on the regulation of use of cyber weapons rather

[1] United Nations, Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.
[2] Council of Europe, *Convention on Cybercrime*.

than the weapons themselves, and this thesis's analysis argues for a greater emphasis on the determination of acceptable and unacceptable uses if an international agreement is to be pursued.

The fourth and final condition reasoned from this thesis is the importance of the active participation of the private sector companies that own and operate the infrastructure that composes much of the cyberspace domain. Given the highly dual-use nature of cyber technology, an effective agreement should not overlook the interests and capabilities of the private sector. The state leaders recognized this reality during the CWC negotiations, with the chemical industry, seeking to correct a poor reputation from the 1970s and 1980s, playing a prominent role in the negotiations.

One of the industry's concerns at the time of the CWC negotiations was, however, that intrusive inspections could lead to espionage of proprietary and confidential information. This concern was ultimately addressed during the negotiations, but it nonetheless illustrates an apprehension that the technology industry may surface in negotiations towards international agreements in cyberspace. It is important to note that during the writing of this thesis, in April 2018, many leading internet companies in the private sector took the initiative to pledge to protect the security of their customers and not to help governments conduct offensive cyber operations.[3] While the private sector is mostly concerned with freeing themselves from governmental oversight and regulation, the technology sector has already demonstrated an interest in suppressing hostile offensive cyber operations that can be leveraged to garner their support for and cooperation with negotiations at a nation state level.

Given these conclusions, this thesis draws two primary policy implications regarding the future of international agreements in cyberspace. As mentioned in the introduction, there is a

[3] *Cybersecurity Tech Accord*, 17 April 2018, available at: https://cybertechaccord.org/accord/.

demonstrated interest among world leaders and private companies in an international agreement as well as an increased need for such an agreement with the heightened severity and frequency of cyberattacks worldwide. Therefore, the conclusions presented here provide policymakers with concrete objectives to strive for.

That is, instead of approaching cyberspace in its entirety, policymakers can narrow the scope of their efforts to bring to reality the conditions listed in this thesis that increase the likelihood of an agreement. This focus reduces the perceived complexity of pursuing international agreements in cyberspace and concentrates policy efforts on the most pressing and favorable conditions for successful negotiations.

The second policy implication derived from this analysis is that policymakers in cyberspace should not proceed with the common assumption that cyber is a unique domain unlike anything the international system has witnessed before. In fact, the case study framework employed in this thesis illustrates that negotiators on cyberspace have much to learn from historical cases. While many of the elements that mirror historical cases are more severe or more nuanced in cyberspace, there are nonetheless many parallels to the CW domain and even the nuclear weapons domain that help to situate cyberspace in common IR and conceptual paradigms. Establishing such connections to historical cases also makes discussions about cyberspace more accessible to the generation of policymakers less educated about the intricacies of the internet.

In summary, this thesis has illuminated specific conditions that can make international agreements in cyberspace more likely. A systematic analysis of historical case studies with characteristics similar to cyberspace and the contextualization of cyberspace within the broader IR theoretical literature have demonstrated the value in carefully applying lessons from history and theory to better understand the complex cyberspace domain.

The research conducted in this thesis should demonstrate to policymakers, scholars, and pundits alike that while international agreements in cyberspace will take time and face significant challenges, the resolution of particular existing challenges carry more weight and can increase the chances of an agreement. Further research should continue this line of study by emphasizing potential areas or means of cooperation rather than focusing on the myriad of impediments to international agreements.

Bibliography

Abe, Tatsuya. "Challenge inspections under the Chemical Weapons Convention: between ideal and reality." *The Nonproliferation Review* 24, no. 1-2 (2017): 167-184.

Agreement between the United States of America and the Union of Soviet Socialist Republics on Destruction and Non-production of Chemical Weapons on Measures to Facilitate the Multilateral Convention on Banning Chemical Weapons, 1 June 1990, 29 ILM 934 (1990).

"An attribution organization to strengthen trust online." Microsoft. https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online.

Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." *Cyber Conflict (CYCON), 2012 4th International Conference On* (IEEE, 2012): 1–19.

Arms Control Unchained, Box 20, Charles Hill Papers, Hoover Institution Archives, Stanford, California.

Axelrod, Robert. *The Evolution of Cooperation* (New York: Basic Books, 1984).

Background Paper on the Following Arms Control Issues Which Are Likely to Arise in the Course of Upcoming U.S.-Soviet Summit Discussions: Nuclear Testing; Chemical Weapons; Open Skies Proposal; Conventional Armed Forces in Europe (CFE) Treaty; Strategic Arms Reduction Talks (START). United States: Department Of State, 1990. http://tinyurl.galegroup.com/tinyurl/5wjA65.

Bailey, Kathleen C. "Problems with the Chemical Weapons Convention." In *Shadows and Substance: The Chemical Weapons Convention,* edited by Benoit Morel and Kyle Olson, Westview Press, 1993.

"Ballistic Missile Defense (BMD)." Ballistic Missile Defense Glossary Version 3.0. Accessed January 31, 2018. http://www.dtic.mil/dtic/tr/fulltext/u2/a338544.pdf.

Banks, William. "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0." 95 TEXAS L. REv. 1487, 1501 (2017).

Bernauer, Thomas and Dieter Ruloff. *The Politics of Positive Incentives in Arms Control*: Univ of South Carolina Press, 1999.

Bernauer, Thomas. "Warfare: Nuclear, Biological, and Chemical Weapons." In *Managing Global Issues: Lessons Learned*, edited by Chantal de Jonge Oudraat, P.J. Simmons, and Jessica Tuchman Mathews, Carnegie Endowment (2001).

Bernauer, Thomas. *Projected Chemical Weapons Convention: A Guide to the Negotiations in the Conference on Disarmament*. New York, United Nations.

Bernauer, Thomas. *The Chemistry of Regime Formation: Explaining International Cooperation for a Comprehensive Ban on Chemical Weapons* (Ashgate Publishing Company, 1993).

Blanton, Thomas and Svetlana Savranskaya, "Reykjavik: When Abolition Was Within Reach." *Arms Control Today; Washington* 41, no. 8 (October 2011).

Boehme, Peter. "The Verification Regime of the Chemical Weapons Convention: An Overview." November 28, 2008. https://www.opcw.org/news/article/the-verification-regime-of-the-chemical-weapons-convention-an-overview/.

Boylan, Edward S., Donald G. Brennan, and Herman Kahn. "An Analysis of "Assured Destruction."" *Hudson Institute* (1972): 1-26.

Bush, George H. W. "Statement on Chemical Weapons." May 13, 1991. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=19575.

Carter, April and Stockholm International Peace Research Institute. *Success and Failure in Arms Control* Negotiations: Oxford, UK: Oxford University Press, 1989.

"Chernobyl Accident 1986," World Nuclear Association. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx.

Cirenza, Patrick. “The Flawed Analogy between Nuclear and Cyber Deterrence.” Bulletin of the Atomic Scientists, February 22, 2016. http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179.

Cirenza, Patrick. *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence.* Center for International Security and Cooperation Honors Thesis, Stanford University, 2015.

Clinton, Hillary Rodham. “Remarks.” Conference on Internet Freedom, The Hague, Netherlands, December 8, 2011.

Convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction, Washington, 10 April 1972, *United Nations Treaty Series*, vol. 1015, available from https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280101653.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their destruction, Geneva, 3 September 1992, *United Nations Treaty Series*, vol. 1974, available from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-3&chapter=26&clang=_en.

Conybeare, John “International Organization and the Theory of Property Rights.” *International Organization* 34 (1980): 307–334.

Council of Europe, *Convention on Cybercrime,* 23 November 2001.

Cybersecurity Tech Accord, 17 April 2018, available at: https://cybertechaccord.org/accord/.

Daily Bulletin of the US Mission to the UN in Geneva, 26 September 1989.

Daoudi, Mohamed and Ralf Trapp. "Verification under the Chemical Weapons Convention." In *Verifying Treaty Compliance*, Springer, Berlin, Heidelberg, (2006): 77-106.

