2022

Delphi Study of International Cybersecurity Norms

Kenneth J. Biskner
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Kenneth J. Biskner

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Michael Knight, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, Committee Member,
Public Policy and Administration Faculty

Dr. Christopher Jones, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Delphi Study of International Cybersecurity Norms

by

Kenneth J. Biskner

MPhil, Walden University, 2020

LLM, The Judge Advocate General's Legal Center and School, 2011

LLM, University of Miami, 1999

JD, University of Miami, 1998

BS, Southern Illinois University, 1995

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2022

Abstract

Unregulated state cyberattacks are an urgent threat to international peace and security because of the costs they impose and the devastating effects they can create. However, international norms governing state cyberattacks (international cybersecurity norms) have not yet emerged. The lack of meaningful consequences for state cyberattacks, and the high rewards derived from them, incentivize states to engage in this new form of hostile conduct (cyberconflict). The problem addressed in this modified Delphi study was the persistent struggle between authoritarian and democratic states over competing international cybersecurity norms that cause cyberconflict to remain unregulated. Kingdon's multiple streams framework was used as a theoretical lens to examine the norm emergence process. Data were collected from a panel of experts in international cybersecurity norms. Three rounds of online questionnaires were administered, with participant feedback between rounds, to build a consensus opinion. Six participants completed all rounds. Terms and phrases of participants were used to create codes, and related codes were grouped to reveal patterns and develop themes. The panel did not establish strong consensus (*Kendal's* $W \geq .75$) regarding the ranking of the issues but defined the points of disagreement and reached a weak consensus on the top three issues: problem nature, attribution, and threat perception. Findings may inform positive social change through future efforts to create the conditions necessary for international cybersecurity norms to emerge, thereby contributing to international peace and security.

Delphi Study of International Cybersecurity Norms

by

Kenneth J. Biskner

MPhil, Walden University, 2020

LLM, The Judge Advocate General's Legal Center and School, 2011

LLM, University of Miami, 1999

JD, University of Miami, 1998

BS, Southern Illinois University, 1995

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2022

Table of Contents

List of Tables

Chapter 1: Introduction to the Study

State cyberattacks for economic, political, and security purposes (i.e., cyberconflict) are an existential threat to international peace and security, making cyberconflict an urgent international policy issue (NATO Cooperative Cyber Defense Center of Excellence, 2019; Statement for the Record, 2021). International political and legal norms normally regulate hostile state conduct of this kind; however, few norms currently exist for responsible state conduct in cyberspace (Broeders et al., 2022; Theohary & Rollins, 2015). A deep divide exists between democratic and authoritarian states over the nature of these norms, so unregulated cyberconflict persists as the status quo (Buchanan, 2020; Kurre, 2017; Musiani & Pohle, 2014). In the current study, I identified the critical points of disagreement that must be bridged so international political norms regulating cyberconflict (i.e., international cybersecurity norms) can emerge.

The struggle between democratic and authoritarian states to control international norms has polarized the international community (Bernard, 2016; Boyle, 2016; Klimburg & Faesen, 2020). After the collapse of the Soviet Union, the United States and its liberal democratic allies (democratic states) emerged as the leading world powers (Bernard, 2016). Western cultural norms dominated international politics and institutions for the next decade (Cooley, 2015a). However, an emerging coalition of authoritarian states, led by Russia and China, rejected many democratic state norms (Horvath, 2016; Inboden & Chen, 2012; Zeng et al., 2017), and especially opposed international cybersecurity norms (Broeders et al., 2019; Eichensehr, 2014; Radu, 2013). A change in a few existing internet governance norms to increase security could alter cyberspace and redistribute international power (Inkster, 2017; Shackelford & Craig, 2014). As a result, the status quo of unregulated cyberconflict persists despite the magnitude of the threat it represents.

In 2012, the U.S. Secretary of Defense said cyberconflict has the potential to "cripple" the United States (Panetta, 2012, para. 79). Every year since that statement, the U.S. Director of National Intelligence has identified cyberconflict as a top national security threat (Statement for the Record, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2021). Although some scholars argue the likelihood of catastrophic cyberconflict is overstated (Gartzke, 2013; Gray, 2013; Rid, 2013), all agree the danger is real (Carlin, 2015; Clarke & Knake, 2011; Shackelford et al., 2017; Singer & Friedman, 2014). In 2018, the Federal Bureau of Investigation underscored the threat when it determined that Russia attacked United States critical national infrastructure (CNI; e.g., national power-grid control systems) and implanted cyberweapons for later use (Cybersecurity and Infrastructure Security Agency, 2018; Hendrickson, 2015; Lee, 2013; Nguyen, 2013). The United States has also accused China of launching cyberattacks against United States CNI (Hendrickson, 2015; Lee, 2013). In the absence of international cybersecurity norms, cyberconflict persists virtually unchecked by the self-help remedies currently available to victim states (Roguski, 2020; Statement for the Record, 2016; Trautman, 2016; U.S. Department of State, 2016).

Scholars generally agree that unilateral actions to deter cyberconflict are ineffective because the costs imposed are insufficient to alter the behavior of responsible states (Kello, 2021; Lam, 2018; Tikk, 2018; Waxman, 2017). Cyberspace is a global resource connecting the CNI of every state, so cyberconflict is a global problem that requires an international solution (Davis, 2017; Shackelford et al., 2017; White House, 2018). International cybersecurity norms are necessary to establish standards for responsible state conduct that can be enforced by the international community (Broeders et al., 2022). Further, the effectiveness of these norms depends on consensus among the leading authoritarian and democratic states (Mazanec, 2015a). Only with full consensus can responsible states be held accountable (Painter, 2021; Mazanec, 2015a). Broad consensus in the international community avers that international cybersecurity norms are the best way to deter cyberconflict (Cyber Diplomacy Act of 2017, 2018; G7 Declaration on Responsible State Behavior in Cyberspace, 2017; United Nations, 2018; United Nations 2015a). Further, the international community has made considerable efforts to develop these political norms in international fora (e.g., U.N. General Assembly, Shanghai Cooperation Organization, Organization for Security and Cooperation in Europe). These efforts indicate international cybersecurity norms are feasible and desirable, but the problem persists (NATO Cooperative Cyber Defense Center of Excellence, 2019; Osula & Roigas, 2016; Sander, 2019).

Despite research on competing international cybersecurity norms, little research exists concerning the conditions necessary for those norms to emerge (Gualtier, 2015). The relevant research has focused primarily on the underlying cause of unregulated cyberconflict (Lantis, 2016; Mazanec, 2014a). Although the literature has indicated those causes, it has not provided a clear model for the emergence of new political norms to solve the problem. Kingdon’s multiple-streams framework (MSF) provides such a model, so it was employed as a lens to focus the current Delphi study and build on the works of Lantis (2016) and Mazanec (2014a). This study was intended to fill the gap in the literature with new knowledge from leading experts in the field. This knowledge may inform efforts to bridge the divide between democratic and authoritarian states so that international cybersecurity norms can emerge. Further, this study was the first application of the MSF and a Delphi study to international regulation of an emerging technology weapon. This research has broader significance to the emergence of international political norms for the regulation of emerging technology weapons like cyberweapons.

The sections of this chapter provide a summary of the literature regarding international cybersecurity norms and the purpose and nature of the study. The MSF is introduced as the theoretical framework (see Kingdon, 1995). The qualitative research question is discussed, key terminology is defined, and the assumptions and limitations of the study are identified. Finally, the significance of this study is discussed.

Background of the Study

State cyberattacks cover a wide spectrum of hostile state conduct referenced as cyberconflict (Kello, 2021; Mazanec, 2014b; Valeriano & Maness, 2015). Cyberconflict is the use of cyberattacks by states to advance their economic, political, and national security interests (Buchanan, 2020; Carlin, 2018; Sanger, 2018; Statement for the Record, 2021). State cyberattacks that cause physical damage to objects or injury to people are at the extreme end of the spectrum and are very rare (Patterson, 2014). Analysts refer to this subset of cyberattacks as cyberwarfare, a broadly used term that often conflates the most dangerous cyberattacks with lesser wrongful conduct (Fraser, 2016; Watkin, 2013).

However, experts argued less dangerous cyberattacks (e.g., espionage, subversion, or theft) are quite common (Devanny et al., 2021; Kaplan, 2016; Kello, 2017). Although not immediately threatening, the cumulative effect of these cyberattacks can damage national security over time (Carlin, 2015; Statement for the Record, 2015; U.S. Department of State, 2016). The Trump administration declared that U.S. adversaries were "recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world" (White House, 2018, p. 1). Former Director of the National Security Agency, General Alexander (Hearing to Receive Testimony on the Future of Warfare, 2015), called Chinese cyberattacks to steal intellectual property "the greatest transfer of wealth in history" (p. 55), costing U.S. companies $250 billion annually.

The unique nature of cyberconflict makes the application of international norms for this new form of hostile state conduct highly ambiguous and uncertain (Deeks, 2020; Haataja, 2013; Jensen, 2013; Schmitt & Vihul, 2016a). Large-scale cyberattacks against Estonia in 2007 drew worldwide attention to the problem for the first time (Davis, 2017; Shakarian et al., 2013). Sustained cyberattacks disrupted communications, commerce, and government services for three weeks (Davis, 2017). Despite the overt nature of the attacks, Estonia had difficulty classifying the conduct under existing international political and legal norms so it could allege a breach (Crandall & Allan, 2015; Segal, 2016). Estonia had no meaningful remedy under existing international norms because they had never been applied to a state cyberattack before (Czosseck et al., 2011; Li, 2013;

Russell, 2014). Many think Russia was responsible for the attacks (Davis, 2017; Rege, 2014) and similar cyberattacks against Georgia in 2008 (Biskner, 2018) and Kyrgyzstan in 2009 (Kozlowski, 2014). Many states have alleged other destructive and threatening state cyberattacks since these initial attacks (Healey & Grindal, 2013; Kello, 2017), and they are increasing in sophistication and destructiveness as cyberweapons evolve (Mok, 2017; von Heinegg, 2015). International cybersecurity norms are necessary to establish enforceable standards of conduct to regulate cyberconflict (Adamson, 2020).

In the absence of international cybersecurity norms, victim states must resort to self-help remedies: retorsions, countermeasures, and the use of armed force (Anderson, 2017; Roguski, 2020). Each of these coercive diplomatic solutions has features that make it ineffective. Countermeasures and the use of armed force are international legal norms I discuss in Chapter 2. Retorsions are lawful reprisals by one state against another (Lowe, 2016). Examples of retorsions include embargoes, tariffs, boycotts, and the expulsion of diplomats (Anderson, 2017). However, retorsions have proven to be ineffective deterrents because they fail to impose sufficient costs on the responsible state (Kello, 2021; Lam, 2018; Tikk, 2018). The domestic law of states is also an ineffective remedy because states are generally immune from the domestic laws of foreign states under the doctrine of state immunity (Foreign Sovereign Immunities Act, 1976; United Nations, 2004). The United States has unsuccessfully attempted to apply its domestic criminal laws to the individual agents responsible for state cyberattacks (*U.S. v. Dong, et al.*, 2014; *U.S. v. Hua and Shilong*, 2018; *U.S. v. Morenets, et al.*, 2018; *U.S. v. Netyksho, et al.*, 2018). However, states generally do not extradite their agents for trials before foreign courts for state cyberattacks. These cases are primarily intended to impose international political costs on the responsible state through public shaming (NATO Cooperative Cyber Defense Center of Excellence, 2019). Finally, victim states could respond with retaliatory cyberattacks to deter future state cyberattacks (White House, 2018). However, most scholars argue this strategy is ineffective because the virtual and covert nature of state cyberattacks removes the signaling necessary to communicate a credible threat of retaliation (Akdag, 2017; Lonergan, 2017; Nye, 2017).

The difficulty in regulating cyberconflict rests on the permissive nature of the international legal system. States are free to act as they wish in the absence of contrary international norms (Permanent Court of International Justice, 1927). When new technologies emerge that enable new forms of state conduct, new international norms must also emerge to regulate the new conduct (Klang, 2006; Lyytinen & Rose, 2003; Moses, 2007). A preponderance of states must reach a consensus regarding new standards of acceptable conduct (Schmitt & Vihul, 2016a; U.S. Supreme Court, 1900). These international norms take many forms, with legally binding norms (e.g., treaties, conventions, or customary law) at one end of the spectrum and politically binding norms (e.g., voluntary codes or United Nations declarations and resolutions) at the other (Schmitt & Vihul, 2016a; Shaffer & Pollack, 2009; Stockburger, 2016). The debate over international cybersecurity norms has focused on the development of politically binding norms (60-day Cybersecurity Review Team, 2009; Finnemore & Hollis, 2016; Sander, 2017).

The international community is deeply divided over international cybersecurity norms (Grigsby, 2017; Klimburg & Faesen, 2020; Krutskikh & Streltsov, 2014). Democratic states, led by the United States, consistently advocate for norms reflecting a free-enterprise governance model for cyberspace, International Human Rights Law, and the Law of Armed Conflict (LOAC) to regulate cyberconflict (Egan, 2016; Koh, 2012; Nye, 2014). In contrast, authoritarian states, led by Russia and China, consistently advocate for norms reflecting a state-dominated governance model for cyberspace, pervasive domestic security, and the international laws of sovereignty and nonintervention to regulate state cyberattacks (Broeders et al., 2019; Kleinwachter, 2012; Slack, 2016). While this struggle persists, a status quo of unregulated cyberconflict fills the void (Banks, 2016a; Buchanan, 2020; Taddeo, 2014).

To bridge the divide, the United Nations established a group of governmental experts (GGE) to develop international cybersecurity norms (Grigsby, 2017). In 2013, the GGE (including representatives from Russia and China) reached a consensus that, in principle, international legal norms apply state conduct in cyberspace (United Nations, 2013). Despite its promise as a forum for international cybersecurity norms, the GGE has not clarified what international legal norms should be used or how they should be applied to cyberconflict (United Nations, 2019). At the conclusion of the 2016–2017 GGE session, the U.S. representative stated

> I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their

> states are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions. (Markoff, 2017, para. 3)

Many other multilateral efforts have attempted to establish international cybersecurity norms without success (Grigsby, 2017; Radu, 2013). Consensus among authoritarian and democratic states is essential to the emergence of international cybersecurity norms (Mazanec, 2015a).

The International Code of Conduct for Information Security (the Code) is arguably the most notable attempt to establish international cybersecurity norms. The Code was adopted by Russia, China, and other authoritarian states in 2009 (Shanghai Cooperation Organization, 2009) and submitted to the U.N. General Assembly in 2011 and 2015 (United Nations, 2011, 2015b). The Code was rejected on both occasions because it failed to gather support among democratic states (Meyer, 2015; Tikk, 2016). Despite the Code's acceptance among authoritarian states, it has not been effective in regulating cyberconflict, and the norms it embodies were not gaining broader international support (Meyer, 2015). The Code illustrates the need for international cybersecurity norms that authoritarian and democratic states both embrace.

In summary, cyberspace has outpaced international legal and political norms, creating a regulatory gap that states are exploiting to advance their strategic interests (Buchanan, 2020; Schmitt & Vihul, 2016a). However, this void means states engaging in cyberattacks face a significant risk of miscalculation and conflict escalation (Li, 2013). Despite the danger to international peace and security that this paradigm represents, international cybersecurity norms have not emerged (Kulikova, 2022; Patterson, 2014).

Using the opinions of international cybersecurity experts and the MSF as a framework for analysis, I identified the critical points of disagreement among authoritarian and democratic states that must be addressed so that international cybersecurity norms can emerge. This knowledge may inform future norm entrepreneurship and may advance existing research regarding the emergence of international norms for other emerging technology weapons.

Problem Statement

States depend on the information and communication technologies (ICTs) that comprise cyberspace for the operation of their CNI (e.g., power, communications, and commerce; Dinniss, 2014). However, the complexity of ICTs makes them difficult to secure against state cyberattacks (Singer & Friedman, 2014). As a result, states are highly vulnerable to state cyberattacks (Finnemore & Hollis, 2016). For example, some experts have concluded that a state cyberattack on the United States power grid could cause catastrophic consequences for the nation (Panetta, 2012; Testimony of the Foundation for Resilient Societies, 2017). International political and legal norms normally regulate hostile state conduct of this kind (Moynihan, 2021; Theohary & Rollins, 2015). However, cyberconflict is so unlike other forms of hostile state conduct that the application of existing international political and legal norms is highly contested, leaving victim states with no effective deterrents (Banks, 2017; Macak, 2021). The lack of meaningful consequences for cyberconflict, and the high rewards derived from it, incentivize states to engage in this new form of hostile conduct (Mazanec, 2016; Moynihan, 2021). This paradigm invites conflict that is dangerous to international peace and security (E. Diamond, 2014; Kello, 2021).

The problem addressed in the current study was the persistent struggle between authoritarian and democratic states over competing international cybersecurity norms that cause cyberconflict to remain unregulated. Identification of the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms may inform future efforts to solve the problem. Researchers called for studies to fill this knowledge gap (Gualtier, 2015; Mazanec, 2014a).

Purpose of the Study

The purpose of this qualitative modified Delphi study was to determine the consensus opinion of a panel of international cybersecurity experts on the critical points of disagreement between authoritarian and democratic states regarding international cybersecurity norms. Toward that end, the MSF was employed as a lens to focus on the key factors in the problem, policy, and political streams of international cybersecurity norms (see Kingdon, 1995). This knowledge may inform future international norm entrepreneurship and may advance existing research regarding the emergence of international norms for other emerging technology weapons.

Research Question

The central research question for this study was the following: What are the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms that must be overcome for international cybersecurity norms to emerge? The following subquestions guided the study to answer the central research question:

1. What are the critical points of disagreement among authoritarian and democratic states in the problem stream for international cybersecurity norms?
2. What are the critical points of disagreement among authoritarian and democratic states in the policy stream for international cybersecurity norms?
3. What are the critical points of disagreement among authoritarian and democratic states in the political stream for international cybersecurity norms?

Theoretical Foundation

The MSF provided the theoretical framework for this study (see Kingdon, 1995). Political science scholars accepted Kingdon's (1995) model as a highly effective model for the study of the policy formation process. The terms *policy* and *norm* were used synonymously in the current study. The MSF is used to explain how and why political problems ripen for government action (Zahariadis, 2019).

Kingdon (1984) developed the MSF to explain national health and transportation policy formation processes in the United States. Since then, researchers have applied the MSF internationally and at all levels of government to diverse issues including housing, industry privatization, and foreign policy (Haacke, 2021; Liangliang, 2007; Rawat & Morris, 2016). In addition to post hoc analysis of successful policy adoption, scholars have used the MSF to gauge the potential for the adoption of new policy (i.e., norm emergence; Goyal et al., 2021; Sarmiento-Mirwaldt, 2015).

The MSF is based on the presumption that the conditions necessary for a new policy to emerge flows in three independent streams (problems, policies, and politics) that interact dynamically (Kingdon, 1995; Zahariadis, 2019). The problem stream focuses on political problems, (i.e., problems that can and should be solved by government action; Beland & Howlett, 2016). Problems gain the attention of policymakers in several ways, often when an issue becomes intolerable and a desire for action emerges (Herweg et al., 2018; Sarmiento-Mirwaldt, 2015). The policy stream supports ideas from the policy community to solve political problems (Beland & Howlett, 2016). Analysts debate and reshape these ideas as they flow through the policy network and compete with alternatives for acceptance (Zahariadis, 2017). The political stream contains the forces influencing the government decision-making environment at a particular point in time (Beland & Howlett, 2016). The national mood, organized political forces, and the composition of government are the primary political forces that interact to make problems more or less likely to receive the attention of policymakers (Kingdon, 1995; Zahariadis, 2019).

The streams interact dynamically and may be coupled by policy entrepreneurs under certain conditions (Ruvalcaba-Gomez et al., 2020; Zahariadis, 2003). Policy entrepreneurs attempt to create conditions favorable to their preferred policy solutions by manipulating conditions in the problem and political streams (Herweg, 2016). When the streams are coupled, a brief opportunity (policy window) exists to move a problem onto an agenda for government action (Beland & Howlett, 2016). Chapter 2 provides a more detailed explanation of this process and the MSF in general.

The MSF was ideal for the current study for two reasons. First, the MSF is used to explain the process through which policies emerge, which was central to this study. Second, the MSF theoretical propositions provided a well-focused framework for the analytical strategy that builds on existing empirical research.

Nature of the Study

A modified Delphi study was conducted to achieve the goals of this research. Qualitative studies are effective for probing phenomena that are difficult to quantify to derive meaning (Patton, 2014). A qualitative approach was appropriate for the examination of the international political problem that was the focus of the current study. Further, a Delphi study was the best approach for several reasons. First, the Delphi technique is a well-established group communication method building expert consensus on a complex problem (Bloor et al., 2013; Davidson, 2013). Next, the Delphi technique is effective in addressing problems that have little historical evidence, great complexity, and rapidly changing conditions that inhibit effective decision making (Franklin & Hart, 2007; Mishra & Mishra, 2014). Finally, the Delphi technique is effective in identifying the key variables of a phenomenon that can be manipulated to influence future outcomes (Barnes & Mattsson, 2016; Davidson, 2013; Okoli & Pawlowski, 2004). In short, a Delphi study was more appropriate for this research than any other approach.

Data collection for this study focused on iterative rounds of questionnaires combined with participant feedback to build consensus among the members of an expert panel (see Habibi et al., 2014). The expert panel was composed of purposefully selected experts in international cybersecurity norms. Rigorous selection criteria were used to ensure the representativeness of the sample. Snowball sampling mitigated researcher bias in participant selection and increased data quality (see Patton, 2014). Creswell and Creswell's (2018) model for qualitative data analysis was employed in each round of questions: prepare and organize, review, code, identify themes, develop narratives, and interpret. I relied on the theoretical propositions of the MSF as an analytical strategy to align with the research question.

Definitions

This section includes definitions of terms that were essential to understanding the central concepts of the research topic. I list these key terms alphabetically, followed by the operational meaning used in this study. Little consensus existed among scholars or the international community regarding key terms for state conduct in cyberspace (Mazanec, 2014b).

Attribution: The assignment of culpability for a cyberattack to the responsible state (Vasiu & Vasiu, 2017).

Critical national infrastructure (CNI): Physical and virtual infrastructure systems vital to national security, the national economy, and public safety and health (e.g., energy, financial system, and communications; Singer & Friedman, 2014).

Cyberattack: The adversarial use of digital information by a state to damage, destroy, or degrade the proper functioning of ICT in another state or to alter or steal information residing in ICT in another state (Hathaway et al., 2012).

Cyberconflict: A spectrum of cyberattacks employed to advance strategic state interests (Mazanec, 2014b). The effects of cyberattacks are benign at the low end of the spectrum (e.g., propaganda) and increase to severe at the high end of the spectrum (e.g., destruction of CNI), with effects comparable to those of conventional warfare.

Cyberspace: The sum of interconnected information and communications infrastructures (Mattis, 2018). In contrast, the internet comprises the networked systems that can be accessed by ordinary users (i.e., a subset of cyberspace; McGuffin & Mitchell, 2014).

Cyberweapon: Digital information designed to conduct a cyberattack (Sanger, 2018).

Emerging technology weapon: A new military capability based on the application of emerging technologies that enables states to engage in previously unknown forms of adversarial conduct (van Creveld, 2000).

Information and communications technologies (ICTs): Electronic devices, telecommunications components, computing applications, and systems that combine to form the global information environment in which users can interact with digital information (Dinniss, 2014; Kent, 2016). Cyberspace, the internet, mobile computing devices, and smart appliances that connect to the internet are examples of ICTs.

International cybersecurity norms: International political norms that deter cyberconflict (Mazanec, 2015a).

Norms: Widely accepted standards of behavior shared by members of a group (Austin, 2016; Carr & Carr, 2016).

State: A country recognized by the international community as having sovereign rights and authority over its territory, people, and affairs (Lowe, 2016).

Assumptions

I assumed that researcher bias did not negatively affect the collection and interpretation of the data and validity of the results. Purposive sampling, data collection, and data analysis carry a significant degree of risk, especially for a new researcher. My background as a lawyer and national security professional were additional considerations. I assumed that the potential threats to credibility were mitigated with the processes and procedures discussed in Chapter 3.

I assumed that the participants had sufficient expertise in international cybersecurity norms to provide high-quality data. Cyberconflict is a highly specialized policy area limited to a few scholars, government officials, and professionals in private industry. Rigorous selection criteria were employed to ensure the sample was representative.

I assumed that all participants would display candor and provide rich information. However, there was a small risk that the data would be affected by the classified nature of cyberconflict. Some participants may have had classified knowledge of cyberconflict. Thus, a lack of candor to protect classified information may have occurred. The unclassified nature of the research question and the questionnaires employed in data collection made this unlikely.

Scope and Delimitations

This study was limited in scope to identification of the critical points of disagreement among authoritarian and democratic states that must be bridged so international cybersecurity norms can emerge. The MSF provided the basis for organizing this research into three independent but interactive streams and the lens for examining the problem. Identification of the critical points of disagreement in the problem, policy, and political streams may inform future norm entrepreneurship. This knowledge may be used to shape conditions in the streams so that a coupling can occur, opening a policy window for international cybersecurity norms to emerge.

This study was bounded by the MSF. Other theories that have been applied to the study of cyberconflict include norm evolution theory (Mazanec, 2014a), rational choice theory (Goldsmith, 2013), and just war theory (Schmitt, 2011). These theories provide a solid basis to identify and define cyberconflict as a political problem to be solved with new international norms. However, these theories lacked a clear model to understand the norm emergence process that was central to the current study. The MSF provided that model. The clarity of the MSF made it well suited to the identification of critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms.

The results of this study may be transferrable to the development of international norms for other nonadversarial forms of state conduct in cyberspace. The findings may also be transferrable to the development of international norms for other emerging technology weapons. In either context, this study added to the understanding of how international norms for new forms of state conduct, enabled by emerging technologies, are adopted.

Limitations

Often scholars criticize qualitative research as lacking in academic rigor and transferability (Creswell & Poth, 2017). Qualitative studies are normally limited to their particular facts and circumstances (Creswell & Creswell, 2018). The intended transferability of the current findings was limited to cases with similar facts and circumstances (i.e., international norm emergence for emerging technology weapons). Researchers may mitigate transferability problems through the use of thick description and purposeful sampling (Anney, 2018). Thick description provides the reader with insight into the processes employed in the study to facilitate judgments regarding transferability (Keeney et al., 2011). Thick description also facilitates comparison of the context of the study to other circumstances (Guba, 1981). Thick description was enhanced in the current study using nonprobability sampling. Purposeful sampling provides richer findings than probability sampling methods (Anney, 2018). Further, the transferability of this study was also enhanced using theory (see Yin, 2017).

In qualitative research, the researcher is the primary instrument of data collection (Patton, 2014), significantly increasing the magnitude of the threat posed by researcher bias compared to other research designs. The first step in mitigating this threat is clarification of the personal bias the researcher brings to the study (Creswell & Creswell, 2018). My Western cultural norms as an American and my professional training and experience as a lawyer and officer in the United States Army were significant sources of potential bias. Next, confirmability is the degree to which a study’s findings are limited to the data and the phenomenon under investigation (Guba, 1981); that is to say, data analysis is not skewed by researcher bias (Anney, 2018). Researchers can establish confirmability using a reflexive journal to document the life cycle of the study (Anney, 2018). A reflexive journal is used to record processes, procedures, rationales for decisions, thoughts on research, plans for data collection, and tentative data interpretations. Researchers use this information to assess the potential influence of researcher bias on the study (Anney, 2018). Researchers commonly use a reflexive journal to enhance confirmability in Delphi studies (Hasson & Keeney, 2011). The participant checks included in the data collection process in a Delphi study also reduce bias by verifying the accuracy of the data (Franklin & Hart, 2007).

Significance of the Study

Researchers have studied the regulation of cyberconflict from many perspectives, but a gap persists in the understanding of why authoritarian and democratic states have failed to reach consensus regarding international cybersecurity norms (Gualtier, 2015). The scholarship on this issue was quite limited and focused primarily on the evolution of international political norms. Although researchers have defined cyberconflict as an international problem, they have not clarified why cyberconflict remains unregulated (United Nations, 2018, 2019). This is noteworthy because states acknowledge the dire nature of the threat posed by cyberconflict but tacitly prefer the existing paradigm.

Cyberconflict is dangerous to international peace and stability in many respects. State cyberattacks on CNI, intellectual property theft, erosion of free speech and privacy, and interference in democratic elections are serious security threats (Statement for the Record, 2021). Further, the magnitude of these threats is increasing as dependence on

ICTs deepens and state cyberweapons become more powerful (Trautman, 2016; Wirtz, 2017). Cyberconflict regulation is an urgent international problem (NATO Cooperative Cyber Defense Center of Excellence, 2019).

The results from the current study increase the understanding of the critical points of disagreement among authoritarian and democratic states that must be bridged so that international cybersecurity norms can emerge. This knowledge informs future international norm entrepreneurship and advances existing research regarding the emergence of international norms for other emerging technology weapons. The results of this study also indicate the divide between democratic and authoritarian states regarding international cybersecurity norms is too great to overcome in the near term, so other policy solutions should be pursued until conditions change. This study effects positive social change by contributing to international peace and security.

Significance to Practice

This study is significant to practice because the findings enable norm entrepreneurs to more effectively focus their efforts to create the conditions necessary for international cybersecurity norms to emerge. This knowledge also enables norm entrepreneurs to make better use of limited resources by focusing efforts on more promising policy solutions until conditions are ripe for a coupling of the streams. Active deterrence and increased passive cyberdefenses are imperfect solutions but may be better than the status quo. The findings of this study also inform the policy community regarding the critical points of disagreement between democratic and authoritarian states concerning international cybersecurity norms and contribute to the development of better policy solutions.

Significance to Theory

This study was the first application of the MSF to international norms for an emerging technology weapon. I nested the MSF in existing norm evolution theory to provide a clear model for the emergence of new norms or the modification of existing ones. I adapted existing theory to a new area of research and extended theory in a manner that may enhance its utility in understanding a new realm of problems. Understanding of international norm emergence for emerging technology weapons is in its infancy. Directed energy weapons, nanotechnology, and robotics are a few cutting edge technologies, like cyberweapons, that will require new international norms (Lantis, 2016). The adaptation and extension of the MSF in the current study may give it new utility in regulating the dangerous emerging technology weapons of tomorrow.

Significance to Social Change

The results of the study may be significant to positive social change because they may promote moral and ethical state conduct in cyberspace, thereby making the world a safer place for all people. The inability of states to protect citizens from the effects of cyberconflict is a serious problem. Without relative security in cyberspace, international tension will continue to build, and global prosperity will erode as the costs of adversarial state conduct mount. Further, in the worst case, a sophisticated state cyberattack on CNI can have devastating consequences for a developed state and its people. The second and third order effects to the global economy from such an attack could also be grievous.

International cybersecurity norms will make the world a safer place for all people (Crowe & Weston-Scheuber, 2015). The current study may effect positive social change by adding to the knowledge of the conditions necessary for those international norms to emerge.

Summary and Transition

Unregulated cyberconflict is a serious international problem (Broeders et al., 2022). Despite the magnitude of the threat, states have not closed this gap in international law. The scholarship on this issue is quite limited, so little is known regarding why this paradigm persists. Identifying the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms may inform future efforts to create the conditions necessary to effectively regulate cyberconflict.

This study decreases the knowledge gap in the literature and contributes to future policy action to regulate cyberconflict. Using the opinions of international cybersecurity experts and the MSF as a framework for analysis, I identified the critical points of disagreement among authoritarian and democratic states that must be bridged so international cybersecurity norms can emerge. This study may create positive social change by enabling efforts to close the gap in international law, thereby contributing to international peace and security that benefits all people.

The following chapter includes a review of the literature regarding cyberconflict and indicates the gap this study filled. The problem is introduced and the literature search strategy is discussed. Next, the MSF is detailed to provide clarity and structure to this Delphi study. Then, the perspectives of scholars and states regarding the nature and scope of the problem are explored. Finally, the policy goals and political interests of authoritarian and democratic states are analyzed.

Chapter 2: Literature Review

This literature review highlights the danger of unregulated cyberconflict and the challenge that must be overcome for international cybersecurity norms to emerge. Efforts to mitigate the problem are explored in detail, along with the diverging security interests of democratic and authoritarian states. The theoretical propositions of the MSF are explained to connect several different areas of research, creating synergy to decrease the gap in the literature regarding the research problem.

The emerging technologies of the information and telecommunications revolution have improved the quality of life of people across the world but have also created a broad spectrum of new dangers. Chief among these dangers is state cyberattacks (Global Perspective on Cyber Threats, 2015; Westerburger, 2014). Cyberconflict is a new form of adversarial state conduct unimagined and impossible before the rise of cyberspace. Cyberconflict is so unlike other forms of adversarial state conduct that it is virtually unregulated (Banks, 2016a; Dev, 2015; Kello, 2021). The result is a permissive environment for cyberconflict that is dangerous to international peace and security (Broeders et al., 2022; Danca, 2015; Mazanec, 2015a). Despite this danger, states have not established new international legal or political norms to address the problem (Finnemore & Hollis, 2016; Painter, 2021; Radu, 2013).

Societal dependence on ICTs and cyberspace is accelerating as ICTs increase in power, decrease in price, and penetrate more deeply into society (Dinniss, 2014). These technologies are so ubiquitous that the physical and virtual worlds are converging (Finnemore & Hollis, 2016). Although this convergence frees people from routine tasks, when technology fails, the consequences can be severe (Wallach, 2015). Developed states are now completely dependent on ICTs and cyberspace for essential private and public functions, from the operation of CNI to national security (Hendrickson, 2015; Trautman, 2016; Wirtz, 2017). As this dependence increases, so does vulnerability to cyberconflict (Ayalew, 2015; Kent, 2016; van der Meer, 2015). Although this new form of conflict is in its infancy, its destructiveness is increasing as cyberweapons become more sophisticated and dependence on cyberspace grows (Mazanec, 2015b; Sanger, 2018).

The literature indicated that states are engaging in cyberconflict to advance their strategic interests (Buchanan, 2020; Meyer, 2015; Vasiu & Vasiu, 2017). The willingness of states to launch cyberattacks makes them the greatest threat in cyberspace (Global Perspective on Cyber Threats, 2015; Trautman, 2016). An invisible cyberarms race is causing a rapid increase in the effectiveness and destructive power of cyberweapons (Singer & Friedman, 2014; von Heinegg, 2015). At the same time, defensive technologies are lagging, creating a widening vulnerability gap (Mok, 2017). Emerging ICTs of the near future (e.g., quantum computing and artificial intelligence) are expected to intensify the problem by expanding the advantage of cyberweapons over cyberdefenses (Simmons, 2014). The gap between offense and defense is already so great that experts argue CNI cannot be secured (Department of Defense, Defense Science Board, 2013; Williams & Fiddner, 2016). This makes cyberconflict a top national security threat for developed states (Chayes, 2015; Foltz, 2012; Moynihan, 2021).

However, a minority of scholars argue that the magnitude of the threat is overstated (Gray, 2013; Mok, 2017; Roigas, 2015). In their view, states are not causing significant damage with cyberattacks, so cyberconflict is not a significant national security threat (Mok, 2017). This logic is flawed in two important ways. First, this logic confuses the low probability of a catastrophic cyberattack with its potential severity (Kshetri, 2014; Shakarian et al., 2013; Trautman, 2016). Second, it assumes states are exercising restraint and will continue to do so. Recent highly destructive state cyberattacks on CNI (e.g., Operation Olympic Games and Saudi Aramco) indicated this is unlikely (Bronk & Tikk-Ringas, 2013; Deeks, 2020; Richmond, 2012).

ICTs are insecure because of their complexity (Singer & Friedman, 2014). Systems also become more complex and more insecure as they are networked and grow (Trautman, 2016). This paradigm makes it impossible to anticipate or identify every security flaw (Finnemore & Hollis, 2016; Goldsmith, 2013). The complexity of modern ICTs means no technical solutions exist for their vulnerability (Mazanec, 2016). As soon as technicians patch a vulnerability, another emerges and the patches sometimes create new vulnerabilities (Wirtz, 2017). Further, even if technological solutions were perfected, ICTs would still be vulnerable to human threats (e.g., hostile insiders and human engineering; Trautman, 2016).

The United States is vulnerable to cyberattacks on its CNI, and this is particularly true of the power grid (Litwak & King, 2015; van Dunk, 2020). Modern society is dependent on electrical power (National Academies of Sciences, Engineering, and Medicine, 2017), but the power grid depends on automated control systems that are vulnerable to cyberattacks (Bhusal et al., 2021; Sood & Enbody, 2014). Experts agreed that a sophisticated cyberattack on the U.S. power grid can cause prolonged and widespread power outages, crippling the country (Clarke & Knake, 2011; Panetta, 2012; Weiss & Weiss, 2019). Power loss of that magnitude could quickly make basic necessities (e.g., water, food, communications, and emergency services) unavailable (Kavan et al., 2021; Petermann et al., 2014; Testimony of the Foundation for Resilient Societies, 2017). If that occurred, law and order would begin to erode as desperate people turned to looting in the absence of state authority (Foster et al., 2008; Pry, 2017). If electricity was unavailable for a year, government reports estimate that 90% of the U.S. population could die, primarily from starvation (Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2017; North Korea Nuclear EMP Attack, 2017; Task Force on National and Homeland Security, 2020). Although such an estimate is speculative, the danger is real.

A catastrophic cyberattack on the U.S. power grid is not merely a hypothetical scenario (Brenner, 2017; Carlin, 2015; Weiss & Weiss, 2019). The United States Department of Energy has demonstrated that cyberattacks can cause catastrophic damage to electric power generators (Bernabeu & Katiraei, 2011; Kiyuna & Conyers, 2015; Troelsen, 2007). The vulnerability exploited in that research is common to power grids worldwide, and few power generation companies have added the security required to mitigate it (H. E. Brown, 2017). Further, experts agreed that a sophisticated cyberattack on only a few key power substations can cause a cascading failure of the entire United States power grid (Buldyrev et al., 2010; Shakarian et al., 2014).

United States Cyber Command has confirmed that China and Russia have the capability to collapse the United States power grid for prolonged periods (Hearing to

Receive Testimony on the Future of Warfare, 2015). China and Russia are also known to have implanted latent cyberweapons in sensitive United States power grid control systems for future exploitation (Cybersecurity and Infrastructure Security Agency, 2018; Hendrickson, 2015; Lee, 2013; Nguyen, 2013). Russia has also demonstrated a willingness to engage in cyberattacks on another state's power grid. In 2015 and 2016, Russia attacked Ukraine's power grid, causing limited duration power outages for hundreds of thousands of people (Cybersecurity and Infrastructure Security Agency, 2016; Grigsby, 2017; Shackelford et al., 2017). Although limited in scope, these attacks demonstrated the capability and communicated a dire threat to developed states.

It is difficult to overstate the magnitude of the national security threat posed by cyberconflict. The CNI of developed states is vulnerable to cyberattacks that can cause catastrophic consequences. Further, the lack of consequences and high rewards for cyberconflict incentivize risk-taking by aggressive states. The result is a dangerous paradigm, ripe for international conflict with severe consequences.

I divided this chapter into four major parts. The first part is a discussion of the theoretical framework employed in this Delphi study. The next three parts present a review of the literature concerning cyberconflict in its problem, policy, and political streams.

Literature Search Strategy

I relied on a diverse array of primary and secondary sources to complete this literature review. Google Scholar, FindLaw, Walden University library databases, Social Science Research Network, and JSTOR were key sources for peer-reviewed journal articles, international law, court cases, government policies, and other materials. An array of books by cybersecurity experts in government, academia, and private industry were also included in this chapter. Keywords employed in Boolean searches included *jus ad bellum*, *law of armed conflict*, *armed attack*, *use of force*, *cyberattack*, *Stuxnet*, *cyberspace*, *information warfare*, *cyberwarfare*, *cyberdiplomacy*, *cybernorms*, *cybertreaty*, *conflict analysis*, *policy streams*, and *agenda setting*. Additional journal articles were obtained by checking the Google Scholar citations to relevant sources and locating sources cited within articles.

Theoretical Framework

Researchers use many frameworks to examine the policy process from different perspectives. Despite the diversity in approaches, scholars generally agree that the policy process comprises six sequential stages: problem identification, agenda setting, policy development, adoption, implementation, and evaluation (Theodoulou & Cahn, 2012). However, scholars disagree on how the stages interact. The MSF provides a model to examine the dynamic interplay between the first four stages (Zahariadis, 2019). Through this examination, the MSF answers three important questions: how the limited supply of government attention is rationed, how competing ideas mature into viable policy alternatives, and what conditions cause problems and solutions to ripen for government action when they do (Zahariadis, 2017).

Although initially applied to the United States government, the MSF has been applied to public policy processes at all levels of government around the world (including in authoritarian states) on diverse issues from health care to foreign policy (Haacke, 2021; Liangliang, 2007; Rawat & Morris, 2016). In addition to explaining the conditions present for successful policy adoption, analysts have also used the MSF to gauge the potential for new policies to emerge (Goyal, 2021; Sarmiento-Mirwaldt, 2015). For example, the MSF has been used to identify obstacles to the emergence of housing policy in Australia (Tiernan & Burke, 2002) and the development of European Union cohesion policy (Sarmiento-Mirwaldt, 2015). The MSF has also been found useful in the development of viable foreign policy alternatives (Haacke, 2021; Neumann, 2006). These studies indicated the extension of the MSF to international cybersecurity policymaking can be beneficial.

The MSF is well suited to the analysis of ambiguous problems with numerous stakeholders who must cooperate to develop solutions (Sarmiento-Mirwaldt, 2015). Ambiguity is a condition caused by having many valid ways of considering an issue, some of which may conflict, causing confusion and ambivalence (Zahariadis, 2003, 2019). Policymakers often have limited knowledge regarding the consequences of their decisions, so they accept political risk when adopting or rejecting policy proposals (Sarmiento-Mirwaldt, 2015). Ambiguity is, however, a persistent condition in political processes that cannot be resolved with more or better information about the issue under consideration (Zahariadis, 2017).

The MSF rests on the assumption that the conditions necessary for the adoption of policy emerge from three independent streams flowing through the policy process: problems, policies, and politics (Kingdon, 1995). The streams interact and may be coupled by policy entrepreneurs under certain conditions (Ruvalcaba-Gomez, 2020;

Zahariadis, 2003). When this occurs, an issue can be moved onto an agenda for government action (Beland & Howlett, 2016).

Agendas

Society has multiple problems that demand the attention of policymakers. However, political systems have limited throughput, so only a limited set of problems can be considered and acted on. It is essential to understand how a problem like cyberconflict enters the decision agenda (Kingdon, 1995). To reach the decision agenda, a policy entrepreneur must couple at least two streams and a policy window must open (Zahariadis, 2017).

Policy Windows

A policy window is when conditions are favorable for policymakers to act on a problem (Kingdon, 1995). These opportunities emerge when significant changes occur in the problem or political stream (Kingdon, 1995). For example, policy windows can be opened as information about problems emerges, institutional events occur (e.g., elections and budgets), or the activities of policy entrepreneurs are effective (Beland & Howlett, 2016). An open window presents a brief opportunity for policy entrepreneurs to move their policies onto the decision agenda by coupling the streams (Herweg, 2018; Zahariadis, 1996).

Policy Entrepreneurs

The policy process is a struggle to control the meaning or creation of norms (Deitelhoff & Zimmermann, 2013). These contests are characterized by ambiguity that is resolved by establishing meaning rather than more or better information about problems and policies (Zahariadis, 2017). Policy entrepreneurs exploit this condition to provide meaning that shapes the conditions in the streams to their favor (Beland & Howlett, 2016). When successful, the policy entrepreneur couples the streams, opening a policy window to move a preferred policy onto the decision agenda (Ruvalcaba-Gomez, 2020; Zahariadis, 2003).

Problems

Because the limited supply of government attention is rationed, an issue must first be a political problem; in other words, the problem can and should be solved by government action (Beland & Howlett, 2016). Many problems are so undefined or contested that policy solutions are unavailable. Next, a problem must be more significant than a persistent condition. A condition is a tolerable issue that is accepted as normal and endured (e.g., unemployment or homelessness). However, conditions can become political problems when they change in a manner that makes them intolerable (Goyal, 2021; Kingdon, 1995).