Department Of State. The Office of Electronic Information, Bureau of Public Affairs. “Strategic Defense Initiative (SDI), 1983,” May 1, 2008. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm.

“Deterrence.” Department of Defense Dictionary of Military and Associated Terms. Accessed January 31, 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

Doctrine of Information Security of the Russian Federation, approved by the President of the Russian Federation Vladimir Putin on December 5, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

Dolan, Ronald E., Russell R. Ross, and Robert L. Worden. “East Asia/Pacific Reactions to the Strategic Defense Initiative.” *Federal Research Division of the Library of Congress,* January-December 1986.

Doty, Paul and Matthew Meselson to Dr. Henry A. Kissinger, May 16, 1972, Department of Chemistry, Harvard University.

Downs, George. *Optimal Imperfection?: Domestic Uncertainty and Institutions in International Relations*: Princeton, NJ: Princeton University Press, 1995.

Drell, Sidney D., Philip J. Farley, and David Holloway. "Preserving the ABM Treaty: A Critique of the Reagan Strategic Defense Initiative." *International Security* 9, no. 2 (1984): 51-91.

Erdmann, Gero et al. “International Cooperation of Authoritarian Regimes: Toward a Conceptual Framework.” GIGA Working Paper 229, (Hamburg: GIGA German Institute of Global and Area Studies, 2013). Available online at: www.giga-hamburg.de/de/publication/international-cooperation-of-authoritarian-regimes-toward-a-conceptual-framework.

EU Commission Information Society Website. Available at: http://ec.europa.eu/archives/ISPO/infocentre/glossary/i_glossary.html#c

Farrell, Henry. “Promoting Norms for Cyberspace.” *Council on Foreign Relations Cyber-Brief*, 2015.

Fearon, James. “Bargaining, Enforcement, and International Cooperation.” *International Organization* 52, no. 2 (1998): 269-305.

Fearon, James. “Domestic Politics, Foreign Policy, and Theories of International Relations.” *Annual Review of Political Science* 1, (1998): 289-313.

Fidler, David P. “The Chemical Weapons Convention After Ten Years: Successes and Future Challenges.” *ASIL Insights* 11, no. 12 (2007). https://www.asil.org/insights/volume/11/issue/12/chemical-weapons-convention-after-ten-years-successes-and-future.

Ford, Gerald. “Executive Order 11850 -- Renunciation of certain uses in war of chemical herbicides and riot control agents.” National Archives, 1975.

Forsberg, Randall, William Driscoll, Gregory Webb, and Jonathan Dean. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons*. MIT Press, 1995.

Forsyth Jr, James W. "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace" (AIR UNIV MAXWELL AFB AL SCHOOL OF ADVANCED AIR AND SPACE STUDIES, 2013), http://www.dtic.mil/docs/citations/ADA595562.

Frieden, Jeffry A., David A. Lake, and Kenneth A. Schultz. *World Politics: Interests, Interactions, Institutions*, 2 edition (New York: W. W. Norton & Company, 2012).

Geneva Protocol, "Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare." *Signed at Geneva, June* 17 (1925).

"Genesis and Historical Development." *Organisation for the Prohibition of Chemical Weapons,* https://www.opcw.org/chemical-weapons-convention/genesis-and-historical-development/.

Glaser, Charles L. *Rational Theory of International Politics: The Logic of Competition and Cooperation:* Princeton, NJ: Princeton University Press, 2010.

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." Hoover Institution, March 9, 2011, http://www.hoover.org/research/cybersecurity-treaties-skeptical-view.

Gorbachev's instructions for the group preparing for Reykjavik, 4 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 5.

Grieco, Joseph. *Cooperation among Nations*: Ithaca, N.Y.: Cornell University. Press, 1990.

Haas, Ernst B. "Words Can Hurt You; Or, Who Said What to Whom about Regimes." *International Organization* 36, no. 2 (1982): 207–43.