Policies

Competing ideas mature into viable policy alternatives as the policy stream is filled with ideas from the policy community to solve political problems (Beland & Howlett, 2016). The policy community is the network of experts and specialists in a particular field who generate and share ideas about problems (Herweg, 2016). Stakeholders debate and reshape these ideas as the ideas flow through the network and compete with alternatives for acceptance (Zahariadis, 2017). Ideas that are feasible (i.e., can be successfully implemented) and acceptable to the policy community (i.e., coherent within existing norms) are more likely to emerge as policy proposals (Kingdon, 1995).

Politics

The conditions that cause problems and solutions to ripen for government action include the political stream composed of forces that influence the government decision-making environment at a particular point in time (Beland & Howlett, 2016). The national mood, organized political forces, and the composition of government are the primary political forces that interact to make problems more or less likely to receive attention (Herweg, 2018; Kingdon, 1995). National mood is the prevailing desire in the electorate for increased attention to certain problems and decreased attention to others (Zahariadis, 2019). Despite the volatility of the national mood, policymakers believe they can accurately gauge it and direct attention to problems and policy proposals accordingly.

Organized political forces include special interests, lobbyists, and activists. The attitudes of these groups reflect larger trends in the electorate (Zahariadis, 1996). The balance of consensus and opposition among these groups on problems and policies influences the attention of policymakers (Seaman, 2013). Finally, the composition of government is the distribution of executive and legislative power to political factions and associated government officials. As elections redistribute political power and turnover changes the composition of institutions, agendas change and new policy windows open (Kingdon, 1995).

The MSF provides a well-established model for the analysis of the policymaking process. The MSF enables a separate analysis of each stream in the policy process that identifies obstacles to the emergence of international cybersecurity norms. Better knowledge of these obstacles informs future policy entrepreneurship and may contribute to successful coupling of the streams and the emergence of new norms.

Cybersecurity Problems

Although the literature concerning international cybersecurity policy is diverse, researchers consistently explore two distinct sets of problems: legal ambiguities and litigation uncertainties (Beard, 2014; Haataja, 2013; Jensen, 2013; Schmitt & Vihul, 2016a). For legal ambiguities, scholars generally agree that the predominantly nonviolent nature of cyberconflict makes it difficult to classify cyberattacks (i.e., war vs. wrongful conduct) so that the appropriate legal regime can be applied (Haataja, 2013; Macak, 2021; Palmieri, 2016). For litigation uncertainties, scholars generally agree that the inability to reliably attribute cyberattacks to responsible states makes it extremely difficult to enforce international law (Banks, 2016b; Haataja, 2013; Kello, 2021).

Legal Ambiguities

States lack consensus regarding what international laws should be applied to state cyberattacks (Calo, 2015; Frederick & Johnson, 2015; Preston, 2016; Roguski, 2020). Cyberconflict blurs the line between acts of war and lesser wrongful acts, making the classification of state cyberattacks a highly contested political issue (Chayes, 2015; Kello 2021). The LOAC or the customary international laws of nonintervention and sovereignty could be used to reasonably regulate cyberconflict (Huang & Macak, 2017; Roguski, 2020; von Heinegg, 2013).

The accurate classification of cyberattacks is essential to determine what legal regime should be applied (Deeks, 2020; Fraser, 2016; Schmitt, 2013b), however, the term cyberattack has no standard definition (Kadivar, 2014). Instead, stakeholders loosely use the term to describe a vast array of malicious conduct in cyberspace (Vasiu & Vasiu, 2017), ranging from cybercrimes by individuals to violent and destructive cyberattacks by states. This conflation confuses the classification of cyberattacks with the consequences that might be appropriate for the hostile conduct (Kello, 2021; Patterson, 2014).

The term cyberconflict provides much needed clarity by separating adversarial state conduct from all other forms of malicious conduct in cyberspace. However, such a definition is merely a beginning point in the classification process. Cyberconflict is a spectrum of state cyberattacks that produce effects with varying degrees of severity (Mazanec, 2014b). Destructive cyberattacks that threaten national security are at the extreme end of the spectrum and includes the catastrophic cyberattack on CNI previously discussed. Nonviolent cyberattacks that do not threaten national security in the near term occupy the other end of the spectrum. Most activity at this end of the spectrum are cyberespionage, which is not proscribed by international law, but is illegal under the domestic law of states (Devanny et al., 2021; Patterson, 2014). The effects of a very limited category of cyberattacks can be classified as acts of war (i.e., a Use of Force under art. 2(4) of the U.N. Charter), whereas classification of the vast majority of cyberattacks remains ambiguous.

All cyberattacks entail conduct that is already unlawful under domestic or international law (Schmitt, 2013b). The virtual nature of cyberattacks disrupts the classification because cyberattacks produce little evidence to infer their purpose (E. Diamond, 2014). Cyberattacks are a radical departure from existing norms for the classification of crimes rooted in the physical world (Chayes, 2015). As a result, scholars exploring classification challenges have focused heavily on the effects cyberattacks produce (Kadivar, 2014; Kremer & Muller, 2013). Much of the literature narrowly focused on the classification of cyberattacks as an act of war.

Many states have adopted an effects-based framework as their preferred classification method (Koh, 2012; Preston, 2016; Schmitt & Vihul, 2017b; U.S. Department of Defense, 2011). The framework evaluates eight factors to classify cyberattacks: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality (Roberts, 2014; Schmitt & Vihul, 2017b). Severity is the dominant factor because it assesses the harm caused by the scale, scope, intensity, duration, and effects of a cyberattack (Schmitt, 2011; Schmitt & Vihul, 2017b). Cyberattacks that produce violent kinetic effects are more likely to be classified as a use of force crime (Schmitt & Vihul, 2017b). This standard fails to classify nonviolent cyberattacks with severe consequences (McGhee, 2013) and leaves the classification of most state cyberattacks in dispute.

Litigation Uncertainties

The unique nature of cyberattacks creates a degree of litigation uncertainty that disconnects international law from cyberconflict (Banks, 2016b; Dev, 2015). Facts essential to reliably assign responsibility for cyberattacks to responsible states are obscured by the virtual nature of cyberspace (Eichenser; 2020; Lin, 2016). Without reliable attribution, international law cannot be enforced (Brown & Friedman, 2014; Derian-Toth et al., 2021; Stevens, 2017). Further, the lack of consequences incentivizes states to engage in cyberconflict to advance their strategic interests (Cavelty, 2014; Jasper, 2015; Kello, 2017).

Multiple challenges impede the collection of evidence necessary for reliable attribution (Beard, 2014; Lin, 2016). First, attackers can conceal the identity of their computer through technical means (Dinniss, 2014). The value of electronic evidence is also questionable because it can be easily altered (Yetter, 2015). Sophisticated attackers can create false evidence that implicates innocent states (Vasiu & Vasiu, 2017). States responsible for cyberattacks do not cooperate with investigations, so essential evidence cannot be collected (Shah, 2015; von Heinegg, 2013). If those challenges are overcome, the computer operator must be identified through technical means or intelligence collection (Vasiu & Vasiu, 2017). Finally, even when the human operator is identified, the responsible state may remain unknown. States often conduct cyberattacks through proxies to create deniability (Biskner, 2018; Giles & Monaghan, 2015).

Achieving the degree of proof necessary to attribute cyberattacks to states is also a serious challenge. Universal evidentiary standards of admissibility and proof do not exist in international law (Lin, 2016; Roguski 2020). In essence, a head of state must make a political decision based on intelligence assessments (Eichensehr, 2020; Lin, 2016). Because no legal process exists, the only standard is reasonableness, based on all facts and circumstances available at the time to the decision-maker (Lin, 2016; Roguski 2020). Reasonableness requires convincing evidence when states are accused of serious offenses that warrant substantial sanctions (International Court of Justice, 1949, 1986; Schmitt & Vihul, 2014). The challenges involved in collecting evidence for state cyberattacks makes it extremely difficult for states to meet this burden of proof.

Cybersecurity Policies

States and scholars generally agree that international law applies to state conduct in cyberspace (Giles, 2017; Markoff, 2017; von Heinegg, 2015). However, states are deeply divided on what international laws are appropriate to regulate cyberconflict (Caton, 2014; Preston, 2016; Frederick & Johnson, 2015). Policy solutions generally take two forms. First, scholars attempt to extend existing international law to cyberconflict by analogy (Boyle, 2016; Schmitt & Vihul, 2016a). Second, states develop nonbinding political agreements (e.g., codes of conduct) to regulate state cyberattacks (Eichensehr, 2014; Murphy, 2013). These evolutionary approaches seek to establish new international norms (i.e., customary international law; Schmitt & Vihul, 2016a).

Customary international law is unwritten law that slowly emerges over time through the practice of states (Lowe, 2016; Schmitt & Vihul, 2016a; U.S. Supreme Court, 1900). In essence, a custom may ripen into law through the normal practice of a preponderance of states and compliance with the custom out of a sense of legal obligation (International Journal of Justice, 1985; U.S. Supreme Court, 1900). Nonbinding political agreements seek to set new standards for state conduct in cyberspace, whereas scholars seek to establish the necessary legal obligation states must observe. However, the highly classified nature of cyberconflict makes it quite difficult to verify compliance with any new norm, so customary international law is unlikely to emerge in the near term (Beard, 2014; Macak, 2017).

Scholarship

While the political struggle to establish norms persists, legal scholars attempt to extend existing international law to cyberconflict by analogy (Beard, 2014; Kello, 2021; Patterson, 2014). The LOAC, sovereignty, noninterference, and countermeasures are the most often discussed bodies of law in this regard (Roguski; 2020; Shibo, 2014). However, the analogies offered generally alter these laws to a degree that undermines their legitimacy (Finnemore & Hollis, 2016; Mueller, 2014).

Research regarding the application of the LOAC to cyberconflict permeates the literature. In general, the LOAC seeks to maintain international peace and security by banning war (i.e., the use of force) as a legitimate means to settle international disputes (Crawford & Pert, 2015; Dinniss, 2014). In most cases, a state must be the victim of a use of force before it can resort to armed force in self-defense (Preston, 2016; Stockburger, 2016). Although this appears to be a simple analysis, the term *use of force* is poorly defined (Garrie, 2012; Schmitt & Watts, 2015), complicating the classification of new forms of hostile state conduct and making the applicability of the LOAC controversial (Liivoja, 2016; Preston, 2016). A use of force that does not resemble conventional warfare (ex., World War II) calls the application of the LOAC into question (E. Diamond, 2014; Wallach, 2015). Legal scholars have struggled for more than a decade to create persuasive analogies between the established meaning of a use of force (i.e., the violent use of weapons resulting in severe physical damage to objects or injuries to persons) and state cyberattacks (Chayes, 2015; Dev, 2015; Schmitt, 2011).

Legal scholarship has led to a limited agreement among states that the LOAC regulates the most dangerous form of state cyberattacks (Preston, 2016; Schmitt & Vihul, 2017a). In essence, state cyberattacks that produce effects similar to a conventional use of force should be regulated by the LOAC (Schmitt & Vihul, 2017a). However, significant flaws in the analogy make it controversial (Patterson, 2014; Rid & Arquilla, 2012). First**,** cyberweapons are unlike conventional weapons in form and effect. Second, state cyberattacks can produce severe effects without the use of violence (Liivoja et al., 2015; Schmitt, 2012), undermining the analogy because it arguably extends the LOAC to other lawful state conduct that also causes severe effects without violence (e.g., embargos and sanctions).

Cyberweapons present unique challenges to the established legal meaning of what constitutes a weapon (Mele, 2014). For centuries, the capacity of a tangible instrument to cause violent effects characterized weapons of war. However, in the last century, weapons that are not readily observable and lack violent effects emerged (e.g., biological and chemical weapons; Watkin, 2013). These weapons concealed the cause-and-effect relationship that is normally evident when adversaries employ conventional weapons. The international community responded by banning these weapons with treaties (United Nations, 1972). However, cyberweapons are merely digital information, so they cannot be so easily regulated.

Many scholars argued that the International Court of Justice Nuclear Weapons Case extends the LOAC to cyberweapons and resolves the issue (Beard, 2014; Dinniss, 2014). In that case, the Court held that the LOAC applies to any use of force, regardless of the form of the weapon employed (International Court of Justice, 1996). However, this decision ignores the United Nations Charter's focus on the instrument used to cause violence. The framers of the United Nations Charter wanted to regulate war and used the conventional instruments of war to clearly define the proscribed conduct (Beard, 2014; Dunoff & Rattner, 2015). Removing the nature of the instrument from the analysis calls the established meaning of the term use of force into question (Murphy, 2013; Waxman, 2013).

In addition, the Court's holding did not erase the requirement that a weapon must be employed to constitute a use of force. The issue before the Court was the applicability of the LOAC to nuclear weapons. Although a new technology at the time, nuclear weapons unquestionably cause extremely violent effects. A direct cause and effect relationship was easily attributed to the instrument, making nuclear weapons analogous to other weapons. In contrast, the causal link between cyberweapons and their effects is tenuous and generally nonexistent (Taddeo, 2014). Cyberweapons cause target ICTs to behave in a manner contrary to their intended purpose, rendering the targeted system the instrument that causes the attacker's desired effect (Eichensehr, 2015; Garrie, 2012). Thus, cyberweapons are arguably not weapons at all, rather they are a method of warfare (Biller & Schmitt, 2019).

Further, state cyberattacks can cause severe effects without the violence normally associated with a use of force (Fidler, 2012; Schmitt, 2013b). Legal scholars argue that the more the effects of a state cyberattack resemble conventional war, the more likely the attack will constitute a use of force (Schmitt, 2012; Schmitt & Vihul, 2017b). Some scholars liberally extended this analogy to any state cyberattack with severe effects, regardless of violence (Piatkowski, 2017). This reasoning radically expands the scope of the LOAC and calls into question the classification of other hostile conduct with severe effects that has always been lawful (e.g., embargos and economic sanctions; Beard, 2014). Political and economic coercion were specifically excluded from the meaning of force when the United Nations Charter was drafted (Remus, 2013; Yoo, 2015).

Many scholars believe expanding the scope of the LOAC in this manner is dangerous (Schmitt, 2012). First, a broader definition of force would make the identification of prohibited conduct more difficult, blurring the line that separates military hostilities from other permissible forms of hostile conduct (Dinniss, 2014). This could destabilize the LOAC framework by destroying the current consensus among states regarding the use of force and undermine the humanitarian protections it provides (Banks, 2016a; von Heinegg, 2013). Further, confusion over an ambiguous new threshold for the use of force would inevitably result in innocent noncompliance (Dunoff & Rattner, 2015).

Consensus is emerging that the LOAC is only appropriate for a very rare class of cyberattacks, so other approaches are required to regulate cyberconflict (Geib & Lahmann, 2013; Hollis & Neutze, 2020; Schmitt & Vihul, 2017b). Researchers offer the laws of nonintervention, sovereignty, and countermeasures as alternatives (Corn & Taylor, 2017; Grigsby, 2017; Roguski, 2020). However, like the LOAC, the analogies are inadequate, and states remain divided on their application (Klimburg & Faesen, 2020; Ohlin, 2016).

The law of nonintervention prohibits activities that exert a coercive effect on the economic, political, or cultural system of another state (International Court of Justice, 2005; United Nations, 1981). An activity is coercive if the victim state is compelled to act in a manner it would not freely choose (Ohlin, 2016). However, the threshold between coercive activities and other lesser activities has never been clearly defined (Stockburger, 2016). Propaganda and disinformation campaigns are well established in international law as lawful activities (Kilovaty, 2018). In contrast, a subversion campaign to change the political system of a state by inciting revolution is unlawful (United Nations, 1970; Watts, 2015).

Scholars argue that the law of sovereignty applies to noncoercive cyberattacks. These attacks fall into two categories: violation of territorial integrity and usurpation of inherently governmental functions (Schmitt & Vihul, 2017a). However, it is unclear which cyberattacks might violate these prohibitions (Schmitt & Vihul, 2017a). Consensus exists that physical damage to objects or injury to persons must occur for a cyberattack to violate a state's territorial integrity (Schmitt & Vihul, 2017a; Watts, 2015). In contrast, cyberattacks that usurp inherently governmental functions are poorly defined, but interference in a state's administration of an election or its ability to determine election results have been offered as examples (Broeders, 2021; Egan, 2016).

Cyberattacks that violate the law of nonintervention or sovereignty are internationally wrongful acts that may empower the victim state to engage in countermeasures (United Nations, 2001). These self-help remedies would otherwise be illegal under international law (Schmitt & Vihul, 2014). To lawfully resort to countermeasures, a victim state must first demand that the responsible state cease the wrongful activity (Schmitt, 2013a). If the responsible state persists, the victim state can employ necessary, proportional, and nonpunitive countermeasures to restore compliance with international law (Geib & Lahmann, 2013).

The use of countermeasures to deter cyberconflict is problematic in three important ways (Simmons, 2014). First, victim states must still attribute the cyberattack to the responsible state with convincing evidence (Schmitt & Vihul, 2017b). As previously noted, this is an extremely difficult burden to meet and takes considerable time to achieve. Second, the victim state must demand that the responsible state cease the cyberattack before resorting to countermeasures. The covert nature of cyberconflict makes such demands extremely rare, and the cyberattack is normally complete by this time. Finally, the delay in detecting a cyberattack and establishing attribution calls the necessity of countermeasures into question (Banks, 2016b).

Ultimately, this framework suffers from the same weaknesses as the LOAC. The virtual nature of cyberweapons makes the application of the customary international laws of nonintervention, sovereignty, and countermeasures highly ambiguous (Kello, 2021). New state practices must emerge to correct the problem, but the covert character of cyberconflict conceals it. Despite its challenges, this framework may have a greater chance of gaining widespread acceptance because it has wider application than the LOAC. Further, countermeasures provide victim states flexible response options that are less dangerous than the use of force.

Codes of Conduct

States and scholars point to codes of conduct as the most viable approach to address uncertainties in the application of international law to cyberconflict (60-day Cybersecurity Review Team, 2009; Sander, 2017). Codes of conduct are well suited to fill emerging gaps in international law like those created by cyberconflict (G. Brown & Poellet, 2012; Finnemore & Hollis, 2016). Codes of conduct have consistent characteristics: they are quickly developed; highly adaptable; inexpensive to create and maintain; they are nonbinding, with political consequences for breaches; have low sovereignty costs; and are good at regulating poorly defined problems with changing conditions (Krisch, 2014; Shaffer & Pollack, 2009). Codes of conduct afford states an opportunity to experiment with new norms that are easily modified as circumstances change (Slack, 2016). Despite many efforts to develop a cyber code of conduct, states have consistently rejected them (Caton, 2014; Etzioni, Painter, 2021; 2013; Shibo, 2014). Further, the literature reflects a consensus that a cyber code of conduct is unlikely to emerge in the near term (Kulikova, 2021; Macak, 2017; Shackelford et al., 2015).

Cybersecurity Politics

The international community is increasingly polarized as democratic and authoritarian states struggle to control international policies to advance their strategic interests (Broeders et al., 2019; Inboden & Chen, 2012; Zeng et al., 2017). After the collapse of the Soviet Union, the United States and its liberal democratic allies (democratic states) emerged as the leading world powers (Bernard, 2016; Cooley, 2015b). However, China and Russia have organized a loose coalition of competing authoritarian states (Broeders et al., 2019; Horvath, 2016; Zeng et al., 2017). These states promote policies that prioritize national sovereignty and Eastern cultural values (Mead, 2014).

Senior national leaders and powerful international interest groups shape the international political environment with competing cybersecurity narratives (Arimatsu, 2012; Giles, 2017). These narratives define the problem posed by cyberconflict in fundamentally different ways that require different policy solutions (Austin et al., 2015; Goychayev, 2014; Klimburg & Fasen, 2020). The political contest for control of international cybersecurity norms is one of the most salient international policy issues of the 21st century (Eichensehr, 2014; Moynihan; 2021; Radu, 2013). Although cyberconflict is a serious problem, a change in a few key norms to increase security could profoundly change cyberspace and redistribute cyberpower (Inkster, 2017; Klimburg & Fasen, 2020; Shackelford & Craig, 2014).

Democratic states have advocated for the application of the LOAC to cyberconflict (Liaropoulos, 2014; White House, 2011) and favor the status quo for cyberspace governance, due to their dominant position in the existing framework (Egan, 2016; Koh, 2012; Nye, 2014). This limited approach seeks to maintain the current balance of cyberpower and rely on well-established international law to manage conflicts (Egan, 2016; Koh, 2012; Nye, 2014). In contrast, authoritarian states have advocated for a non-LOAC paradigm to regulate cyberconflict (Broeders et al., 2019; Grigsby, 2017), claiming the democratic state approach is dangerous because it militarizes cyberspace and legitimizes cyberattacks (Inkster, 2017). Instead, they have advocated for the application of customary international laws of nonintervention, sovereignty, and countermeasures (Creemers, 2016; International Strategy of Cooperation on Cyberspace, 2017). Authoritarian states have also advocated for a new cyberspace governance framework that redistributes cyberpower (Klimburg & Fasen, 2020; Segal, 2017; Xinbao, 2017).

Democratic and authoritarian states have diverging strategic interests in cyberspace (Krutskikh & Streltsov, 2014; Mazanec, 2015a). The coalitions pursue different, and often conflicting cybersecurity policies to achieve their goals (Huang & Macak, 2017; Inkster, 2017) resulting in consistent policy clashes at international cybersecurity fora along entrenched political and ideological lines (Kleinwachter, 2012; Roguski, 2020; Slack, 2016). In fact, the divide is so deep that many scholars refer to it as the *Digital Cold War* (Kurre, 2017; Musiani & Pohle, 2014).

Democratic State Cybersecurity Politics

Democratic states occupy a dominant position in the struggle to control international cybersecurity norms because they only need a limited solution for cyberconflict. They effectively control international cyberspace governance through their influence over domestic nongovernmental organizations (NGOs) that reflect their values (Shen, 2016). This control limits the scope of the debate over the nature of the problem to be solved in cyberspace and the solutions that can be considered (Eichensehr, 2014).

The salient cyberthreat to democratic states is a catastrophic state cyberattack on CNI (Butrimas, 2014; Slack, 2016; Wirtz, 2017). Democratic states perceive their primary cyberthreat as a technology problem that is international in nature (Nocetti, 2015; Nye, 2014). This makes the LOAC a suitable, and narrowly tailored, solution to regulate state cyberattacks that produce effects similar to a use of force.

Cyberspace hegemony by the United States and its allies means they need only defend the status quo to achieve their political ends (Lantis & Bloomberg, 2018). The United States government and academic institutions are responsible for the invention and early development of cyberspace (Goldsmith & Wu, 2008), giving the United States control over the technical aspects of cyberspace functionality and operation that comprise the software infrastructure of cyberspace (Lessig, 2006). As the scope and importance of cyberspace grew, the current multistakeholder model (MSM) of cyberspace governance emerged to perform these functions (Pinheiro, 2016; van Eeten & Mueller, 2013). In this model, NGOs, private industry, academia, and states all participate in managing various aspects of cyberspace as an enterprise (Raustiala, 2016; Waz & Weiser, 2012).

Multistakeholder organizations provide expertise, efficiency, speed, and innovation that enables problem solving at the lowest level (Kurre, 2017). This loose collection of functional and technical organizations develops rules and procedures that shape the operation and evolution of cyberspace (Shackelford & Craig, 2014). Some MSM NGOs produce technical norms that are binding on their respective stakeholders (Knake, 2010). When these norms extend beyond technical matters, friction among stakeholders can emerge (Brunnee & Meshel, 2015) causing constant tension between the effectiveness and legitimacy of the MSM and the norms they produced (Kurre, 2017).

Democratic states defend the MSM by pointing to the phenomenal success of cyberspace under the MSM free-market approach (Rosenzweig, 2012). Democratic states believe the future success of cyberspace depends on the MSM, so they resist efforts to change it to increase the power of states (Kurre, 2017). The pace of ICT innovation is also advancing faster than states can adequately regulate (Macak, 2017); some scholars believe the MSM to be the best means to govern cyberspace because stakeholders have the necessary expertise and greatest incentives to continue innovation and development (Giles, 2017; Nocetti, 2015).

Authoritarian State Cybersecurity Politics

Authoritarian states face the challenge of replacing the cyberspace status quo to achieve their cybersecurity goals (Lantis & Bloomberg, 2018). They advocate for a new state dominated model of cyberspace governance and the application of the customary international laws of sovereignty, nonintervention, and countermeasures to manage cyberconflict (Creemers, 2020; Kurowska, 2020). This approach seeks to break the democratic state monopoly on cyberpower and protect authoritarian regimes from domestic political opposition (Segal, 2017; Xinbao, 2017). This approach appeals to many developing states because a multilateral model of cyberspace governance would give them new cyberpower to advance their interests (Meyer, 2013).

Unlike democratic states, the primary cyberthreat to authoritarian states is revolution fomented by subversive information on social media platforms (Zeng &

Breslin, 2016). Such a threat makes the primary cybersecurity problem to be solved a domestic political issue (Litwak & King, 2015; Nocetti, 2015). Although authoritarian states must also contend with catastrophic state cyberattacks, the gravity of that threat is significantly less immediate than domestic political unrest (Kshetri, 2014).

In authoritarian states, the regime and its immediate associates are the key stakeholders rather than the population, so regime survival is the highest national security interest (Goychayev, 2014; Nocetti, 2015). Authoritarian states are politically fragile, so internal unrest is generally more dangerous to the regime than external threats (Zeng, 2016). The key to regime survival is prevention of organized domestic political opposition and dissent (Goychayev, 2014). However, social media platforms provide opposition groups fora to organize and coordinate activities (Tullos, 2012). Since the internet's rapid spread in the 1990s, the rate of authoritarian regime change due to popular revolt has tripled (Frantz & Kendall-Taylor, 2017). Social media was the leading factor in eight successful revolutions between 2003 and 2014 (Tullos, 2012). Subversive internet content and free speech are existential national security threats to authoritarian states (Broeders et al., 2019; Mix, 2014).

Some scholars believe democratic states have engaged in social media subversion campaigns to topple authoritarian regimes (Dev, 2015; Goychayev, 2014). Democratic states have supported political opposition groups in authoritarian states by spreading anonymizing software, organizing opposition groups with social media, and disseminating subversive information (Shen, 2016; Singer & Friedman, 2014). Further, in 2010, the United States announced an internet freedom policy with the goal of spreading democracy to authoritarian sates through social media (Andres, 2014; Clinton, 2010). In essence, this strategy was implemented to subvert the legitimacy of authoritarian regimes with Western norms (Nathan, 2015).

To advance their strategic interests, authoritarian states have advocated for the replacement of the MSM with a multilateral model of cyberspace governance (Kurowska, 2020; Osula & Roigas, 2016). Authoritarian states want essential cyberspace governance functions transferred to the United Nations (Broeders et al., 2019; Shibo, 2014) to further their security interests in two important ways. First, it would shift enormous cyberpower to themselves (Galloway & Baogang, 2014). Second, state control of cyberspace governance would enable authoritarian states to impose regulations that would increase their domestic security (Creemers, 2020; Post & Kehl, 2015). State control of the domain name system would confer regulatory power that could be used to mandate global censorship and enable state mass surveillance (Klimburg & Fasen, 2020; Post & Kehl, 2015).

Authoritarian Sates also advocate for a non-LOAC paradigm to regulate cyberconflict (Grigsby, 2017). The LOAC does not offer a solution to their primary national security threats. Instead, they need a framework that can regulate free speech and subversive information (Giles, 2012; Nathan, 2015). When combined, the customary international laws of nonintervention, sovereignty, and countermeasures arguably provide the necessary solution (Creemers, 2016; International Strategy of Cooperation on Cyberspace, 2017).

Summary and Conclusions

The deep disagreement between democratic and authoritarian states regarding what is the problem that needs to be solved with international cybersecurity norms predictably produces divergent solutions. The result is rigid polarization in the cybersecurity debate (Inkster, 2017; Klimburg & Fasen, 2020). Despite much research regarding competing international cybersecurity norms, little research exists concerning the conditions necessary for those norms to emerge (Gualtier, 2015). This Delphi study, as detailed in the next chapter, reduced that gap with new knowledge from leading experts in the field. This knowledge informs future efforts to bridge the divide between democratic and authoritarian states so that international cybersecurity norms can emerge.

Chapter 3: Research Method

The purpose of this study was to determine the critical points of disagreement (the issues) between authoritarian and democratic states regarding international cybersecurity norms. To achieve this goal, I obtained a consensus opinion of a panel of experts in the field of international cybersecurity norms using a modified Delphi study. The data collected identified and ranked the issues, then forecasted what the top three issues mean for the future of international cybersecurity norms. The results of this study inform future efforts to bridge the divide between authoritarian and democratic states so that international cybersecurity norms can emerge.

This chapter begins with the rationale for designing this research as a Delphi study, followed by a description of my role. The methodology section details the participant selection logic, data collection procedures, and data analysis plan. Matters concerning trustworthiness are then addressed, followed by a summary of the chapter.

Research Questions

The central research question for this study was the following: What are the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms that must be overcome for international cybersecurity norms to emerge? The following subquestions guided the study to answer the central research question:

1. What are the critical points of disagreement among authoritarian and democratic states in the problem stream for international cybersecurity norms?

2. What are the critical points of disagreement among authoritarian and democratic states in the policy stream for international cybersecurity norms?
3. What are the critical points of disagreement among authoritarian and democratic states in the political stream for international cybersecurity norms?

Research Design and Rationale

A modified Delphi study was the best research design for this qualitative study due to its utility in identifying the key variables of a phenomenon that can be manipulated to influence future outcomes (see Barnes & Mattsson, 2016; Davidson, 2013; Habibi et al., 2014). Phenomenological and case study research designs were also considered, but they proved inferior to the Delphi technique for the goals of this research. A Delphi study is a structured group communication technique employed to build expert consensus regarding a complex problem (Bloor et al., 2013; Davidson, 2013). The Delphi technique is effective in addressing problems that have little historical evidence, great complexity, and rapidly changing conditions that inhibit effective decision making (Franklin & Hart, 2007; Mishra & Mishra, 2014). In such cases, subject matter experts often have access to information that is more current or detailed than the literature, making their opinions the richest source of data (Barnes & Mattsson, 2016; Franklin & Hart, 2007). The quality and timeliness of these data also make the Delphi technique an effective forecasting method (Sobaih et al., 2012). In the current study, a panel of experts was formed to build consensus using multiple rounds of questionnaires administered confidentially (see Keeney et al., 2011). Each round included the collection of qualitative and quantitative data (see Bloor et al., 2013). Participant feedback and iteration in the Delphi technique provides richer data collection than other methodologies, and the consensus formed provides deeper understanding of the research questions (du Plessis & Human, 2007; Mishra & Mishra, 2014). A Delphi study was the best approach for the current research.

Case study and phenomenological designs were also considered for this study. Case studies are well established in legal and political research due to their effectiveness in probing “how” and “why” questions (Creswell & Creswell, 2018; Yin, 2017). An instrumental case study design was considered because of its focus on a particular phenomenon rather than the case under study (see Yin, 2017). This approach could have been appropriate to explore the research question. However, an extensive review of the literature failed to reveal a reliable case for study. Because international cybersecurity norms have not yet emerged, the available cases are limited to a few failed efforts with little available data. Therefore, a case study approach was not a viable option for this research.

A phenomenological approach was also unsuitable. A phenomenological study is conducted to explore the essence of a lived experience for participants (Creswell & Creswell, 2018). This approach could have been used to develop generalizations about how international cybersecurity norm entrepreneurs view the political divide between authoritarian and democratic states over international cybersecurity norms. However, the goal of this study was to establish a consensus of experts regarding the research problem, which would provide a richer source of information than an aggregation of expert opinions. Accordingly, a phenomenological approach was discarded because it was not the best method to address the research question.

Role of the Researcher

The researcher is the focal point for data collection in qualitative studies (Denzin, 2012). It is essential that researchers discuss aspects of themselves relevant to the study and disclose biases that may affect the research (Greenbank, 2003). My relationship to international cybersecurity norms was that of an objective outsider. Although I am a judge advocate in the United States Army, my practice of law has never included cybersecurity or international law matters. I have, however, received specialized legal training in those areas that informs my subjective decision making (e.g., research question and research design). My interest in this topic was academic and humanitarian in nature. Further, I had no relationship with the participants in the study, and no financial gain from the study's results was anticipated.

The role of the researcher in the Delphi technique is that of an objective facilitator (Keeney et al., 2011). Subjective judgments by the researcher may undermine a study's trustworthiness (Keeney et al., 2011). Participant selection, design of the first-round questionnaire, and data analysis are significant points of vulnerability for researcher bias in the Delphi technique. Specific measures to mitigate these vulnerabilities are addressed in the following sections of this chapter.

Methodology

Developed by the Rand Corporation in the 1950s, the Delphi technique was first used to forecast the influence of emerging technology weapons on the future of warfare (du Plessis e& Human, 2007; Gupta & Clarke, 1996). The Delphi technique has been widely used as a method of determining expert consensus on diverse issues since that time (Bloor et al., 2013; De Loe et al., 2016). The Delphi technique has been used extensively in health, business, and technology research (De Loe et al., 2016; Keeney et al., 2011). Delphi studies have three stages: creation of an expert panel, identification of relevant issues for the first questionnaire, and data collection and analysis (Bourrie et al., 2014; Kalaian & Kasim, 2012).

In a modified Delphi study, researchers often develop closed-ended questions for the first questionnaire from a thorough review of the literature and themes grounded in theory (Pare et al., 2013; Sobaih et al., 2012). Researchers provide closed-ended questions to experts for ranking or response (Hasson & Keeney, 2011; Hasson et al., 2000). In the current study, a list of issues developed from the literature was provided for narrative comments. The development of the first-round questionnaire is a critical step due to the potential for researcher bias to influence the direction of the research (Davidson, 2013). To mitigate this risk, open-ended questions were used to capture any issues not included in the list provided (see De Loe et al., 2016; Hasson et al., 2000). Delphi studies that rank a list of issues typically include three data collection and analysis phases (Barnes & Mattsson, 2016; Mishra & Mishra, 2014): brainstorming, narrowing down, and ranking. Researchers employ confidential participant communication (i.e., controlled feedback) between rounds to facilitate the formation of consensus (Davidson, 2013; Hasson & Keeney, 2011).

Participant Selection Logic

The population for a Delphi study is a collection of individuals with the expertise necessary to speak authoritatively regarding the research question (Hsu & Sandford, 2007). The population for the current study was a small heterogeneous group of policy experts with specialized expertise in the field of international cybersecurity norms. Expert sampling was used to select participants for this study (see Etikan et al., 2015). This purposive sampling strategy is appropriate when the judgment of the researcher is the best way to select the most representative sample from a small population with specialized knowledge (du Plessis & Human, 2007; Hasson et al., 2000). The literature and LinkedIn were used to develop a list of candidates and solicit peer nominations (i.e., snowball sampling) to identify additional candidates. Snowball sampling is useful in identifying participants who are difficult to find, such as experts in a specialized field like international cybersecurity norms (Habibi et al., 2014; Naderifar et al., 2017). Snowball sampling also mitigates the threat of researcher bias in sample selection (Patton, 2014).

No established criteria exist for selecting experts for a Delphi study (Bourrie et al., 2014; du Plessis & Human, 2007). Sampling criteria commonly used in Delphi studies include scholarly writing, professional experience, education, credentials, commitment, and peer nomination (Barry et al., 2008). The criteria employed in the selection of participants for the current study were (a) published scholarly writing regarding international cybersecurity norms, (b) 5 years of professional experience relating to international cybersecurity matters, (c) minimum graduate level education, (e) preference for professional credentials (e.g., law license), (f) peer nomination to validate the sample, and (g) commitment to participate in all rounds of the study. Participant qualifications were verified using the literature and publicly available biographical data. Objective and accurate sampling criteria are critical to the representativeness of a Delphi panel of experts and the credibility of a Delphi study (Franklin & Hart, 2007; Habibi et al., 2014).

Researchers measure representativeness by the quality of the panel rather than its size (Okoli & Pawlowski, 2004; Powell, 2003). Also, no standard exists for the size of a Delphi panel, but the recent trend for homogeneous panels is generally between five and 12 participants (Bourrie et al., 2014; Habibi et al., 2014; Linstone & Turoff, 2011; Pare et al., 2013). Studies concerning highly specialized topics with small expert communities like the current study include smaller homogeneous panels (Barry et al., 2008; Habibi et al., 2014). Researchers also indicated that oversized panels suffer from diminished participant commitment that may adversely impact the findings (Keeney et al., 2011; Skulmoski et al., 2007). For the current study, a minimum of six participants across all rounds was deemed sufficient to achieve data saturation; however, 11 participants were recruited to achieve that goal.

Participants for this study were identified, contacted, and recruited in phases using the following procedure. In the first phase, a pool of candidates was identified using the literature. The candidates were vetted against the sampling criteria using their biographical information to narrow the pool to the best qualified candidates. The remaining candidates were contacted through email to determine their interest in participation and to arrange a telephone interview. The first phase was used to select half of the participants. In the second phase, the pool of candidates identified with snowball sampling were vetted using the procedure from the first phase. This procedure was repeated to select the remainder of the participants.

Instrumentation

Online questionnaires administered through the SurveyMonkey website were used for data collection in this study. SurveyMonkey is a secure online survey provider well suited to Delphi studies (Gill et al., 2013). Participants received an email message with a link to the study. Participants were notified of each round of the study and were provided controlled feedback between rounds through email.

The first-round questionnaire in a Delphi study employs researcher-developed questions to collect qualitative data for content analysis (Davidson, 2013; Keeney et al., 2011). The participants were provided a list of issues (including brief definitions) for comments. For each issue, the participants were able to recommend modifications, merger with another issue, or removal from the list. The participants were also asked to provide new issues they considered to be among the top 10 most important. New issues were specified in a few words and then defined in a few sentences. The definition of terms enhanced the quality of the data analysis process (see Schmidt, 1997).

The initial intent for the second round was to narrow the list to the ten issues the participants considered the most important (see Barnes & Mattsson, 2016; Okoli & Pawlowski, 2004). However, this became unnecessary because the first-round produced a list of only nine issues. Therefore, I asked participants to rank the new list of issues in descending order of importance. Participants were also asked to provide the rationale for their ranking. The questionnaire for the final ranking round was developed from the results of the second-round questionnaire and participant feedback.

Participants received controlled feedback between rounds to facilitate the formation of consensus (Davidson, 2013; Hasson & Keeney, 2011). Controlled feedback in the current study consisted of a report of the results of the preceding round. For all rounds, the report contained a summary of participant statements. Reports for the ranking rounds contained a statistical summary of the rankings. This information enabled participants to validate their information and consider the viewpoints of the other participants (see Arof, 2015; Pare et al., 2013). All questionnaires were accompanied with a set of instructions (see Keeney et al., 2011). Finally, participants were assured that their participation and information was confidential and they could withdraw at any time.

Data Collection Procedures

The Delphi technique relies on expert consensus formed through an iterative communication process to explore complex problems (Barnes & Mattsson, 2016). The data for the current study were collected from a panel of experts in the field of international cybersecurity norms. This was a small pool of geographically dispersed professionals who were difficult to reach. The flexibility of the Delphi technique (e.g., remote participation and flexible timing) made it well suited to access the collective knowledge of a hard-to-reach population like the one in this study (see Barnes & Mattsson, 2016).

The remote participation aspect of the Delphi technique also affords the participants confidentiality (Keeney et al., 2011). Confidentiality makes the Delphi technique superior to other group collaboration techniques because it eliminates the influence of dominant personalities, peer pressure, and fear of retaliation (Davidson, 2013; du Plessis & Human, 2007). The participants never meet, and researchers generally achieve participant collaboration through electronic means (Hsu & Sandford, 2007). SurveyMonkey was employed for data collection in the current study. The convenience and speed of web-based software applications increase participant commitment and data quality in Delphi studies (Gill et al., 2013).

Typically, researchers complete Delphi studies with homogeneous samples in three or four rounds (Hasson et al., 2000; Skulmoski et al., 2007). In the current study, each round took two weeks to complete. Participants needed that time to respond to the questionnaires, review the results, and enter their feedback (see Westner & Kobus, 2016). The electronic data from each round were easily exportable to other software applications for qualitative and quantitative analysis (see Franklin & Hart, 2007).

Participants were debriefed at the conclusion of the last round to inform them of the findings and thank them for their participation. Participant debriefing normally involves disclosure of aspects of the study that were not shared with the participants (Onwuegbuzie et al., 2008). However, all aspects of the current study were disclosed during the recruiting process.

Data Analysis Plan

Data analysis in a Delphi study typically involves content analysis and ranking techniques (Skulmoski et al., 2007). The expert opinions collected during each round of the current study required content analysis to extract meaning from the data. The qualitative data were analyzed using conventional content analysis and Microsoft Excel software. That approach facilitated development of codes directly from the data (see

Saldana, 2015). Researchers typically use a content analysis approach when little research exists regarding the phenomenon being explored (Hsieh & Shannon, 2005), which was well suited to the current study.

Saldana (2015) described content analysis as a cyclical process through which codes emerge, related codes are grouped into categories, and categories reveal themes. In the current study, in vivo coding was employed in the first cycle of data coding. This technique involves the use of terms and phrases of participants to create codes that provide meaning and insight (Corbin & Strauss, 2015). In vivo coding enhances trustworthiness by reducing researcher bias in the data analysis process (Hsieh & Shannon, 2005). The coded data were further refined in the second cycle using focused coding of group-related codes to identify patterns in and between categories and to develop themes (see Charmaz, 2014).

However, conventional content analysis carries the risk that the researcher will overlook key concepts (Hsieh & Shannon, 2005). Qualitative data analysis computer programs diminish this risk by enabling researchers to efficiently manage large amounts of data (Creswell & Creswell, 2018). The initial intent was to use QSR NVivo software for content analysis, but the smaller than anticipated volume of data made Microsoft Excel a better choice. Peer debriefing and member checks were also employed to mitigate the risk of incomplete coding (see Guba, 1981).

The results of the content analysis were provided to participants as controlled feedback between rounds. Each participant received a summary of the expert opinions for each issue and a copy of the expert’s own opinion (Kalaian & Kasim, 2012). This enabled participants to verify the credibility of the results and provide clarification, if necessary (Skulmoski et al., 2007).

The focus of Round 1 was the creation of a list of issues for ranking (Pare et al., 2013; Westner & Kobus, 2016). Closed ended questions were used to validate the preliminary list of issues developed from the literature. The issues were modified according to participant feedback. Open ended questions captured qualitative information for use in developing new issues.

Round 2 focused on ranking the new list of issues in Round 1. The list was ordered according to the popularity of each issue in Round 1. Many Delphi studies order the list in this way to facilitate the formation of consensus in ranking rounds (Pare et al., 2013). Participants ranked the issues in descending order of importance with 1 being the most important (Westner & Kobus, 2016). Participants also provided their rationale for their ranking (Pare et al., 2013). The issues were then reordered according to their mean ranks (Schmidt, 1997; Westner & Kobus, 2016). Kendall's coefficient of concordance (Kendall's *W*) was used to measure the strength of consensus among participants regarding the rankings. Kendall's *W* measures the level of agreement among judges participating in a ranking activity (Grzegorzewski, 2006; Weiler, 1995). Values of *W* range from 0 to 1 with agreement defined as weak $W \leq .3$, moderate $W = .5$, and strong $W \geq .7$ (Habibi et al., 2014; Westner & Kobus, 2016). Researchers frequently use Kendall's *W* in Delphi studies (see Bourrie et al., 2014; I. R. Diamond et al., 2014; Keeney et al., 2011).

In Round 3, participants modified their rankings based on the results and feedback from Round 2. Participants were asked to describe what they believe the top three issues from Round 2 mean for the future of international cybersecurity norms. The controlled feedback for Rounds 2 and 3 included summarized narrative comments, mean scores, the participant's own score, and top-half scores (i.e., the percentage of participants placing each issue in their top five; Schmidt, 1997; Westner & Kobus, 2016).

Many scholars believe that clearly articulated criteria for determining when consensus has been reached and iteration should stop enhances trustworthiness in Delphi studies (I. R. Diamond et al., 2014; Pare et al., 2013). Researchers commonly employ two standards: the strength of consensus and stability in the results (Bourrie et al., 2014; Habibi et al., 2014; Pare et al., 2013). The stopping criteria for this study was strong consensus ($W \geq .7$) or a change in W between rounds of $\leq .15$ (Schmidt, 1997; Westner & Kobus, 2016). An insignificant increase in W indicated consensus did not increase and the process should be stopped (Bourrie et al., 2014; Hasson & Keeney, 2011). Delphi studies typically see little variation in the level of consensus after two ranking rounds (Hasson et al., 2000; Skulmoski et al., 2007).