Halberstam, Malvina. "The Use of Legislative History in Treaty Interpretation: The Dial Treaty Approach," *Cardozo Law Review* 12 (1991 1990): 1645–1652.

Harbour, Frances V. “The ABM Treaty, New Technology and the Strategic Defense Initiative.” *J. Legis* 15 (1988): 119-138.

Harris, Elisa D. (1989). Testimony. U.S. Senate, Committee on Governmental Affairs, *Global Spread of Chemical and Biological Weapons: Assessing Challenges and Responses.* 101st Congress, 1st sess., February 9. Washington, DC: U.S. Government Printing Office.

Hodgson, Grant. “Cyber Attack Treaty Verification.” *ISJLP* 12 (2015): 231-260.

Holloway, David. “The Strategic Defense Initiative and the Soviet Union,” *Daedalus* 114, no. 3 (1985): 257-278.

International Code of Conduct for Information Security, transmitted by “Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General,” UN Doc. A/69/723, January 13, 2015.

International Law Commission, *Draft Articles of Responsibility of States for Internationally Wrongful Acts,* November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1.

Jervis, Robert. “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167-214.

Jervis, Robert. “Security Regimes.” *International Organization* 36, no. 2 (1982): 357-378.

Jervis, Robert. *Perception and Misperception in International Politics*, 1st edition: Princeton, N.J: Princeton University Press, 1976.

Kanuck, Sean. “Deterrence and Arms Control in Cyberspace.” The Berkman Klein Center for Internet & Society, March 30, 2016.

Katzenbach, Nicholas deB to Mr. Walt W. Rostow, “Policy on Chemical and Biological Weapons.” February 20, 1967, Department of State, Washington, D.C.

Kelle, Alexander. “Developing Control Regimes for Chemical and Biological Weapons.” *The International Spectator* 32, no. 3–4 (July 1, 1997): 137-157, https://doi.org/10.1080/03932729708456788.

Kenyon, Ian R. and Daniel Feakes, eds. *The Creation of the Organisation for the Prohibition of Chemical Weapons: A Case Study in the Birth of an Intergovernmental Organisation,* 1st edition: The Hague : West Nyack, NY: T.M.C. Asser Press, 2007.

Kenyon, Ian. “The USA/USSR Arms Control Relationship and Its Impact on the CWC.” *CBW Conventions Bulletin* (2006).

Keohane, Robert O. “Reciprocity in International Relations.” *International Organization* 40 (Winter 1986): 1-27.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*: Princeton University Press, 1984. http://www.jstor.org/stable/j.ctt7sq9s.

Keohane, Robert O. and Joseph S. Nye. “Two Cheers for Multilateralism.” *Foreign Policy*, no. 60 (1985): 148-167.

Kimball, Daryl G. "The Chemical Weapons Convention (CWC) at a Glance." January 2018. https://www.armscontrol.org/factsheets/cwcglance.

Koblentz, Gregory D. and Brian M. Mazanec. “Viral Warfare: The Security Implications of Cyber and Biological Weapons.” *Comparative Strategy* 32, no. 5 (November 1, 2013): 418–434.

Koplow, David A. “Long Arms and Chemical Arms: Extraterritoriality and the Draft Chemical Weapons Convention.” *Yale Journal of International Law* 15 (1990): 1-83.

Krasner, Stephen D. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization* 36, no. 2 (1982): 185-205.

Kröll, Patricia. “The Chemical Weapons Prohibition Regime - Organizational, Political and Technical Elements of Success.” Doctoral diss., Universität Wien, (2011).

Kruzel, Joseph. “From Rush-Bagot to START: The Lessons of Arms Control.” *Orbis* 30, no. 1 (1986).

Lambeth, Benjamin S. and Kevin Lewis, “The Kremlin and SDI.” Foreign Affairs, March 1, 1988. https://www.foreignaffairs.com/articles/russian-federation/1988-03-01/kremlin-and-sdi.

Lambeth, Benjamin S. and Kevin Lewis, “The Strategic Defense Initiative in Soviet Planning and Policy.” Santa Monica: RAND Corporation (1988).