Issues of Trustworthiness

Trustworthiness in qualitative studies comprises credibility, transferability, dependability, and confirmability (Guba, 1981; Hasson & Keeney, 2011). Researchers use these criteria to maintain rigor in Delphi studies and establish confidence in findings (Anney, 2018; Hasson et al., 2000). This section discusses how the criteria were employed to produce trustworthy findings.

Credibility

Credibility is the degree of confidence in the accuracy of the findings (Anney, 2018). A study is credible when the conclusions drawn from the data accurately reflect the views of participants (Guba, 1981). Peer review and member checks are common strategies to enhance credibility (Anney, 2018) that were used in the current study. Peer review is critical feedback from mentors that improves the quality of the findings (Patton, 2014). Member checks verify the accuracy of data analysis through feedback (Creswell & Creswell, 2018). Member checks are essential to mitigate researcher bias and internal conflict (Guba, 1981).

Some scholars believe the iterative process and formation of consensus in the Delphi technique also enhance credibility (Hasson & Keeney, 2011). Researchers address negative cases (i.e., dissenting opinions) by soliciting the rationale for the dissent so it can be considered by the participants. Specific threats to credibility in the Delphi method are panel selection, formulation of the first-round questionnaire, and continued engagement by participants (Davidson, 2013; Gill et al., 2013).

The consensus opinion of a panel of experts is more reliable than the opinions of individuals (du Plessis & Human, 2007; Franklin & Hart, 2007). No standard exists for selecting experts, but participants must have sufficient knowledge to speak authoritatively about the research question (i.e., a representative sample; Davidson, 2013; Hsu & Sandford, 2007). Researchers measure the representativeness of the sample by the quality of the panel rather than its size (Okoli & Pawlowski, 2004; Powell, 2003). Purposive sampling and rigorous sample selection criteria were used in the current study to ensure participants possess the necessary knowledge and expertise to contribute credible data (see du Plessis & Human, 2007; Hasson et al., 2000).

The design of the first-round questionnaire is also critical to the credibility of a Delphi study because it has the highest potential for researcher bias (Davidson, 2013). Researchers must take great care to ensure that the initial questionnaire accurately reflects the key elements of the research question (Franklin & Hart, 2007). The current modified Delphi study used a semi-structured approach to the first-round questionnaire. Researchers frequently use this approach to build on existing research concerning the topic of the study (Hsu & Sandford, 2007). Closed ended questions for the current study were developed from the literature, focused by MSF, to enhance credibility (du Plessis & Human, 2007; Franklin & Hart, 2007). To mitigate the risk of researcher bias, open ended questions were also used to capture any issues not included in the list provided (De Loe et al., 2016; Hasson et al., 2000).

Credibility in a Delphi study also depends on continued engagement by participants across all rounds. The literature indicates the quality of a Delphi study increases as the time between rounds decreases (van Zolingen & Klaassen, 2003). Shorter waiting times align with higher rates of participant engagement and study completion. The use of a web-based portal for data collection, analysis, and communication can minimize the time between rounds and maximize convenience for participants (Gill et al., 2013). The speed and convenience of web-based Delphi studies improves data quality (Bloor et al., 2013). Participant engagement is also enhanced by selecting experts who are interested in the research question and the significance of the research to the field

(Keeney et al., 2011). Recruiting participants through direct contact increases commitment (du Plessis & Human, 2007; Hasson et al., 2000).

Transferability

Transferability is the degree to which the findings may be generalized to other settings or participants (Hasson & Keeney, 2011). Qualitative research often criticized as lacking academic rigor and transferability (Creswell & Creswell, 2018). However, qualitative studies are normally limited to their particular facts and circumstances (Creswell & Creswell, 2018).

A researcher establishes transferability by providing sufficient information for the audience to determine whether the findings are applicable to other settings or participants (Guba, 1981). The researcher ensures transferability through thick description and purposive sampling (Anney, 2018). Thick description provides the potential user with insight into the processes employed in the study to facilitate judgments regarding transferability (Hasson & Keeney, 2011). The detailed discussion of the use of the Delphi technique in this chapter provides such information (as in Anney, 2018). Thick description was enhanced in this study through purposive sampling. Purposive sampling provides richer findings than probability sampling methods (Anney, 2018). Additionally, the use of theory also enhanced transferability of the current study (see Yin, 2017).

Dependability

Dependability is the degree to which other researchers can consistently replicate a study's findings (Hasson & Keeney, 2011). Trustworthiness requires that a study's research report provide sufficient information to repeat the study and obtain similar results (Anney, 2018). In the current study, trustworthiness was achieved using an audit trail, code–recode strategy, and peer examination (as suggested by Anney, 2018). An audit trail facilitates validation of the data by establishing a record of the researcher's activities and decisions concerning data collection and analysis (Guba, 1981). An audit trail is the main factor enhancing trustworthiness in a Delphi study (Hasson & Keeney, 2011). The code–recode strategy involves coding the data at least twice with a wait between coding sessions (Anney, 2018). Consistency in the results enhances the study's dependability (Anney, 2018). Finally, peer examination involves discussing the findings with mentors to obtain critical feedback. Representative sampling also increases dependability in Delphi studies (Hasson & Keeney, 2011).

Confirmability

Confirmability is the degree to which a study's findings are limited to the data and the phenomenon under investigation (Guba, 1981). Confirmability is the assurance that researcher bias does not skew data analysis (Anney, 2018). Confirmability can be established through reflexive journaling to document the lifecycle of the study (Creswell & Creswell, 2018). A reflexive journal records all processes, procedures, rationales for decisions, thoughts on the research, plans for data collection, and tentative data interpretations (Patton, 2014). Researchers use this information to assess the potential influence of researcher bias on the study (Anney, 2018). In Delphi studies, researchers commonly use a reflexive journal to enhance confirmability (Hasson & Keeney, 2011). Member checks included in each round of a Delphi study also reduce researcher bias by verifying the accuracy of the data analysis (Franklin & Hart, 2007).

Ethical Procedures

The Walden University Institutional Review Board approved the research proposal for this study on July 28, 2021 (approval number 07-28-21-0539340). Ethical concerns regarding recruitment were very low. Participants were recruited with direct contact by email and minimal protected personally identifiable information was collected. Participant confidentiality was maintained using research identification codes. The master code list and all personally identifiable information were maintained in an offline encrypted file. Informed consent was obtained electronically from participants prior to data collection. The consent form educated participants on the nature of the study, their time commitment, data collection and analysis processes, and ethical issues (see du Plessis & Human, 2007; Hasson et al., 2000).

The potential for physical or psychological harm to study participants was also very low due to the nature of the study and sample demographics (i.e., adult, professional, and highly educated). There were no sensitive topics in the current study and the study included no vulnerable populations. The confidential nature of the Delphi technique frees participants from undue influence and fear of retribution (Keeney et al., 2011). Participation in the current study was completely voluntary and participants were able to withdraw at any time. Further, no special planning was required for predictable adverse events.

Finally, electronic collection and maintenance of all data creates a risk of unauthorized disclosure. Password protection and data encryption were used at every step of the current study to establish and maintain data security. Data access was limited to the researcher, the dissertation committee, and those identified by Walden University as having an official need for access. The data was securely stored for 5 years and then destroyed according to Walden University policy. All data-protection laws and regulations were followed rigorously.

Summary

This chapter detailed the research methodology used in the current study and the rationale for its selection, the data collection and analysis procedures, and the safeguards employed to ensure the trustworthiness of the findings. The chapter concluded with discussion of the ethical considerations undertaken in this study.

The Delphi technique is effective in addressing problems that have little historical evidence, great complexity, and rapidly changing conditions that inhibit effective decision-making (Franklin & Hart, 2007; Mishra & Mishra, 2014). Thus, the Delphi technique was well suited to a problem like unregulated cyberconflict. A modified Delphi study was the best research design for the current study due to its utility in identifying the key variables of a phenomenon that can be manipulated to influence future outcomes (Barnes & Mattsson, 2016; Okoli & Pawlowski, 2004). This makes a modified Delphi study uniquely suited to answering the current study's research question.

Chapter 4: Results

The purpose of the current study was to form a consensus opinion of a panel of international cybersecurity experts on the critical points of disagreement between authoritarian and democratic states regarding international cybersecurity norms. Toward that end, the following research question and subquestions were employed:

RQ: What are the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms that must be overcome for international cybersecurity norms to emerge?

SQ1: What are the critical points of disagreement among authoritarian and democratic states in the problem stream for international cybersecurity norms?

SQ2: What are the critical points of disagreement among authoritarian and democratic states in the policy stream for international cybersecurity norms?

SQ3: What are the critical points of disagreement among authoritarian and democratic states in the political stream for international cybersecurity norms?

This chapter details the research setting, sample demographics, data collection and analysis procedures, and the study's trustworthiness. The results of each round of the study are then presented. Finally, a summary answer to the research question is provided.

Research Setting

The virtual nature of this study provided the participants confidentiality. Further, no information was collected from the participants beyond the questionnaires. Conditions that may have influenced the participants during the study were unknown.

Demographics

A list of thirty potential participants was developed from the literature and publicly available biographical data. The candidates were vetted using the following criteria: (a) published scholarly writing regarding international cybersecurity norms, (b) five years of professional experience relating to international cybersecurity matters, (c) minimum graduate level education, (d) preference for professional credentials (e.g., law license), (e) peer nomination, and (f) commitment to participate in all rounds of the study. The list was narrowed to fifteen candidates who were invited to participate in the study via email. Positive responses were obtained from seven candidates who nominated additional experts for the study. Through snowball sampling, four additional candidates were identified for an initial panel of eleven experts.

The original panel was composed of three women and eight men, with four participants from Europe, one from the Middle East, and six from North America. All participants had a strong background in international law, and ten of the eleven participants had a doctoral level education. The panel had an average of eleven published scholarly articles regarding international cybersecurity norms per participant. Additional information regarding the qualifications of the participants is contained in Appendix A.

Data Collection and Analysis

The data for this study were collected remotely from a panel of experts in the field of international cybersecurity norms. Over the course of five weeks, three rounds of online questionnaires were administered, with participant feedback between rounds, to build a consensus opinion. The study began with nine participants completing the Round 1 questionnaire. Despite the use of multiple retention techniques, attrition across rounds was high. Only six participants, the minimum sample size established in Chapter 3, completed all rounds. The data in Tables 3, 5, 6, and 7 are limited to the final six participants. Table 1 presents the data collection chronology, and Table 2 indicates participant attrition.

Table 1

Data Collection Chronology

Action	Start date	End date
Round 1 questionnaire issued	09/27/21	10/01/21
Round 1 data analyzed	10/02/21	10/08/21
Round 2 questionnaire issued	10/11/21	10/15/21
Round 2 data analyzed	10/16/21	10/22/21
Round 3 questionnaire issued	10/25/21	11/08/21
Round 3 data analyzed	11/09/21	1/05/22

Table 2

Participant Attrition

Round	Questionnaires completed	Completion rate	Attrition rate
1	9	100%	NA
2	7/9	78%	22%
3	6/7	86%	14%

Round 1

The goal of Round 1 was the creation of a list of the most significant disagreements between authoritarian and democratic states regarding international cybersecurity norms. Participants were asked to identify and define the most significant issues in the MSF problem, policy, and political streams so those issues could be ranked in later rounds. Each participant was sent an email to begin Round 1 data collection, which contained the participant's unique identification number and a hyperlink to the informed consent form located on Surveymonkey. Access to the Round 1 questionnaire was granted after participants entered their unique participant identification number into the consent form. The questionnaire asked the participants to modify a list of nine issues developed from the literature, nominate issues for removal from the list, and nominate new issues to be added to the list.

The Round 1 quantitative data were limited to participant votes to retain or remove issues from the list. The data were analyzed using Microsoft Excel to determine the score for each issue. Short narrative statements regarding ten open-ended questions provided the qualitative data for this round. I originally planned to use QSR NVivo for qualitative analysis; however, the data were easily managed with Microsoft Excel instead. Two cycles of conventional content analysis, on separate days, were used to develop codes from the data. Side-by-side comparison of the narrative statements in a spreadsheet facilitated coding and the development of themes. In the first cycle, the terms and phrases of participants were used to create codes. Related codes were then grouped together to reveal patterns and develop themes in the second cycle. The themes were used to redefine the issues that were retained by the participants for future rounds. There were no discrepant cases in Round 1.

Customized reports of the Round 1 results were provided to each participant via email. Each report included the individual participant's vote to retain or delete each issue, the panel score to retain or delete each issue, the individual participant's verbatim modifications to each issue, the eight redefined issues (with participant modifications to the original language in bold text), and the new issue that was submitted. No feedback was received from the participants regarding the reports.

Round 2

The results of Round 1 were used to create the second questionnaire. Each participant was sent an email to begin Round 2 data collection, which contained the participant's unique identification number and a hyperlink to the survey located on SurveyMonkey. The original intent for this round was to narrow the list, but this became unnecessary with only nine issues on the list. Instead, I asked participants to rank the issues developed in Round 1 in descending order of importance and explain their reasoning. The purpose of this questionnaire was to build a consensus opinion regarding which three issues presented the greatest obstacles to the emergence of international cybersecurity norms.

Participant rankings of the issues provided the quantitative data for Round 2. The data were analyzed with Microsoft Excel to determine the mean score and top half score for each issue and gauge the degree of consensus regarding the top three issues. Participant narrative statements regarding their reasoning for their rankings provided the qualitative data for this round. The original intent was to use QSR NVivo for qualitative analysis; however, Microsoft Excel was used instead. The data were coded following the same process used in Round 1. The themes developed were used to produce summarized panel reasoning for ranking each issue. There were no discrepant cases in Round 2.

Customized reports of the Round 2 results were provided to each participant via email. Each report included the individual participant's rankings, the panel mean rankings, the individual participant's verbatim reasoning for their rankings, the summarized reasoning of the panel for each ranking, and top half scores. No feedback was received from the participants regarding their reports.

Round 3

The results of Round 2 were used to create the third questionnaire with the issues ordered according to their mean ranks. Each participant was sent an email to begin Round 3 data collection, which contained the participant's unique identification number and a hyperlink to the survey located on SurveyMonkey. This questionnaire required participants to confirm or modify their ranking of the issues. Participants were also required to forecast how the top three issues from Round 2 will affect the emergence of international cybersecurity norms over the next 5–10 years.

Participant rankings of the issues provided the quantitative data for Round 3, which were analyzed using Microsoft Excel. Participant narrative statements regarding their forecast and reasoning for their rankings provided the qualitative data for this round. The original intent was to use QSR NVivo for qualitative analysis; however, Microsoft Excel was used instead. The data were coded following the same process used in Rounds 1 and 2. The themes developed were used to produce summarized panel reasoning for ranking each issue and a forecast.

Customized reports of the Round 3 results were provided to each participant via email. Each report included the individual participant's rankings, the panel mean rankings, the individual participant's verbatim reasoning for their rankings, the summarized reasoning of the panel for each ranking, the individual participant's verbatim forecast, the summarized forecast of the panel, and top half scores. No feedback was received from the participants regarding the reports.

Safeguards

Several precautions were observed to protect the confidentiality anonymity of participants. First, narrative statements were summarized across rounds. This mitigated the risk that participants might be identified by their writing style or use of specific phrases. Next, all data that could be used to identify the participants were maintained in encrypted files on a removable storage device that was secured in a locked container. All email correspondence was deleted from the email server and stored in encrypted file on the removable storage device. The personally identifiable information was redacted from these records, and they were labeled with unique participant identification numbers. Finally, all survey data were deleted from the SurveyMonkey servers and stored in an encrypted file on a removable storage device.

Evidence of Trustworthiness

Credibility

Multiple procedures were followed to ensure the conclusions drawn from the data accurately reflected the opinions of the participants. Member checks were employed to verify the accuracy of data analysis and mitigate researcher bias across rounds. Peer review was used to ensure the quality of the findings. A combination of purposive and snowball sampling and the use of rigorous selection criteria reduced the threat of researcher bias in sample selection. Potential researcher bias in the development of the first questionnaire was mitigated by developing the list of issues from the literature, employing a theoretical lens, and using open-ended questions that allowed participants to reshape the list of issues. The noteworthy adjustment to the credibility safeguards was the use of Microsoft Excel for qualitative data analysis instead of QSR NVivo. The volume of qualitative data collected was smaller than anticipated, so the data analysis features of QSR NVivo were not required to reduce the risk that key concepts might be overlooked.

Transferability

One goal of the current study was to enable researchers to transfer the findings to similar research regarding the development of international norms for other emerging technology weapons. With that in mind, I used thick description to detail the processes employed in the study. This would enable researchers to determine whether the findings were transferrable to other settings or participants. Thick description was enhanced using purposive sampling to obtain rich findings from highly qualified experts. Further, a theoretical lens was employed to enhance the transferability of the findings. There were no departures from the transferability strategies detailed in Chapter 3.

Dependability

The dependability strategies outlined in Chapter 3 were implemented without adjustments. Three techniques were employed to ensure other researchers can replicate the study's findings. First, the audit trail provided in this chapter includes all significant data collection and analysis activities and decisions to facilitate validation of the data. Next, a code–recode strategy was employed to enhance the consistency of the results. Finally, peer examination was employed by discussing the findings with mentors to obtain critical feedback.

Confirmability

The confirmability strategies detailed in Chapter 3 were followed to ensure the findings were not skewed by researcher bias. A reflexive journal was used to document the life cycle of the study and facilitate the assessment of potential researcher bias. Member checks were employed to enhance confirmability by verifying the accuracy of the data analysis across rounds.

Study Results

The list of issues developed from the literature and provided with the Round 1 questionnaire was divided into three issues from each of the MSF streams. This approach facilitated data analysis across rounds and assisted in answering the primary research question and subquestions. The problem, policy, and political streams were briefly explained in the first questionnaire to provide context to the participants. The results of the quantitative and qualitative data analysis for each round are discussed in the following sections.

Round 1

Table 3 reflects the results of participant voting to retain or remove issues from the list of nine issues provided in the first questionnaire. One issue was removed, and one was added, leaving nine issues. The urgency issue was removed by a majority vote of the participants (75%), and workforce was provided by a participant.

Table 3

Round 1 Quantitative Results

Issue	Retain votes	Remove votes
Threat perception	100%	NA
Significance	100%	NA
Asymmetry	100%	NA
Attribution	83%	17%
Problem character	83%	17%
Problem nature	83%	17%
Norm selection	83%	17%
International cyberpower	67%	33%
Urgency	33%	67%

Participants also recommended modifications to the definitions of the eight issues that were retained (see Table 4). In some instances, the modifications were simple verbatim changes to the text. Other recommendations, however, required content analysis to identify and combine related concepts that were used to modify the text.

Table 4

Round 1 Qualitative Results

Issue	Narrative statements	Text modifications
Threat perception	0	0
Significance	1	1
Asymmetry	2	1
Attribution	1	1
Problem character	0	0
Problem nature	4	3
Norm selection	6	3
International cyberpower	2	4
Urgency	1	NA

The original definitions provided in the Round 1 questionnaire, and modified definitions with changes in bold, are contained in Appendix B. The results of the voting and the modified definitions were reported back to the participants in the Round 1 reports. No feedback was received from the participants regarding the reports.

Round 2

In this round, a weak level of consensus was established regarding the rankings, with a *Kendal's W* of 0.405. While the bottom four issues received little support from the panel, support for Workforce was essentially limited to one participant who ranked it first. The quantitative results for Round 2 are reflected in Table 5 below.

Table 5

Round 2 Quantitative Results

Rank	Issue	Mean score	Top half score
1	Problem nature	2.00	83%
2	Threat perception	3.50	67%
3	Attribution	4.17	67%
4	Problem character	4.33	50%
5	Asymmetry	4.50	67%
6	International cyberpower	6.17	0%
7	Norm selection	6.33	33%
8	Significance	6.50	17%
9	Workforce	7.50	17%

The qualitative data for Round 2 consisted of short narrative statements regarding participant reasoning for their rankings. These statements were summarized and reported back to the participants in the Round 2 reports, along with the rankings. No feedback was received from the participants regarding the reports.

Round 3

In this round, the level of consensus decreased by 0.029 as *Kendal's W* decreased to 0.376. With the degree of change between rounds being less than 0.15, the stability criteria for stopping data collection was met. The top three issues and bottom four issues remained the same across Rounds 2 and 3. Workforce was ranked last by all but one participant who again ranked it first. The quantitative results for Round 3 are reflected in Table 6 below.

Table 6

Round 3 Quantitative Results

Rank	Issue	Mean score	Top half score
1	Problem nature	3.00	67%
2	Attribution	3.50	83%
3	Threat perception	3.67	67%
4	Problem character	4.00	50%
5	Asymmetry	4.50	50%
6	Significance	5.33	33%
7	International cyberpower	6.17	17%
8	Norm selection	7.17	17%
9	Workforce	7.67	17%

Regarding qualitative data for Round 3, the participants again provided justifications for their rankings. These statements indicated the participants found the Round 2 feedback generally unpersuasive. However, 50% of the participants specifically stated they were convinced to rank the attribution issue higher. As a result, attribution moved up the list to number 2.

The participants also provided narrative statements forecasting how the top three issues from Round 2 will affect the emergence of international cybersecurity norms. Content analysis of the data revealed the following themes. First, the issues of problem nature, threat perception, and attribution make it unlikely that international cybersecurity norms will emerge over the next 5-10 years. Next, the magnitude of the obstacles presented by the problem nature and threat perception issues have been undervalued. Proscriptive norms are unlikely to be adopted until these issues are better understood. Reliable attribution technologies are necessary to create the conditions necessary for norms to emerge. Further, the status quo may change in favor of limited political norms if the interests of authoritarian and democratic states become aligned on specific issues. Until that time, states should increase investments in offensive and defensive cyber-capabilities to deter hostile states.

Primary Research Question Results

The results indicate problem nature, attribution, and threat perception are the top 3 issues. These points of disagreement among authoritarian and democratic states regarding international cybersecurity norms must be overcome for international cybersecurity norms to emerge. Table 7 below reflects the quantitative ranking data for Rounds 2 and 3.

Table 7

Top 3 Points of Disagreement

Final rank	Issue	R2 mean scores	R3 mean scores	R2 top half scores	R3 top half scores
1	Problem nature	2.00	3.00	83%	67%
2	Attribution	4.17	3.50	67%	83%
3	Threat perception	3.50	3.67	67%	67%

Research Subquestion 1 Results

SQ1 asked: What are the critical points of disagreement among authoritarian and democratic states regarding the problem to be solved with international cybersecurity norms? The term “problem” was defined as a political issue that can and should be solved by government action. The panel identified and defined problem nature, threat perception, problem character, and workforce as the critical points of disagreement in the

MSF problem stream. Table 8 below reflects the problem stream issues as defined by the panel.

Table 8

MSF Problem Stream Issues

Issue	Definition	Rank
Problem nature	Democratic states (DS) consider cyberconflict: a technology problem caused by incredibly complex networks of information systems that by design lack security; and an international law problem caused by disagreement over and lack of compliance with pre-existing international law norms. Authoritarian states (AS) consider it: a sociopolitical problem caused by subversive information that foments civil unrest and incites revolution; and a structural problem caused by DS control of most international cyber mechanisms.	1
Threat perception	DS perceive the salient cyberconflict threat as a catastrophic cyber-attack on critical national infrastructure. AS perceive their primary threat as subversive information that foments civil unrest and incites revolution.	3
Problem character	DS desire limited norms to regulate cyber-attacks that produce effects analogous to conventional armed attacks. AS seek broadly applicable international cybersecurity norms that increase state control over subversive information.	4
Workforce	AS enjoy a faster and more consistent ability to proportionally increase its work force with cybersecurity and offensive cyber capabilities given the style of government and greater control over the educational systems at all levels. DS cannot replicate or increase such a workforce at the same speed. Instead, DS must rely on incentive-based efforts to increase the technology proficient workforce.	9

Research Subquestion 2 Results

SQ2 asked: What are the critical policy disagreements among authoritarian and democratic states regarding international cybersecurity norms? The term "policy" was defined as a government solution to a political problem. The panel identified and defined attribution and norm selection as the critical points of disagreement in the MSF policy stream. Table 9 below reflects the policy stream issues as defined by the panel.

Table 9

MSF Policy Stream Issues

Issue	Definition	Rank
Attribution	DS seek robust international law enforcement cooperation to collect the evidence necessary to attribute cyber-attacks to responsible states and enforce norms. AS desire limited international law enforcement cooperation that safeguards their control and autonomy with respect to cyber actions.	2
Norm selection	DS policy solutions focus heavily on a narrow type of destructive cyber-attack they classify as an armed attack. As a result, they emphasize advocacy for norms that apply the law of armed conflict to the most dangerous type of state conduct in cyberspace. This solution mitigates the primary threat to DS without jeopardizing fundamental human rights (e.g., privacy, free speech). AS classify cyberconflict more broadly as wrongful state conduct and they emphasize advocacy for norms that apply the international laws of nonintervention, sovereignty, and countermeasures to cyberconflict. AS feel this approach offers less dangerous remedies for cyber-attacks that are difficult to classify and regulates a broader spectrum of hostile conduct.	8

Research Subquestion 3 Results

SQ3 asked: What are the critical political disagreements among authoritarian and democratic states regarding international cybersecurity norms? The term “political” was defined as the sum of political forces (e.g., international mood, organized political forces, national governments) that influence government decision-making at a particular point in time. The panel identified and defined asymmetry, significance, and international cyberpower as the critical points of disagreement in the MSF political stream. Table 10 below reflects the political stream issues as defined by the panel.

Table 10

MSF Political Stream Issues

Issue	Definition	Rank
Asymmetry	Unregulated cyberconflict provides AS an asymmetric means to counter the economic and military advantages of DS. Cyberconflict is a low cost and low risk means to create effects far exceeding what could be produced with the conventional capabilities of AS. Therefore, DS need international cybersecurity norms to maintain their economic and military advantages. In the interim, DS require greater defensive/offensive deterrent capabilities.	5
Significance	Intellectual property obtained via cyberespionage has fueled rapid economic growth in some AS. Such intellectual property theft provides AS discount imports through which the victim entity generally cannot seek retribution. Therefore, unregulated cyberconflict provides AS an enormous economic advantage. In contrast, the corresponding economic loss to DS is nearing a trillion dollars annually.	6
International cyberpower	DS maintain a dominant position in cyberspace through heavy influence over sympathetic non-governmental organizations that regulate critical internet functions. This enables DS to control international norms that serve their interests. In contrast, AS require a redistribution of international cyberpower to create new norms that further their national security interests (i.e., increased surveillance and information control).	7

Summary

This chapter discussed the collection and analysis of the data and the results of the study. Three rounds of online surveys were conducted with a panel of six experts in the field of international cybersecurity norms. The data collection and analysis procedures established in Chapter 3 were rigorously followed to obtain trustworthy results, with two minor departures as discussed. While the results of the study did not establish a strong consensus (*Kendal's* $W \geq .75$) regarding the ranking of the list of issues developed in Round 1, the panel did answer the primary research question. Analysis of the data indicates problem nature, attribution, and threat perception were the salient points of disagreement among authoritarian and democratic states. The participant forecast indicated these issues make it unlikely that international cybersecurity norms will emerge in the next 5-10 years. The following chapter provides a summary and conclusion of the study.

Chapter 5: Discussion, Conclusions, and Recommendations

This modified Delphi study was conducted to establish a consensus opinion of a panel of international cybersecurity experts on the critical points of disagreement between authoritarian and democratic states regarding international cybersecurity norms. Because international cybersecurity is a broad topic, the scope of the study was limited to the disagreements between authoritarian and democratic states. The theoretical propositions of the MSF were used as an analytical strategy to align data collection and analysis with the research question and subquestions (see Kingdon, 1995). This research informs future norm entrepreneurship for international cybersecurity norms and furthers knowledge regarding the norm development process for other emerging technology weapons.

The expert panel did not establish a strong consensus (*Kendal's W* ≥ .75) regarding the ranking of the list of issues developed in Round 1. However, the panel did define the points of disagreement and reach a weak consensus regarding the top three issues. Analysis of the data indicated problem nature, attribution, and threat perception are the most important points of disagreement among authoritarian and democratic states. The panel forecast indicated these issues will inhibit the emergence of international cybersecurity norms over the next 5–10 years.

This chapter includes an interpretation of the findings and the limitations of the study. Then, recommendations for further research regarding the development of international cybersecurity norms are offered. Finally, the implications of this research for positive social change are discussed.

Interpretation of Findings

I used the MSF as a lens to focus on components of the norm emergence process for international cybersecurity norms (see Kingdon, 1995). The research subquestions addressed the key factors in the problem, policy, and political streams to answer the research question which was: What are the critical points of disagreement among authoritarian and democratic states regarding international cybersecurity norms that must be overcome for international cybersecurity norms to emerge? The results indicated problem nature, attribution, and threat perception are the top three critical points of disagreement.

The MSF asserts that the policy process (i.e., norm emergence process) is composed of three independent streams (problems, policies, and politics) that interact dynamically (Kingdon, 1995; Zahariadis, 2019). Problems are significant issues that can and should be solved by government action (Beland & Howlett, 2016). Policies are competing ideas developed by the policy community to solve problems (Beland & Howlett, 2016). Politics are the conditions and forces that influence the government decision-making environment at a particular point in time (Beland & Howlett, 2016). Norm entrepreneurs manipulate conditions in the streams to create windows of opportunity for the adoption of new government policies (i.e., norm emergence; Beland & Howlett, 2016).

Problem Stream

The problem stream contained four of the nine issues on the list. Problem nature and threat perception were the top issues in the problem stream and the first and third most important issues overall. The panel concurred with the literature regarding the meaning of these issues. However, the panel forecast indicates the literature has undervalued the magnitude of the challenge these issues represent to the emergence of international cybersecurity norms.

Developed states are increasingly dependent on ICTs and cyberspace for essential functions (Hendrickson, 2015; Trautman, 2016; Wirtz, 2017). However, ICTs are insecure because of their complexity (Mazanec, 2016; Singer & Friedman, 2014). States are exploiting this vulnerability by engaging in cyberconflict to advance their strategic interests (Buchanan, 2020; Vasiu & Vasiu, 2017). This makes cyberconflict an urgent national security threat (Ayalew, 2015; Kent, 2016; Moynihan, 2021).

Democratic states perceive the cyberconflict threat as a catastrophic cyberattack on critical national infrastructure (Simmons, 2014; Trautman, 2016). Authoritarian states perceive the cyberconflict threat as subversive information that foments civil unrest and incites revolution (Creemers, 2020; Kurowska, 2020). Cyberconflict creates different security gaps for democratic and authoritarian states (Klimburg & Faesen, 2020; Mazanec, 2015a).

Diverging threat perceptions cause different definitions of the security problem to be solved (Klimburg & Faesen, 2020). Democratic states consider cyberconflict a technology problem caused by complex networks of information systems that by design lack security, and an international law problem caused by disagreement over and lack of compliance with preexisting international law norms (Moynihan, 2021; Nocetti, 2015). In contrast, authoritarian states consider cyberconflict a sociopolitical problem caused by subversive information that foments civil unrest and incites revolution, and a structural problem caused by democratic state control of most international cyber mechanisms (Broeders et al., 2019; Litwak & King, 2015).

Different definitions of the security problem cause democratic and authoritarian states to pursue different solutions to achieve their cybersecurity goals (Huang & Macak, 2017; Inkster, 2017). Despite discussions in international fora, states remain divided regarding the norms applicable to cyberconflict (Painter, 2021; Preston, 2016). Democratic states require a limited solution to regulate catastrophic state cyberattacks on CNI (Izycki & Vianna, 2021). This makes the LOAC a natural solution to mitigate their primary cyberconflict threat (Liaropoulos, 2014; White House, 2011). In contrast, protecting authoritarian regimes from internal political opposition is a more challenging problem to solve (Segal, 2017; Xinbao, 2017). Authoritarian states require state control of cyberspace governance to impose regulations that increase their domestic security (Lantis & Bloomberg, 2018; Post & Kehl, 2015). In other words, authoritarian states require a new cyberspace governance paradigm that enables state regulation of free speech and subversive information (Klimburg & Faesen, 2020; Nathan, 2015).

Policy Stream

The policy stream contained two of the nine issues on the list. Attribution was the top issue in the policy stream and the second most important issue overall. The panel concurred with the literature regarding the meaning of the Attribution issue and indicated reliable attribution technologies are necessary to create the conditions necessary for norms to emerge.

Attribution is the assignment of culpability for a cyberattack to the responsible state (Eichensehr, 2020; Vasiu & Vasiu, 2017). Reliable attribution is essential to the enforcement of norms regulating cyberconflict to deter hostile state conduct in cyberspace (Derian-Toth et al., 2021; Stevens, 2017). The status quo lack of meaningful consequences for state cyberattacks incentivizes the use of cyberconflict as a tool to advance strategic interests (Deeks, 2020; Jasper, 2015; Kello, 2017).

Evidence essential to reliable attribution is difficult to collect because it is obscured by the virtual nature of cyberspace (Lin, 2016; Roguski, 2020). Further, states responsible for cyberattacks do not cooperate with investigations, making essential evidence in that state unavailable (Eichensehr, 2020; Shah, 2015). Regarding cybersecurity policies, democratic states seek robust international law enforcement cooperation to collect the evidence necessary to attribute cyberattacks to responsible states and enforce norms (Derian-Toth et al., 2021; Eichensehr, 2020; Roguski, 2020). In contrast, authoritarian states desire limited international law enforcement cooperation that safeguards their control and autonomy with respect to cyber actions (Broeders et al., 2019; Creemers, 2020; Kurowska, 2020).

Political Stream

The political stream contained three of the nine issues on the list. Asymmetry was the top issue in the political stream, but only the fifth most important issue overall. The panel consistently ranked the issues in the political stream in the bottom half of the list.

Coupling the Streams

According to Zahariadis (2019), the struggle to create norms is characterized by ambiguity that is resolved by establishing meaning rather than more or better information about problems and policies. Policy entrepreneurs supply meaning by framing problems with narratives to shape conditions in the problem and political streams (Beland & Howlett, 2016). When a policy entrepreneur is successful in coupling the streams, a window of opportunity opens for new norms to emerge (Kingdon, 1995; Ruvalcaba-Gomez, 2020).

Senior national leaders and powerful international interest groups are shaping the international political stream with competing cybersecurity narratives (Broeders et al., 2019; Giles, 2017). These elite norm entrepreneurs are framing cyberconflict in different ways to address fundamentally different security challenges (Austin et al., 2015; Klimburg & Fasen 2020). As a result, democratic and authoritarian states advocate for competing international cybersecurity norms to address their national security needs (Huang & Macak, 2017; Inkster, 2017; Klimburg & Fasen 2020).

The findings of the current study may guide future efforts by norm entrepreneurs to open a policy window for international cybersecurity norms to emerge. The panel forecast indicated it may be possible to couple the streams on discrete aspects of cyberconflict in which the interests of democratic and authoritarian states are aligned. Findings indicated that norm entrepreneurs should focus on framing issues in the problem stream with narratives that highlight the shared interests of democratic and authoritarian states. Doing so requires a deeper understanding of the problem nature and threat perception issues. Further, the means and methods to identify states engaging in cyberattacks, and the capabilities to impose costs on those states, are essential to the emergence of international cybersecurity norms. To create those conditions, norm entrepreneurs should advocate for increased research and development into attribution technologies. Norm entrepreneurs should also seek greater state investments in offensive and defensive cyber capabilities to impose costs on responsible states that will deter cyberconflict.

Limitations of the Study

Qualitative studies are normally limited to their particular facts and circumstances (Creswell & Creswell, 2018). The transferability of the current study is limited to international norm entrepreneurship regarding the emergence of international norms for cyberconflict and other emerging technology weapons. Despite this limited scope, the following limitations to transferability were noted during data collection and analysis.

The composition of the panel raised two issues. First, the panel experienced a high attrition rate. With small samples, high dropout rates may cause response bias (Hasson et al., 2000). No standard for participation across rounds has been established for Delphi studies (Keeney et al., 2011), but Sumsion (1998) recommended a 70% participation rate for each round. Although that standard was achieved for all rounds in the current study, the loss of 33% of the participants reduced the sample to the minimum size necessary for data saturation specified in Chapter 3. Next, despite my efforts to recruit experts from authoritarian states, the sample was composed exclusively of experts from democratic states. Therefore, the findings are limited to the opinions of experts who may not fully appreciate the issues from the perspective of authoritarian states.

Recommendations

Further research could be conducted with a different methodology and design to address the limitations of this study. The use of a focus group instead of a Delphi study may produce richer data. Control measures could be designed to mitigate the danger of dominant personalities controlling the debate. The research could also be conducted in conjunction with an international cybersecurity conference. This would enable the participants to interact in person and discuss issues between sessions. Personal interaction may also reduce the attrition rate across rounds, which would improve the quality of the data. It would also be important to include participants from authoritarian states in a new study. An international conference where such experts are speaking or are likely to attend may facilitate their participation. Inclusion of voices from authoritarian sates may improve transferability of the findings and overall trustworthiness of the study.

Finally, research is needed to gauge the impact of cyberattacks by nonstate actors (NSAs) on the emergence of international cybersecurity norms. Reliable attribution of cyberattacks to responsible foreign NSAs may be just as difficult as attributing an attack to a state (Lin, 2016). Further, successful attribution of an attack to an NSA would require additional analysis to determine whether the NSA acted on behalf of a state (Schmitt & Vihul, 2014). This would complicate the Attribution issue and affects the way states evaluate cyberconflict solutions in a manner that was outside the scope of the current study.

Implications

Implications for Positive Social Change

International cybersecurity norms are needed to mitigate the danger cyberconflict presents to international peace and stability (NATO Cooperative Cyber Defense Center of Excellence, 2019; Statement for the Record, 2019). The findings of the current study increase the understanding of the critical points of disagreement among authoritarian and democratic states that must be bridged so international cybersecurity norms can emerge. This knowledge informs future international norm entrepreneurship and advances existing research regarding the development of norms for emerging technology weapons. This study may also create positive social change by promoting moral and ethical state conduct in cyberspace that contributes to international peace and security (see Crowe & Weston-Scheuber, 2015).

Methodological and Theoretical Implications

This study contributes to the understanding of the norm development process for new forms of hostile state conduct enabled by emerging technologies. This study was the first application of the MSF to the development of norms for an emerging technology weapon. I nested the MSF in existing norm evolution theory to provide a clearer model for the norm emergence process. I adapted existing theory to a new area of research and extended it in a manner that enhances its utility in understanding a new realm of problems. Scholarship regarding international norm emergence for emerging technology weapons is in its infancy. Directed energy weapons, nanotechnology, and robotics are a few cutting edge technologies that will require new international norms as they are weaponized. The adaptation of the MSF in the current study extended its utility to the regulation of these emerging technology weapons.

Recommendations for Practice

This study informs future efforts to develop international cybersecurity norms. Norm entrepreneurs may use this knowledge to shape conditions in the problem, policy, and political streams more effectively. This may contribute to the creation of the conditions necessary to bridge the divide between authoritarian and democratic states so that international cybersecurity norms can emerge.

The results of this study also increases the knowledge of the policy community. The panel identified the critical points of disagreement among authoritarian and democratic states that must be overcome. The findings highlight the need for norm entrepreneurship focused on the top obstacles rather than ideal norms. This provides a baseline to focus the efforts of the policy community. Further, the MSF provides a lens to facilitate the development of new policy solutions. This enables norm entrepreneurs to better inform policymakers and contributes to the development of solutions with enhanced viability.

The results of this study also indicated the obstacles to international cybersecurity norms cannot be overcome in the near term. This knowledge may enable norm entrepreneurs to make better use of limited resources by focusing on more promising solutions until conditions in the problem, policy, and political streams improve. The panel forecast also indicated states should increase investments in research and development of attribution technologies and offensive and defensive cybersecurity capabilities. Active deterrence and increased passive cyber defenses are imperfect solutions, but they offer states tangible near term options to enhance their resilience to cyberconflict.

Conclusion

Cyberconflict is an urgent threat to international peace and security (NATO Cooperative Cyber Defense Center of Excellence, 2019; Statement for the Record, 2019). However, democratic and authoritarian states perceive the threat posed cyberconflict in different ways, so they are attempting to solve different security problems (Klimburg & Faesen, 2020; Mazanec, 2015a). As a result, they persistently struggle over competing international cybersecurity norms, leaving cyberconflict virtually unregulated (Kurre, 2017; Painter, 2021). The lack of meaningful consequences for state cyberattacks and the high rewards derived from them incentivize states to engage in cyberconflict (Buchanan, 2020; Mazanec, 2016). This paradigm invites conflict with the potential to produce devastating consequences (E. Diamond, 2014; Moynihan, 2021). Little research existed concerning the conditions necessary for international cybersecurity norms to emerge and mitigate the problem (Gualtier, 2015). The current study extended research by Lantis (2016) and Mazanec (2014a) to decrease that gap in the literature.

A modified Delphi design was employed to obtain the opinions of experts regarding the critical points of disagreement among authoritarian and democratic states that must be overcome to successfully regulate cyberconflict. Further, the MSF was employed as a lens to focus on the components of the norm emergence process for international cybersecurity norms (see Kingdon, 1995). The findings indicated problem nature, attribution, and threat perception are the top obstacles to successful regulation of cyberconflict. This knowledge may contribute to the creation of the conditions necessary to bridge the divide between authoritarian and democratic states so that international cybersecurity norms can emerge.

References

60-day Cybersecurity Review Team. (2009). *2009 cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. U.S. Department of Homeland Security. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (fas.org)

Adamson, L. (2020). International law and international cyber norms: A continuum? In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace: Behavior, power and diplomacy* (pp. 19-42). Rowman & Littlefield.

Akdag, Y. (2017). *Cyber deterrence against cyberwar between the United States and China: A power transition theory perspective* (Publication No. 10640499) [Master's thesis, University of South Florida]. ProQuest Dissertations and Theses Global.

Anderson, T. (2017). Fitting a virtual peg into a round hole: Why existing international law fails to govern cyber reprisals. *Arizona Journal of International and Comparative Law*, *34*(1), 135–158. Microsoft Word - 05_TROY_V2.docx (arizonajournal.org)

Andres, R. B. (2014). Inverted-militarized-diplomacy: How states bargain with cyber weapons. *Georgetown Journal of International Affairs*, 119–129. The-Emerging-Structure-of-Strategic-Cyber-Offense-Cyber-Defense-and-Cyber-Deterrence.pdf (researchgate.net)

Anney, V. N. (2018). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational*

Research and Policy Studies, *5*(2), 272–281. https://www.researchgate.net/profile/Vicent-Anney/post/How-are-validity-and-reliability-issues-dealt-with-in-qualitative-studies/attachment/59d61daa79197b8077979180/AS%3A272153998495749%401441897977647/download/Ensuring+the+quality+of+the+findings+of+qualitative+research+%284%29.pdf

Arimatsu, L. (2012). A treaty for governing cyber-weapons: Potential benefits and practical limitations. In C. Czosseck, R. Ottis, & K. Ziolkoski (Eds.), *2012 4th International conference on cyber conflict (CYCON 2012)* (pp. 91–109). NATO Cooperative Cyber Defense Center of Excellence.

Arof, A. M. (2015). The application of a combined Delphi-AHP method in maritime transport research-A review. *Asian Social Science*, *11*(23), 73–82. https://doi.org/10.5539/ass.v11n23p73

Austin, G. (2016). International legal norms in cyberspace: Evolution of China's national security motivations. In A.-M. Osula & H. Roigas (Eds.), *International cyber norms: Legal policy and industry perspectives* (pp. 171–201). NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch9.pdf

Austin, G., McConnell, B., & Neutze, J. (2015). *Promoting international cyber norms: A new advocacy forum.* EastWest Institute. https://issuu.com/ewipublications/docs/bgcybernorms

Ayalew, Y. E. E. (2015). Cyber warfare: A new hullaballoo under international humanitarian law. *Beijing Law Review*, *6*(4), 209–223. https://doi.org/blr.2015.64021

Banks, W. (2016a). *Developing norms for cyber conflict.* Social Science Research Network. https://doi.org/10.2139/ssrn.2736456

Banks, W. (2016b). State responsibility and attribution of cyber intrusions after Tallinn 2.0. *Texas Law Review*, *95*(7), 1487–1513. https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/

Banks, W. (2017). Developing norms for cyber conflict. In J. Ohlin (Ed.), *Research handbook on remote warfare* (pp. 273–297). Edward Elgar.