Letter to Senator William Cohen (R-Maine) from Secretary of State George Shultz Concerning Measures to Prevent the World-Wide Spread of Chemical Weapons. United States: Department Of State, 1988. http://tinyurl.galegroup.com/tinyurl/5wj7o3.

Lewis, James A. “Confidence-Building and International Agreement in Cybersecurity.” in *Disarmament Forum*, vol. 4 (2011): 51–60. https://citizenlab.org/cybernorms2012/Lewis2011.pdf.Lewis.

Lewis, James A. “Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms.” *Strategic Technologies Program*, Center for Strategic and International Studies (February 2014).

Lin, Herbert S. "Arms Control in Cyberspace: Challenges and Opportunities." World Politics Review (March 05, 2012). https://www.worldpoliticsreview.com/articles/11683/arms-control-in-cyberspace-challenges-and-opportunities.

Lin, Herbert S. “Attribution of Malicious Cyber Incidents: From Soup to Nuts.” Journal of International Affairs (Winter 2016).

Lin, Herbert. “A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity.” *Bulletin of the Atomic Scientists* 68, no. 5 (March 2012): 75-87.

Lindblom, Charles. *The Intelligence of Democracy*: New York: Free Press, 1965.

Livingstone, Neil C. and Joseph D Douglass. *CBW, the Poor Man's Atomic* Bomb: Cambridge, Mass.: Institute for Foreign Policy Analysis, 1984.

Major Issues for the meetings of the General Secretary of the CPSU Central Committee Mikhail Gorbachev with Ronald Reagan on the question of nuclear disarmament, October, Box 4, Folder 13, Vitalli Leonidovich Kataev Collection, Hoover Institution Archives, Stanford, California.

Matlock Jr., Jack F. *Reagan and Gorbachev:* New York: Random House, 2004.

Mattes, Michaela and Mariana Rodríguez. “Autocracies and International Cooperation.” *International Studies Quarterly* 58, no. 3 (2014): 527-538.

Memorandum for Zbigniew Brzezinski from Jessica Tuchman regarding U.S. approach to a chemical weapons treaty with the Soviet Union. National Security Council, 7 June 1977. *U.S. Declassified Documents Online*, http://tinyurl.galegroup.com/tinyurl/5wj8E0. Accessed 15 Mar. 2018.

Memorandum to the President, Secretary of State George Shultz, “Subject: Reykjavik,” 2 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 4.

Meselson, Matthew. Keynote Address to the Sixth Annual Scientific Conference on Chemical Defense Research, U.S. Army Chemical Research, Development and Engineering Center, Edgewood Area, Aberdeen Proving Ground, Maryland, 13-16 November 1990.

Mikhail Gorbachev letter to Ronald Reagan, 15 September 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 1.

Mikheyev, Dmitry. *The Soviet Perspective on the Strategic Defense Initiative*: Washington: Brassey's Inc, 1987.

Milner, Helen. "International Theories of Cooperation among Nations: Strengths and Weaknesses." *World Politics* 44, no. 3 (1992): 466-496.

Morgenthau, Hans J., Kenneth W. Thompson, and David Clinton. *Politics Among Nations,* 7 edition: Boston: McGraw-Hill Education, 2005.

Morrow, James D. "Modeling the Forms of International Cooperation: Distribution Versus Information." *International Organization* 48, no. 3 (1994): 387-423.

"National Authorities." Organisation for the Prohibition of Chemical Weapons. https://www.opcw.org/about-opcw/member-states/national-authorities/.

National Cybersecurity Strategy, released by the Cyberspace Administration of China on December 27, 2016. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

"NRC: Backgrounder on Chernobyl Nuclear Power Plant Accident." Accessed January 31, 2018. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html.

"Nuclear Weapons: Who Has What at a Glance | Arms Control Association." Arms Control Association. Accessed January 31, 2018. https://www.armscontrol.org/factsheets/Nuclear-weaponswhohaswhat.