Barnes, S. J., & Mattsson, J. (2016). Understanding current and future issues in collaborative consumption: A four-stage Delphi study. *Technological Forecasting and Social Change*, *104*, 200–211. https://doi.org/10.1016/j.techfore.2016.01.006

Barry, M.-L., Steyn, H., & Brent, A. (2008). *Determining the most important factors for sustainable energy technology selection in Africa: Application of the focus group technique.* PICMET '08 - 2008 Portland International Conference on Management of Engineering Technology, Capetown, South Africa. https://doi.org/10.1109/PICMET.2008.4599622

Beard, J. M. (2014). Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law. *Vanderbilt Journal of Transnational Law*, *47*, 67–144. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1195&context=lawfacpub

Beland, D., & Howlett, M. (2016). The role and impact of the multiple-streams approach in comparative policy analysis. *Journal of Comparative Policy Analysis: Research and Practice*, *18*(3), 221–227. https://doi.org/10.1080/13876988.2016.1174410

Bernabeu, E. E., & Katiraei, F. (2011, July 24). *Aurora vulnerability issues & solutions hardware mitigation devices (HMDs). Quanta Technology.* https://www.smartgrid.gov/files/documents/Aurora_Vulnerability_Issues_Solution_Hardware_Mitigation_De_201102.pdf

Bernard, V. (2016). Tactics, techniques, tragedies: A humanitarian perspective on the changing face of war. *International Review of the Red Cross, 97*(900), 959–968. https://doi.org/10.1017/S1816383116000497

Bhusal, N., Gautam, M., & Benidris, M. (2021). Detection of cyber attacks on voltage regulation in distribution systems using machine learning. *IEEE Access*, *9*, 40402-40416. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9373306

Biller, J., & Schmitt, M. N. (2019). Classification of cyber capabilities and operations as weapons, means, or methods of warfare. *International Law Studies, 95*, 180-224. viewcontent.cgi (usnwc.edu)

Biskner, K. (2018). Russian exploitation of the cyber gap in international law. *Army War College Review, 4*(1, 2), 1–14. https://publications.armywarcollege.edu/pubs/3553.pdf

Bloor, M., Sampson, H., Baker, S., & Dahlgren, K. (2013). Useful but no oracle: Reflections on the use of a Delphi Group in a multi-methods policy research study. *Qualitative Research, 15*(1), 57–70. https://doi.org/10.1177/1468794113504103

Bourrie, D. M., Cegielski, C. G., Jones-Farmer, L. A., & Sankar, C. S. (2014). Identifying characteristics of dissemination success using an expert panel. *Decision Sciences Journal of Innovative Education, 12*(4), 357–380. https://doi.org/10.1111/dsji.12049

Boyle, M. J. (2016). The coming illiberal order. *Survival, 58*(2), 35–66. https://doi.org/10.1080/00396338.2016.1161899

Brenner, J. (2017). *Keeping America safe: Toward more secure networks for critical sectors.* https://internetpolicy.mit.edu/critical-infrastructure-2017/

Broeders, D. (2021). The (im) possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: A mid-process assessment. *Journal of Cyber Policy*, 1-21. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1916976

Broeders, D., Adamson, L., & Creemers, R. (2019). Coalition of the unwilling? Chinese and Russian perspectives on cyberspace. *The Hague Program For Cyber Norms Policy Brief* (*October 1, 2019)*, 1-20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493600

Broeders, D., de Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? *Journal of Cyber Policy*, 1-39. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2022.2041061

Bronk, C., & Tikk-Ringas, E. (2013). *Hack or attack? Shamoon and the evolution of cyber conflict. Survival, Global Politics, and Strategy, 55*(2), 81-96. https://doi.org/10.2139/ssrn.2270860

Brown, C. S., & Friedman, D. (2014). A cyber warfare convention? Lessons from the conventions on chemical and biological weapons. In E. B. Landau, & A. Kurz (Eds.), *Arms control and national security: New horizons* (pp. 45–63). The Institute for National Security Studies. http://www.inss.org.il/publication/a-cyber-warfare-convention-lessons-from-the-conventions-on-chemical-and-biological-weapons/

Brown, G., & Poellet, K. (2012). The customary international law of cyberspace. *Strategic Studies Quarterly, 6*(3), 126–145. https://www.hsdl.org/?view&did=722315

Brown, H. E. (2017). *A study of power grid cyber-physical vulnerability through subversion of feedback controllers* [Unpublished doctoral dissertation]. University of Wisconsin, Madison.

Brunnee, J., & Meshel, T. (2015). Teaching an old law new tricks: International environmental law lessons for cyberspace governance. *German Yearbook of International Law, 58,* 1–37. http://www.gyil.org/?page_id=735

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature, 464*(7291), 1025–1028.

https://doi.org/10.1038/nature08932

Butrimas, V. (2014). National security and international policy challenges in a post Stuxnet world. *Lithuanian Annual Strategic Review, 12*(1), 11–31. https://doi.org/10.2478/lasr-2014-0001

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review, 103*(3), 513–563. https://digitalcommons.law.uw.edu/faculty-articles/23

Carlin, J. P. (2015). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harvard National Security Journal, 7,* 391–436. https://harvardnsj.org/wp-content/uploads/sites/13/2016/06/Carlin-FINAL.pdf

Carlin, J. P. (2018). *Dawn of the code war: America's battle against Russia, China, and the rising global cyber threat.* Hachette UK.

Carr, E., & Carr, M. (2016). Beyond 'quasi-norms': The challenges and potential of engaging with norms in cyberspace. In A.-M. Osula & H. Roigas (Eds.), *International cyber norms: Legal policy and industry perspectives* (pp. 87–109). NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives/

Caton, J. L. (2014). *Distinguishing acts of war in cyberspace: Assessment criteria, policy considerations, and response implications.* U.S. Army War College Press.

Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). SAGE Publications.

Chayes, A. (2015). Rethinking warfare: The ambiguity of cyber attacks. *Harvard National Security Journal, 6,* 474–519. https://harvardnsj.org/wp-content/uploads/sites/13/2015/06/Chayes.pdf

Ciglic, K., & Hering, J. (2022). A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy*, 1-15. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2023603

Clarke, R. A., & Knake, R. (2011). *Cyber war: The next threat to national security and what to do about it.* Ecco.

Clinton, H. R. (2010, January 21). *Remarks on internet freedom*. U.S. Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. (2017). *Assessing the threat from electromagnetic pulse (EMP)*. https://michaelmabee.info/wp-content/uploads/2018/05/2017-Executive-Report-on-Assessing-the-Threat-from-EMP-FINAL-April2018.pdf

Cooley, A. (2015a). Authoritarianism goes global: Countering democratic norms. *Journal of Democracy, 26*(3), 49–63. https://www.journalofdemocracy.org/articles/authoritarianism-goes-global-countering-democratic-norms/

Cooley, A. (2015b). Countering democratic norms. *Journal of Democracy, 26*(3), 49–63. https://doi.org/10.1353/jod.2015.0049

Corbin, J. M., & Strauss, A. (2015). Basics of qualitative research (4th ed.). SAGE Publications.

Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. *AJIL Unbound, 111,* 207–212. https://doi.org/10.1017/aju.2017.57

Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary Security Policy, 36*(2), 346–368. https://doi.org/10.1080/13523260.2015.1061765

Crawford, E., & Pert, A. (2015). *International humanitarian law.* Cambridge University Press.

Creemers, R. (Ed.). (2016). *National cyberspace security strategy*. China Copyright and Media. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Creemers, R. (2020). China's conception of cyber sovereignty. In D., Broeders & B., van den Berg (Eds.). *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107-145). *London: Rowman and Littlefield.* https://www.researchgate.net/profile/Dennis-Broeders-2/publication/343833386_Governing_Cyberspace_Behavior_Power_and_Diplomacy/links/5f43c484a6fdcccc43f584f0/Governing-Cyberspace-Behavior-Power-and-Diplomacy.pdf#page=116

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J. W., & Poth, C. N. (2017). *Qualitative inquiry and research design: Choosing* *among five approaches* (4th ed.). SAGE Publications.

Crowe, J., & Weston-Scheuber, K. (2015). *Principles of international humanitarian law.* Edward Elgar.

Cyber Diplomacy Act of 2017, H.R.3776 115th Cong. (2018). https://www.congress.gov/bill/115th-congress/house-bill/3776

Cybersecurity and Infrastructure Security Agency. (2016). *Cyber-attack against Ukrainian critical infrastructure* (ICS Alert IR-ALERT-H-16-056-01). U.S. Department of Homeland Security. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Cybersecurity and Infrastructure Security Agency. (2018). *Russian government cyber activity targeting energy and other critical infrastructure sectors.* U.S. Computer Emergency Readiness Team. https://www.us-cert.gov/ncas/alerts/TA18-074A

Czosseck, C., Ottis, R., & Talihärm, A. M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic, and organizational changes in cyber security. *International Journal of Cyber Warfare and Terrorism, 1*(1), 24–34. https://doi.org/10.4018/ijcwt.2011010103

Danca, D. (2015). Cyber diplomacy—A new component of foreign policy. *Journal of Law and Administrative Sciences, 3,* 91–97. http://jolas.ro/wp-content/uploads/2015/03/jolas3a7.pdf

Davidson, P. (2013). The Delphi technique in doctoral research: Considerations and rationale. *Review of Higher Education & Self-Learning, 6*(22), 53–65. https://pdfs.semanticscholar.org/da18/c89e29b00a24982eb7b40632c40e7083643f

.pdf

Davis, G. D. (2017). *The digital fog of cyber: Case study of the 2007 cyber attack on Estonia* (Publication No. 10618770) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations and Theses Global.

Deeks, A. (2020). Defend forward and cyber countermeasures. *Aegis Series Paper* No. 2004. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670896#

De Loe, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the state of policy Delphi practice: A systematic review evaluating methodological evolution, innovation, and opportunities. *Technological Forecasting and Social Change, 104,* 78–88. https://doi.org/10.1016/j.techfore.2015.12.009

Deitelhoff, N., & Zimmermann, L. (2013). *Things we lost in the fire: How different types of contestation affect the validity of international norms* (PRIF Working Papers No. 18). Frankfurt am Main: Hessische Stiftung Friedens- und Konfliktforschung. http://nbn-resolving.de/urn:nbn:de:0168-ssoar-455201

Denzin, N. (2012). *The landscape of qualitative research* (4th ed.). SAGE Publications.

Department of Defense, Defense Science Board. (2013). *Resilient military systems and the advanced cyber threat.* https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

Derian-Toth, G., Walsh, R., Sergueeva, A., Kim, E., Coon, A., Hadan, H., & Stancombe, J. (2021). Opportunities for public and private attribution of cyber operations. Tallinn Paper No. 12 2021. https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, 1-22. https://doi.org/10.1080/23738871.2021.2000628

Dev, P. R. (2015). Use of force and armed attack thresholds in cyber conflict: The looming definitional gaps and the growing need for formal U.N. response. *Texas International Law Journal, 50*(2 & 3), 381–399. https://texashistory.unt.edu/ark:/67531/metapth838918/

Diamond, E. (2014, July 1). Applying international humanitarian law to cyber warfare. *Law and National Security, 67*. https://papers.ssrn.com/abstract=3093068

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology, 67*(4), 401–409. https://doi.org/10.1016/j.jclinepi.2013.12.002

Dinniss, H. H. (2014). *Cyber warfare and the laws of war.* Cambridge University Press.

du Plessis, E., & Human, S. P. (2007). The art of the Delphi technique: Highlighting its scientific merit. *Health SA Gesondheid, 12*(4), 13–24. https://doi.org/10.4102/hsag.v12i4.268

Dunoff, J., & Rattner, S. R. (2015). *International law: Norms, actors, process: A problem-oriented approach* (4th ed.). Wolters Kluwer Law & Business.

Egan, B. J. (2016, November 10). *Remarks on international law and stability in cyberspace* [Speech]. http://2009-2017.state.gov/s/l/releases/remarks/264303.htm

Eichensehr, K. E. (2014). The cyber-law of nations. *Georgetown Law Journal, 103,* 317–

380. https://ssrn.com/abstract=2447683

Eichensehr, K. E. (2015). Cyberwar & international law step zero. *Texas International Law Journal, 50,* 357–380. https://texashistory.unt.edu/ark:/67531/metapth838918/

Eichensehr, K. E. (2020). The law and politics of cyberattack attribution. *UCLA L. Rev.*, *67*, 520. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3453804

Etikan, I., Musa, S. A., & Alkassim, R. S. (2015). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Etzioni, A. (2013). Mutually assured restraint: A new approach for United States-China relations. *Brown Journal of World Affairs, 20,* 37–51. https://jstor.org/stable/24590973

Fidler, D. P. (2012). Inter arma silent leges redux? The law of armed conflict and cyber conflict. In D. S. Reverton (Ed.), *Cyberspace and national security: Threats, opportunities, and power in a virtual world* (pp. 71–87). Georgetown University Press.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law, 110*(3), 425–479. https://doi.org/10.1017/S0002930000016894

Foltz, A. C. (2012). Stuxnet, Schmitt analysis, and the cyber use of force debate. *Joint Forces Quarterly, 67,* 40–48. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-

48_Foltz.pdf

Foreign Sovereign Immunities Act, 28 U.S.C. §§ 1602 et seq. (1976). 28 USC 1602: Findings and declaration of purpose (house.gov)

Foster, J. S., Jr., Gjelde, E., Graham, W. R., Hermann, R. J., Kluepfel, H. M., Lawson, R. L., Soper, G. K., Wood, L. L., Jr., & Woodard, J. B. (2008). *Report of the Commission to assess the threat to the United States from electromagnetic pulse (EMP) attack: Critical national infrastructures.* http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

Franklin, K. K., & Hart, J. K. (2007). Idea generation and exploration: Benefits and limitations of the policy Delphi research method. *Innovative Higher Education, 31*(4), 237–246. https://doi.org/10.1007/s10755-006-9022-8

Frantz, E., & Kendall-Taylor, A. (2017). The evolution of autocracy: Why authoritarianism is becoming more formidable. *Survival, 59*(5), 57–68. https://doi.org/10.1080/00396338.2017.1375229

Fraser, A. (2016). From the Kalashnikov to the keyboard: International law’s failure to define a cyber use of force is dangerous and may lead to a military response to a cyber use of force. *Hibernian Law Journal, 15,* 86–113. http://hibernianlawjournal.com

Frederick, B., & Johnson, D. E. (2015). *The continued evolution of U.S. law of armed conflict implementation: implications for the U.S. military.* Rand.

G7 Declaration on Responsible States Behavior in Cyberspace, April 11, 2017. https://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf

Galloway, T., & Baogang, H. (2014). China and technical global internet governance: Beijing's approach to multi-stakeholder governance within ICANN, WSIS and the IGF. *China: An International Journal, 12*(3), 72–93. https://doi.org/10.1353/chn.2014.0026

Garrie, D. B. (2012). Cyber warfare, what are the rules. *Journal of Law & Cyber Warfare, 1*(1), 1–7. https://www.jstor.org/stable/26441232

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security, 38*(2), 41–73. https://doi.org/10.1162/ISEC_a_00136

Geib, R., & Lahmann, H. (2013). Freedom and security in cyberspace: Shifting the focus away from military responses towards non-forcible countermeasures and collective threat-prevention. In K. Ziolkowski (Ed.), *Peacetime regime for State activities in cyberspace: International law, international relations and diplomacy* (pp. 621–657). Cooperative Cyber Defense Center of Excellence.

Giles, K. (2012). Russia's public stance on cyberspace issues. In C. Czosseck, R. Ottis, & K. Ziolkoski (Eds.), *2012 4th International conference on cyber conflict (CYCON 2012)* (pp. 63–75). NATO Cooperative Cyber Defense Center of Excellence.

Giles, K. (2017). *Prospects for the rule of law in cyberspace.* Defense Department, Army, Strategic Studies Institute. Prospects for the Rule of Law in Cyberspace (armywarcollege.edu)

Giles, K., & Monaghan, A. (2015). *Legality in cyberspace: An adversary view.* Defense Department, Army, Strategic Studies Institute. Legality in Cyberspace: An

Adversary View (armywarcollege.edu)

Gill, F., Leslie, G., Grech, C., & Latour, J. (2013). Using a web-based survey tool to undertake a Delphi study: Application for nurse education research. *Nurse Education Today, 33*(11), 1322–1328. https://doi.org/10.1016/j.nedt.2013.02.016

Global perspective on cyber threats: Hearings before the U.S. House of Representatives Committee on Appropriations*,* 114th Cong. (2015). https://www.hsdl.org/?view&did=790874

Goldsmith, J. (2013). How cyber changes the laws of war. *European Journal of International Law, 24*(1), 129–138. https://doi.org/10.1093/ejil/cht004

Goldsmith, J., & Wu, T. (2008). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Goyal, N., Howlett, M., & Taeihagh, A. (2021). Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework. *Regulation & Governance*, *15*(4), 1020-1034. Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework (researchgate.net)

Goychayev, R. (2014). *Clash of threat perceptions: In nuclear and cyber paradigms* [Unpublished Master's Thesis]. University of Washington.

Gray, C. S. S. (2013). *Making strategic sense of cyber power: Why the sky is not falling.* U.S. Army War College Press. Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling (armywarcollege.edu)

Greenbank, P. (2003). The role of values in educational research: The case for reflexivity. *British Educational Research Journal, 29*(6), 791–801. https://doi.org/10.1080/0141192032000137303

Grigsby, A. (2017). The end of cyber norms. *Survival, 59*(6), 109–122. https://doi.org/10.1080/00396338.2017.1399730

Grzegorzewski, P. (2006). The coefficient of concordance for vague data. *Computational Statistics & Data Analysis, 51*(1), 314–322. https://doi.org/10.1016/j.csda.2006.04.027

Gualtier, K. (2015). *Information operations under international law: A Delphi study into the legal standing of cyber warfare* [Unpublished doctoral dissertation]. Walden University.

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Communication and Technology, 29*(2), 75–91. https://doi.org/10.1007/BF02766777

Gupta, U. G., & Clarke, R. E. (1996). Theory and applications of the Delphi technique: A bibliography (1975–1994). *Technological Forecasting and Social Change, 53*(2), 185–211. https://doi.org/10.1016/S0040-1625(96)00094-7

Haacke, J. (2021). Foreign policy entrepreneurs, policy windows, and “pragmatic engagement”: Reconsidering insights of the multiple streams framework and the Obama Administration’s 2009 policy shift toward military-run Myanmar. *Foreign Policy Analysis*, *17*(3).

Multiple Streams Framework and the Obama Administration&#x0027;s 2009 Policy Shift Toward Military-Run Myanmar (silverchair.com)

Haataja, S. (2013). Technology, violence, and law: Cyber attacks and uncertainty in international law. In R. Kuusisto & E. Kurkinen (Eds.), *Proceedings of the European conference on information warfare and security* (pp. 315–322). Academic Conferences.

Habibi, A., Sarafrazi, A., & Izadyar, S. (2014). Delphi technique theoretical framework in qualitative research and science. *International Journal of Engineering and Science, 3*(4), 8–13. www.theijes.com

Hasson, F., & Keeney, S. (2011). Enhancing rigor in the Delphi technique research. *Technological Forecasting and Social Change, 78*(9), 1695–1704. https://doi.org/10.1016/j.techfore.2011.04.005

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008–1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–885. http://digitalcommons.law.yale.edu/fss_papers/3852

Healey, J., & Grindal, K. (Eds.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012.* Cyber Conflict Studies Association.

Hearing to Receive Testimony on the Future of Warfare: U.S. Senate Armed Services Committee, 114th Cong. (2015) (Testimony of K. Alexander). Microsoft Word - KAB SASC Testimony - Final (11.2.15).docx (senate.gov)

Hendrickson, B. T. (2015). *Chinese cyber espionage and cyber sovereignty: Lack of acceptable behavior in cyberspace* [Unpublished master's thesis]. Utica College.

Herweg, N., Zahariadis, N., & Zohlnhofer, R. (2018). The multiple streams framework: Foundations, refinements, and empirical applications. In C. Weible & P. Sabatier (Eds.). *Theories of the policy process* (pp. 17-53). Routledge.

Herweg, N. (2016). Clarifying the concept of policy-communities in the multiple-streams framework. In R. Zohlnhofer & F. W. Rub (Eds.), *Decision-making under ambiguity and time constraints: Assessing the multiple-streams framework* (pp. 125–145). ECPR Press.

Hollis, D. B., & Neutze, J. (2020). Defending democracies via cybernorms. In D. B. Hollis & J. D. Ohlin (Eds.). *Defending Democracies: Combating Foreign Election Interference in a Digital Age* (pp. 315-348). Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3635782

Horvath, R. (2016). The reinvention of 'traditional values': Nataliya Narochnitskaya and Russia's assault on universal human rights. *Europe-Asia Studies, 68*(5), 868–892. https://doi.org/10.1080/09668136.2016.1184230

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Hsu, C., & Sandford, B. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation 12*(10), 1–8. https://doi.org/10.7275/pdz9-th90

Huang, Z., & Macak, K. (2017). Towards the international rule of law in cyberspace: Contrasting Chinese and western approaches. *Chinese Journal of International Law, 16*(2), 271–310. https://doi.org/10.1093/chinesejil/jmx011

Inboden, R. S., & Chen, T. C. (2012). China's response to international normative pressure: The case of human rights. *International Spectator, 47*(2), 45–57. https://doi.org/10.1080/03932729.2012.683277

Inkster, N. (2017). *China's cyber power* (1st ed.). Routledge.

International Court of Justice. (1949). *Affaire du Détroit de Corfou* [The Corfu Channel Case]. http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

International Court of Justice. (1985). *Libyan Arab Jamahriya v. Malta,* 1985 ICJ 13. http://www.icj-cij.org/files/case-related/68/068-19850603-JUD-01-00-EN.pdf

International Court of Justice. (1986). *Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America) Merits Judgment of 27 June 1986.* International Court of Justice. http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

International Court of Justice. (1996). *Legality of the threat or use of nuclear weapons* (Advisory Opinion of 8 July 1996). http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

International Court of Justice. (2005). *Democratic Republic of the Congo v. Uganda*, 2005 ICJ 168. http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf

Izycki, E., & Vianna, E. W. (2021). Critical infrastructure: A battlefield for cyber warfare? In J., Lopez, A., Ambareen, & K., Perumalla (Eds.). *16th International Conference on Cyber Warfare and Security* (pp. 454-464). Academic Conferences Limited. 58552webtoc.pdf (proceedings.com)

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly, 9*(1), 60–85. https://www.jstor.org/stable/26270834

Jensen, E. T. (2013). The future of the law of armed conflict: Ostriches, butterflies, and nanobots. *Michigan Journal of International Law, 35*(2), 253–317. https://repository.law.umich.edu/mjil/vol35/iss2/3

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review, 4*(11), 22–27. http://www.timreview.ca

Kalaian, S. A., & Kasim, R. M. (2012). Terminating sequential Delphi survey data collection, practical assessment. *Research & Evaluation, 17*(5), 1–10. http://pareonline.net/getvn.asp?v=17&n=5

Kaplan, F. (2016). *Dark territory: The secret history of cyber war.* Simon & Schuster.