Nye Jr., Joseph S. “From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?” *Bulletin of the Atomic Scientists* 69, no. 5 (September 2013): 8–14. https://doi.org/10.1177/0096340213501338.

Nye Jr., Joseph S. “Nuclear Lessons for Cyber Security.” (AIR UNIV PRESS MAXWELL AFB AL, 2011). http://www.dtic.mil/docs/citations/ADA553620.

Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities.” Global Commission on Internet Governance Paper Series, Paper No. 1. (2014). https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf.

O’Donnell, Lindsey. “RSA 2018: Tech Giants form Cybersecurity Tech Accord.” ThreatPost, April 17, 2018. https://threatpost.com/rsac-2018-tech-giants-form-cybersecurity-tech-accord/131253/.

Offit, Paul A. *Pandora’s Lab: Seven Stories of Science Gone Wrong*: Washington, DC: National Geographic, 2016.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with New Preface and Appendix*, Revised edition: Cambridge, Mass.: Harvard University Press, 1971.

"Origins of the Chemical Weapons Convention and the OPCW." September 12, 2014. https://www.acs.org/content/dam/acsorg/events/program-in-a-box/documents/2016-global-security/cw-history.pdf.

Oye, Kenneth A. “Explaining Cooperation under Anarchy: Hypotheses and Strategies.” *World Politics* 38, no. 01 (October 1985): 1-24.

Oye, Kenneth Akito. *Bargaining, Belief Systems, and Breakdown: International Political Economy, 1929-1936* (Harvard University, 1983).

Price, Richard. “A Genealogy of the Chemical Weapons Taboo.” *International Organization* 49, no. 1 (1995): 73–103.

Prospects for the Creation of a U.S. Space Ballistic Missile Defense System and the Likely Impact on the World Military Political Situation, Report of the Committee of Soviet Scientists in Defence of Peace and Against the Threat of Nuclear War, Moscow, 1983, mimeo.

Randall, Kenneth C. “The Treaty Power.” *Ohio State Law Journal* 51 (1990): 1089–1126.

Reagan, Ronald. “Address to the Nation on Defense and National Security.” Speech at The White House, Washington, D.C., March 23, 1983, Ronald Reagan Presidential Library, *Public Papers*, Reagan Library.

Record of Conversation between George Shultz and Eduard Shevardnadze in Helsinki, July 31, 1985, in National Security Archive Electronic Briefing Book No. 481, document no. 3.

Richelson, Jeffrey T. “The CIA and Signals Intelligence.” 20 March 2015, in National Security Archive Electronic Briefing Book No. 506.

Roberts, Brad. “The Chemical Weapons Convention and World Order.” *Shadows and Substance: The Chemical Weapons Convention,* edited by Benoit Morel and Kyle Olson, Westview Press, 1993.

Robinson, Julian Perry. “Difficulties Facing the Chemical Weapons Convention.” *International Affairs* 84, no. 2 (March 1, 2008): 223–39. https://doi.org/10.1111/j.1468-2346.2008.00701.x.

Robinson, Julian Perry. “The Negotiations on the Chemical Weapons Convention: A Historical Overview.” *The New Chemical Weapons Convention: Implementation and Prospects,* edited by Michael Bothe et al., Martinus Nijhoff Publishers, 1998: 17-37.

Rõigas, Henry and Tomáš Minárik. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” NATO Cooperative Cyber Defence Centre of Excellence, 31 August 2015. https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

Rowen, Hobart. “Soviets See SDI as Economic First Strike.” The Washington Post, 19 October 1986. https://www.washingtonpost.com/archive/business/1986/10/19/soviets-see-sdi-as-economic-first-strike/36fddf24-5dba-4137-a65c-3af999381250/?utm_term=.4abd7dd56f5b.

Ruggie, John G. “International Responses to Technology: Concepts and Trends.” *International Organization* 29 (Summer 1975): 557-583.

Russian transcript of Reagan-Gorbachev Summit in Reykjavik, 12 October 1982, in National Security Archive Electronic Briefing Book No. 203, document no. 16.

Schelling, Thomas C. *The Strategy of Conflict*, Reprint edition: Cambridge, Mass.: Harvard University Press, 1981.

Schelling, Thomas and Morton Halperin. *Strategy and Arms Control:* New York: Twentieth Century Fund, 1961.

Schmitt, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations:* Cambridge: Cambridge University Press, 2017.

Schmitt, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare:* New York: Cambridge University Press, 2013.

Secretary George Shultz, interviewed by Rachel Hirshman, Stanford, CA, February 2018.

Shackelford, Scott J. and Andraz Kastelic. “Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity.” *NYUJ Legis. & Pub. Pol’y* 18 (2015).

Shackelford, Scott. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.” SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, April 28, 2009), https://papers.ssrn.com/abstract=1396375.

Shultz, George P. *Turmoil and Triumph: My Years as Secretary of State:* New York: Charles Scribner's Sons, 1993.

Simmons, Beth A. “Compliance with International Agreements.” *Annual Review of Political Science* 1, no. 1 (1998): 75-93.

Slack, Chelsea. “Wired yet Disconnected: The Governance of International Cyber Relations.” *Global Policy* 7, no. 1 (2016): 69-78.

Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” International Security, Vol. 41, No. 3 (2017): 72-109.

Slomanson, William R. *Fundamental Perspectives on International Law*: St. Paul: West Pub., 1990.

Smidovich, Nikita. “The Russian and Other Perspectives.” *Shadows and Substance: The Chemical Weapons Convention,* edited by Benoit Morel and Kyle Olson, Westview Press, 1993.

Smith, Brad. “The Price of Cyber-Warfare.” Speech at the RSA Conference, San Francisco, CA, April 17, 2018.

Sofaer, Abraham D. “The ABM Treaty and the Strategic Defense Initiative.” *Harvard Law Review* 99, no. 8 (1986): 1972–1985. https://doi.org/10.2307/1341216.

Sofaer, Abraham, David Clark, and Whitfield Diffie. “Cyber Security and International Agreements.” In National Research Council, Proceedings of a Workshop on Deterring Cyberattacks, 2009, http://sites.nationalacademies.org/CSTB/cs/groups/cstbsite/documents/webpage/cstb_059440.pdf.

Sofaer, Abraham. “A Legacy of Reykjavik: Negotiating with Enemies.” In implications of the Reykjavik Summit on its Twentieth Anniversary, eds. S. Drell & G. P. Shultz, (Stanford: Hoover Institution, 2007): 127-145.

Soviet Embassy, Information Department, Statement on a Ban on Chemical Weapons, News and Views from the USSR (Mar. 26, 1987).

Stein, Arthur A. “Coordination and Collaboration: Regimes in an Anarchic World.” *International Organization* 36, no. 2 (1982): 299-324.

Strategic Defense Initiative, Box 20, Folder 18, Joan Beecher Eichrodt Collection, Hoover Institution Archives, Stanford, California.

Taubman, Philip. *The Partnership: Five Cold Warriors and Their Quest to Ban the Bomb:* New York: HarperCollins, 2012.

Taubman, William. *Gorbachev His Life and Times:* Simon & Schuster, 2017.

Text of a memorandum of understanding between the U.S. and the U.S.S.R. with respect to a bilateral verification experiment and a data exchange program to deal with the prohibition of chemical weapons. White House, 23 Sept. 1989. *U.S. Declassified Documents Online*, http://tinyurl.galegroup.com/tinyurl/5wj9R9. Accessed 17 Mar. 2018.

“The Military Balance 2010,” The International Institute for Strategic Studies, 2010. https://www.iiss.org/en/publications/military-s-balance.

"The President's Trip to Reykjavik, Iceland, October 9-12, 1986 - Issues Checklist for the Secretary," U.S. Department of State, 7 October 1986, in National Security Archive Electronic Briefing Book No. 203, document no. 7.

To the Geneva Summit: Perestroika and the Transformation of U.S.-Soviet Relations, in National Security Archive Electronic Briefing Book No. 172.

Treaty on the Limitation of Anti-Ballistic Missile Systems, May 26, 1972, United States-U.S.S.R., 23 U.S.T. 3435, T.I.A.S. No. 7503.

Tsagourias, Nicholas. "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts." *Journal of Conflict and Security Law* 21, no. 3 (2016): 455–474.

Tucker, Jonathan B. "The Future of Chemical Weapons." *The New Atlantis*, Number 26, Fall 2009/Winter 2010: 3-29. https://www.thenewatlantis.com/publications/the-future-of-chemical-weapons.

Unauthorized Disclosures of Classified Information, September 2011, in National Security Archive Electronic Briefing Book No. 506, document no. 42.

United Nations General Assembly Resolution 2603, *Question of Chemical and Bacteriological (Biological) Weapons,* A/RES/2603(XXIV)A (16 December 1969), available from https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/257/37/IMG/NR025737.pdf?OpenElement.

United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General." U.N. Doc. A/68/156 (2013), https://undocs.org/A/68/156.

United Nations Report, *Report of the Executive Chairman on the activities of the Special Commission established by the Secretary-General pursuant to paragraph 9 (b) (i) of resolution 687 (1991)*, S/1999/401, 9 April 1999, http://www.un.org/Depts/unscom/sres401eng.htm.

United Nations Security Council Resolution 687, S/Res/687 (3 April 1991), http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/687(1991).

United Nations Special Commission, *Letter dated 25 January 1999 from the Executive Chairman of the Special Commission established by the Secretary-General pursuant to paragraph 9 (b) (i) of Security Council resolution 687 (1991) addressed to the President of the Security Council*, S/1999/94, 29 January 1999, http://www.un.org/Depts/unscom/s99-94.htm.

United Nations, Conference on Disarmament, *Final record of the 428th plenary meeting, held at the Palais des Nations, Geneva*, CD/PV.428 (6 August 1987), available from https://digitallibrary.un.org/record/143615/.

United Nations, Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2014), available from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

United States, and Harry Lorenzo Gilchrist. *A comparative study of World War casualties from gas and other weapons*: Washington, D.C.: Govt. Printing Office, 1928.

United States, Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* JP 1-02 (Washington, D.C.: Defense Technical Information Center, 2016).

United States Congress, Office of Technology Assessment, The Chemical Weapons Convention: Effects on the U.S. Chemical Industry, OTA-BP-ISC-1O6 (Washington, DC: U.S. Government Printing Office, August 1993).

Vice President Bush, "U.S. Proposes Banning Chemical Weapons." *Current Policy No. 566,* U.S. Department of State, Bureau of Public Affairs, Washington, D.C.

Vienna Convention on the Law of Treaties, 1155 UNTS 311 (May 23, 1969), art. 2, s 1(a).

Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)." *Yale Journal of International Law* 36 (2011).

Webster, William H. (1989). Testimony. U.S. Senate, Committee on Governmental Affairs, *Global Spread of Chemical and Biological Weapons: Assessing Challenges and Responses.* 101st Congress, 1st sess., February 9. Washington, DC: U.S. Government Printing Office.

Wiznowski, Karen. "Opting Out of the Iron Triangle: The US Chemical Industry and US Chemical Weapons Policy." The Nonproliferation Review 18, no. 2 (July 2011), 331-347.

Writings 2 of 2, Box 69, Henry Rowen Collection, Hoover Institution Archives, Stanford, California.

Yadron, Danny. "Iranian Hackers Infiltrated New York Dam in 2013." *Wall Street Journal*, December 21, 2015, sec. US. http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559.

Young, H. Peyton. *Equity: In Theory and Practice*: Princeton University Press, 1995.

Zanders, Jean Pascal. "Chemical-Weapons Deproliferation and the Chemical Weapons Convention Communications." *Revue Belge de Droit International / Belgian Review of International Law* 26 (1993): 264-282.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*: Crown, 2014.

Zoller, Elizabeth. *Peacetime Unilateral Remedies: An Analysis of Countermeasures:* Dobbs Ferry, N.Y.: Transnational, 1984.