Kavan, S., Dvorackova, O., Pokorny, J., & Brumarova, L. (2021). Long-term power outage and preparedness of the population of a region in the Czech Republic: A case study. *Sustainability*, *13*(23), 1-14. https://doi.org/10.3390/su132313142

Keeney, S., McKenna, H., & Hasson, F. (2011). *The Delphi technique in nursing and* *health research.* John Wiley & Sons.

Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, 1-15. https://doi.org/10.1093/cybsec/tyab014

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kent, R. (2016). The future of warfare: Are we ready? *International Review of the Red Cross, 97*(900), 1341–1378. https://doi.org/10.1017/S1816383116000412

Kilovaty, I. (2018). Doxfare: Politically motivated leaks and the future of the norm on non-intervention in the era of weaponize d information. *Harvard National Security Journal, 9*(1), 146–179. https://harvardnsj.org/wp-content/uploads/sites/13/2018/01/4_Kilovaty_Doxfare-1.pdf

Kingdon, J. W. (1984). *Agendas, alternatives, and public policies*. Longman Higher Education.

Kingdon, J. W. (1995). *Agendas, alternatives, and public policies* (2nd ed.). Harper Collins.

Kiyuna, A., & Conyers, L. (2015). *Cyberwarfare sourcebook.* Lulu.com.

Klang, M. (2006). *Disruptive technology: Effects of technology regulation on democracy* [Unpublished doctoral thesis]. University of Gothenburg.

Kleinwachter, W. (2012). Internet governance outlook 2012: Cold War or constructive dialogue? *Journal of Computer, Media & Telecommunications, 17*(1), 14. http://connection.ebscohost.com/c/articles/73764090/internet-governance-outlook-2012-cold-war-constructive-dialogue

Klimburg, A. & Faesen, L. (2020). A balance of power in cyberspace. In D., Broeders &

B., van den Berg (Eds.). *Governing cyberspace: Behavior, power, and diplomacy* (pp. 145-172). Rowman and Littlefield. https://www.researchgate.net/profile/Dennis-Broeders-2/publication/343833386_Governing_Cyberspace_Behavior_Power_and_Diplomacy/links/5f43c484a6fdcccc43f584f0/Governing-Cyberspace-Behavior-Power-and-Diplomacy.pdf#page=116

Knake, R. K. (2010). *Internet governance in an age of cyber insecurity.* Council on Foreign Relations. https://www.cfr.org/report/internet-governance-age-cyber-insecurity

Koh, H. H. (2012, September 18). *International law in cyberspace* [Speech]. USCYBERCOM Inter-Agency Legal Conference. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia, and Kyrgyzstan. *European Scientific Journal, 10*(7), 237–245. https://doi.org/10.19044/esj.2014.v10n7p%p

Kremer, J. F., & Muller, B. (2013). SAM: A framework to understand emerging challenges to states in an interconnected world. In J. F. Kremer & B. Muller (Eds.), *Cyberspace and international relations: Theory, prospects, and challenges* (pp. 41–58). Springer.

Krisch, N. (2014). The decay of consent: International law in an age of global public goods. *American Journal of International Law, 108*(1), 1–40. https://doi.org/10.5305/amerjintelaw.108.1.0001

Krutskikh, A., & Streltsov, A. (2014). International law and the problem of international information security. *International Affairs, 6,* 64–76. https://academic.oup.com/ia

Kshetri, N. (2014). *Cybersecurity and international relations: The U.S. engagement with China and Russia.* http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf

Kulikova, A. (2022). Cyber norms: Technical extensions and technological challenges. *Journal of Cyber Policy*, 1-20. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2020316?scroll=top&needAccess=true

Kurowska, X. (2020). What does Russia want in cyber diplomacy? A primer. In D., Broeders & B., van den Berg (Eds.). *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 85-106). *Rowman and Littlefield.* https://www.researchgate.net/profile/Dennis-Broeders-2/publication/343833386_Governing_Cyberspace_Behavior_Power_and_Diplomacy/links/5f43c484a6fdcccc43f584f0/Governing-Cyberspace-Behavior-Power-and-Diplomacy.pdf#page=116

Kurre, C. (2017). *Participation, coordination, agreement...action? Evaluating the multistakeholder model in internet governance* [Masters Thesis, Georgetown University]. https://doi.org/10.2139/ssrn.2955231

Lam, C. (2018). A slap on the wrist: Combatting Russia's cyber attack on the 2016 U.S. presidential election. *Boston College Law Review, 59,* 2167–2201.

https://lawdigitalcommons.bc.edu/bclr/vol59/iss6/7/

Lantis, J. S. (2016). *Arms and influence: U.S. technology innovations and the evolution of international security norms*. Stanford Security Studies.

Lantis, J. S., & Bloomberg, D. J. (2018). Changing the code? Norm contestation and US antipreneurism in cyberspace. *International Relations*, *32*(2), 149-172. https://doi.org/10.1177/0047117818763006

Lee, J.-A. (2013). The red storm in uncharted waters: China and international cyber security. *UMKC Law Review, 82*, 951–966. https://umkclawreview.org

Lessig, L. (2006). Commons. In J. N. Drobak (Ed.), *Norms and the law* (pp. 89–104). Cambridge University Press.

Li, S. (2013). When does internet denial trigger the right of armed self-defense. *Yale Journal of International Law, 38,* 179–216. http://digitalcommons.law.yale.edu/yjil/vol38/iss1/5

Liangliang, B. (2007). The applicability of "the multiple-streams framework" to policy process in China: Taking policy process of water pollution management and cooperation between Jiangsu province and Zhejiang province as examples. *Journal of Public Management, 2007*(2), 5–25. The Applicability of"the Multiple-Streams Framework" to Policy Process in China --Taking Policy Process of Water Pollution Management and Cooperation Between Jiangsu Province and Zhejiang Province as Examples--《Journal of Public Management》2007年02期 (cnki.com.cn)

Liaropoulos, A. (2014). Cyberconflict and theoretical paradigms: Current trends and future challenges in the literature. In G. Tsihrintzis & A. Liaropoulos (Eds.), *Proceedings of the 13th European conference on cyber warfare and security* (pp. 133–139). Academic Conferences. https://www.researchgate.net/publication/264337838

Liivoja, R. (2016). Technological change and the evolution of the law of war. *International Review of the Red Cross, 97*(900), 1157–1177. https://doi.org/10.1017/S1816383116000424

Liivoja, R., Leins, K., & McCormack, T. (2015). Emerging technologies of warfare. In R. Liivoja & T. McCormack (Eds.). *Routledge handbook of the law of armed conflict* (pp. 603–622). Routledge.

Lin, H. (2016). Attribution of malicious cyber incidents: From soup to nuts. *Journal of International Affairs, 70*(1), 106–171. https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents

Linstone, H. A., & Turoff, M. (2011). Delphi: A brief look backward and forward. *Technological Forecasting and Social Change, 78*(9), 1712–1719. https://doi.org/10.1016/j.techfore.2010.09.011

Litwak, R., & King, M. (2015). *Arms control in cyberspace*? Wilson Center. https://www.wilsoncenter.org/sites/default/files/arms_control_in_cyberspace.pdf

Lonergan, S. W. (2017). *Cyber power and the international system* (Publication No. 10620131) [Doctoral dissertation, Columbia University]. ProQuest Dissertations and Theses Global.

Lowe, V. (2016). *International law: A very short introduction*. Oxford University Press.

Lyytinen, K., & Rose, G. M. (2003). Disruptive information system innovation: The case of internet computing. *Information Systems Journal, 13*(4), 301–330. https://doi.org/10.1046/j.1365-2575.2003.00155.x

Macak, K. (2021). Unblurring the lines: Military cyber operations and international law. *Journal of Cyber Policy*, 1-18. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2014919

Macak, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law, 30*(4), 877–899. https://doi.org/10.1017/S0922156517000358

Markoff, M. (2017). *Explanation of position at the conclusion of the 2016–2017 UN group of governmental experts (GGE) on developments in the field of information and telecommunications in the context of international security.* United Nations Institute for Disarmament Research. https://tinyurl.com/ychz6bhc

Mattis, J. (Ed.). (2018). *DoD dictionary of military and associated terms* (Rev. ed.). U.S. Department of Defense. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Mazanec, B. M. (2014a). *Norm wars: The evolution of norms for emerging-technology weapons, from chemical weapons to cyber warfare* [Unpublished doctoral dissertation]. George Mason University.

Mazanec, B. M. (2014b). Towards a cyber war taboo? A framework to explain the emergence of norms for the use of force in cyberspace. *National Cybersecurity Institute Journal, 1*(1), 48–55.

https://www.excelsior.edu/about/publications/national-cybersecurity-institute-journal/

Mazanec, B. M. (2015a). *The evolution of cyber war: International norms for emerging-technology weapons.* Potomac Books.

Mazanec, B. M. (2015b). Why international order in cyberspace is not inevitable. *Strategic Studies Quarterly, 9*(2), 78–98. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-2/mazanec.pdf

Mazanec, B. M. (2016). Constraining norms for cyber warfare are unlikely. *Georgetown Journal of International Affairs, 17*(3), 100–109. https://doi.org/10.1353/gia.2016.0040

McGhee, J. E. (2013). Cyber redux: The Schmitt analysis, Tallinn manual, and US cyber policy. *Journal of Law & Cyber Warfare, 2*(1), 64–103. Cyber Redux on JSTOR

McGuffin, C., & Mitchell, P. (2014). On domains: Cyber and the practice of warfare. *International Journal, 69*(3), 394–412. https://doi.org/10.1177/0020702014540618

Mead, W. R. (2014). The return of geopolitics: The revenge of the revisionist powers. *Foreign Affairs, 93*(3), 69–79. https://www.foreignaffairs.com/articles/china/2014-04-17/return-geopolitics

Mele, S. (2014). Legal considerations on cyber-weapons and their definition. *Journal of Law & Cyber Warfare, 3,* 52–69. https://jstor/org/stable/26432559

Meyer, P. (2013). Digital diplomacy: Working towards a cyber code of conduct. *Jane's*

Intelligence Review, 25(10), 30-33.

Meyer, P. (2015). Seizing the diplomatic initiative to control cyber conflict. *Washington Quarterly, 38*(2), 47–61. https://doi.org/10.1080/0163660X.2015.1064709

Ministry of Foreign Affairs of the People's Republic of China. (2017). *International Strategy of Cooperation on Cyberspace.* Ministry of Foreign Affairs of the People's Republic of China. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

Mishra, D., & Mishra, S. (2014). Understanding factors affecting attrition and retention among shipping company employees in Kutch: A Delphi approach. *International Journal of Management, IT and Engineering, 4*(7), 277–289. http://www.ijmra.us

Mix, C. (2014). Internet communication blackout: Attack under non-international armed conflict. *Journal of Law & Cyber Warfare, 3*(1), 70–102. https://www.jstor.org/stable/26432560

Mok, K. (2017). Cyber threat or cyber threat inflation? Assessing the risk to U.S. National security. *Small Wars Journal.* https://smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security

Moses, L. B. (2007). Recurring dilemmas: The law's race to keep up with technological change. *University of Illinois Journal of Law, Technology & Policy, 2007*(7), 239–415. http://illinoisjltp.com/journal/wp-content/uploads/2013/10/05-05-08_Moses_AHW_Formatted_FINAL.pdf

Moynihan, H. (2021). The vital role of international law in the framework for responsible state behavior in cyberspace. *Journal of Cyber Policy*, *6*(3), 394-410. https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550

Mueller, B. (2014). *The laws of war and cyberspace on the need for a treaty concerning cyber conflict* (Monograph 14.2; Strategic Update). London School of Economics.

Murphy, J. F. (2013). Cyber war and international law: Does the international legal process constitute a threat to U.S. vital interests? *International Law Studies, 89*(1), 309–340. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1030&context=ils

Musiani, F., & Pohle, J. (2014). NETmundial: Only a landmark event if "digital cold war" rhetoric abandoned. *Internet Policy Review, 3*(1), 1–9. https://doi.org/10.14763/2014.1.251

Naderifar, M., Goli, H., & Ghaljaei, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education, 14*(3), e67670. https://doi.org/10.5812/sdme.67670

Nathan, A. J. (2015). China's challenge. *Journal of Democracy, 26*(1), 156–170. https://doi.org/10.1353/jod.2015.0012

National Academies of Sciences, Engineering, and Medicine. (2017). *Enhancing the resilience of the nation's electricity system.* National Academies Press.

NATO Cooperative Cyber Defense Center of Excellence. (2019). *Trends in International Law for Cyberspace.* https://www.ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf

Neumann, V. (2006). The incoherence of US counternarcotics policy in Colombia:

Exploring the breaches in the policy cycle. *European Journal of Development Research, 18*(3), 412–434. https://doi.org/10.1080/09578810600893494

Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *California Law Review, 101,* 1079–1130. Navigating Jus Ad Bellum in the Age of Cyber Warfare (californialawreview.org)

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189

North Korea Nuclear EMP Attack: An Existential Threat. U.S. House of Representatives Committee on Homeland Security, 115th Cong. (2017) (testimony of W. R. Graham & P. V. Pry). https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf

Nye, J. S. (2014). *The regime complex for managing global cyber activities* (No. 1; Global Commission on Internet Governance Paper Series, p. 16). Chatham House. https://dash.harvard.edu/handle/1/12308565

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Ohlin, J. D. (2016). Did Russian cyber interference in the 2016 election violate international law. *Texas Law Review, 95*(7), 1579–1598. Did Russian Cyber Interference in the 2016 Election Violate International Law? (archive.org)

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management,* *42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. T. (2008). Interviewing the interpretive researcher: A method for addressing the crises of representation, legitimation, and praxis. *International Journal of Qualitative Methods, 7*(4), 1–17. https://doi.org/10.1177/160940690800700401

Osula, A.-M., & Roigas, H. (2016). International norms limiting state activity in cyberspace. In A.-M. Osula & H. Roigas (Eds.), *International cyber norms: Legal policy and industry perspectives* (pp. 11–13). NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf

Painter, C. (2021). The United Nations' cyberstability processes: Surprising progress but much left to do. *Journal of Cyber Policy*, 1-6. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2014920

Palmieri, D. (2016). How warfare has evolved—A humanitarian organization's perception: The case of the ICRC, 1863–1960. *International Review of the Red Cross, 97*(900), 985–998. https://doi.org/10.1017/S1816383116000370

Panetta, L. E. (2012, March 1). *Remarks by Secretary of Defense Leon E. Panetta* [Speech]. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4988

Pare, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi studies. *Information & Management, 50*(5), 207–217.

https://doi.org/10.1016/j.im.2013.03.003

Patterson, R. (2014). Silencing the call to arms: A shift away from cyber attacks as warfare. *Loyola of Los Angeles Law Review, 48,* 969–1015. https://digitalcommons.lmu.edu/llr/vol48/iss3/10

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

Permanent Court of International Justice. (1927). *Recueil des arrêts: Affaire du "Lotus"* [The case of the S.S. "Lotus"]. http://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf

Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M., & Riehm, U. (2014). *What happens during a blackout: Consequences of a prolonged and wide-ranging power outage.* The Institute for Technology Assessment and Systems Analysis. What happens during a blackout: Consequences of a prolonged an... (kit.edu)

Piatkowski, M. (2017). The definition of the armed conflict in the conditions of cyber warfare. *Polish Political Science Yearbook, 46*(1), 271–280. https://doi.org/10.15804/ppsy2017117

Pinheiro, L. (2016). *Reflections on internet governance and regulation with special consideration of the ICANN* (SSRN Scholarly Paper ID 2796402). Social Science Research Network. https://papers.ssrn.com/abstract=2796402

Post, D. G., & Kehl, D. (2015). *Controlling Internet Infrastructure: The "IANA Transition" and why it matters for the future of the internet, Part 1.* Open Technology Institute. https://static.newamerica.org/attachments/2964-controlling-internet-infrastructure/IANA_Paper_No_1_Final.32d31198a3da4e0d859f989306f6d480.pdf

Powell, C. (2003). The Delphi technique: Myths and realities. *Journal of Advanced Nursing, 41*(4), 376–382. https://doi.org/10.1046/j.1365-2648.2003.02537.x

Preston, S. W. (Ed.). (2016). *Department of Defense law of war manual* (2nd ed.). Department of Defense.

Pry, P. V. (2017). *Life without electricity: Storm-induced blackouts and implications for EMP attack* (Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack). Electromagnetic Pulse Commission. https://michaelmabee.info/wp-content/uploads/2018/05/2017-Life-Without-Electricity-FINAL-April2018.pdf

Radu, R. (2013). Negotiating meanings for security in the cyberspace. *Info, 15*(6), 32–41. https://doi.org/10.1108/info-04-2013-0018

Raustiala, K. (2016). Governing the Internet. *American Journal of International Law, 110*(3), 491–503. https://doi.org/10.1017/S0002930000016912

Rawat, P., & Morris, J. C. (2016). Kingdon's "streams" model at thirty: Still relevant in the 21st century? *Politics & Policy, 44*(4), 608–638. https://doi.org/10.1111/polp.12168

Rege, A. (2014). Digital information warfare trends in Eurasia. *Security Journal, 27*(4), 374–398. https://doi.org/10.1057/sj.2012.35

Remus, T. (2013). Cyber-attacks and international law of armed conflicts; a jus ad bellum perspective. *J. Int't Com. L. & Tech.*, *8*, 179. Cyber-Attacks and International Law of Armed Conflicts; a Jus ad Bellum Perspective 8 Journal of International Commercial Law and Technology 2013 (heinonline.org)

Richmond, J. (2012). Evolving battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict? *Fordham International Law Journal, 35*(3), 842–894. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2433&context=ilj

Rid, T. (2013). *Cyber war will not take place.* Oxford University Press.

Rid, T., & Arquilla, J. (2012). Think again: Cyberwar. *Foreign Policy, 192,* 80–84. https://foreignpolicy.com/2012/02/27/think-again-cyberwar/

Roberts, S. (2014). Cyber wars: Applying conventional laws to war to cyber warfare and non-state actors. *Northern Kentucky Law Review, 41,* 535–572. Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors Notes 41 Northern Kentucky Law Review 2014 (heinonline.org)

Roigas, H. (2015). The Ukraine Crisis as a test for proposed cyber norms. In K. Geers (Ed.). *Cyber war in perspective: Russian aggression against Ukraine* (pp. 135–144). NATO Cooperative Cyber Defense Center of Excellence. https://www.ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine

Roguski, P. (2020). *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views.* The Hague Program For Cyber Norms Policy Brief. March 2020.

https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y

Rosenzweig, P. (2012). The international governance framework for cybersecurity. *Canada-United States Law Journal, 37*(2), 405–432. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1071&context=cuslj

Russell, A. L. (2014). *Cyber blockades*. Georgetown University Press.

Ruvalcaba-Gomez, E., Criado, J., & Gil-Garcia, J. (2020). Analyzing open government policy adoption through the multiple streams framework: The roles of policy entrepreneurs in the case of Madrid. *Public Policy and Administration*. https://doi.org/10.1177/0952076720936349

Saldana, J. (2015). *The coding manual for qualitative researchers* (3rd ed.). SAGE Publications.

Sander, B. (2017). *Cyber insecurity and the politics of international law* (SSRN Scholarly Paper ID 2983813; European Society of International Law Reflections Series). Social Science Research Network. https://papers.ssrn.com/abstract=2983813

Sander, B. (2019). *The sound of silence: International law and the governance of peacetime cyber operations* (SSRN Scholarly Paper ID 3411907). Social Science Research Network. https://papers.ssrn.com/abstract=3411907

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown.

Sarmiento-Mirwaldt, K. (2015). Can multiple streams predict the territorial cohesion debate in the EU? *European Urban and Regional Studies, 22*(4), 431–445. https://doi.org/10.1177/0969776413481984

Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences, 28*(3), 763–774. https://doi.org/10.1111/j.1540-5915.1997.tb01330.x

Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Villanova Law Review, 56*(3), 569–605. Cyber Operations and the Jud Ad Bellum Revisited (villanova.edu)

Schmitt, M. N. (2012). “Attack” as a term of art in international law: The cyber operations context. In C. Czosseck, R. Ottis, & K. Ziolkoski (Eds.), *2012 4th international conference on cyber conflict (CYCON 2012)* (pp. 283–293). NATO Cooperative Cyber Defense Center of Excellence.

Schmitt, M. N. (2013a). Below the threshold cyber operations: The countermeasures response option and international law. *Virginia Journal of International Law, 54*(3), 697–732. 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law by Michael N. Schmitt :: SSRN

Schmitt, M. N. (2013b). Classification of cyber conflict. *International Law Studies, 89*(1), 233–251. viewcontent.cgi (usnwc.edu)

Schmitt, M. N., & Vihul, L. (2014). Proxy wars in cyberspace: The evolving international law of attribution. *Fletcher Security Review, 1,* 53–73. https://ssrn.com/abstract=2388202

Schmitt, M. N., & Vihul, L. (2016a). The nature of international law cyber norms. In A.-M. Osula & H. Roigas (Eds.), *International cyber norms: Legal policy and industry perspectives* (pp. 23–47). NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf

Schmitt, M. N., & Vihul, L. (2016b). Respect for sovereignty in cyberspace. *Texas Law Review, 95,* 1639–1671. Schmitt.Vihul_.pdf (texaslawreview.org)

Schmitt, M. N., & Vihul, L. (2017a). Sovereignty in cyberspace: Lex lata vel non? *AJIL Unbound, 111,* 213–218. https://doi.org/10.1017/aju.2017.55

Schmitt, M. N., & Vihul, L. (Eds.). (2017b). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.

Schmitt, M. N., & Watts, S. (2015). The decline of international humanitarian law opinion juris and the law of cyber warfare. *Texas International Law Journal, 50,* 189–231. The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare by Michael N. Schmitt, Sean Watts :: SSRN

Seaman, S. L. (2013). *Policy, problems, and politics: A multiple streams analysis of Arizona's Senate Bill 1070* [Unpublished doctoral dissertation] Walden University.

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age.* Public Affairs.

Segal, A. (2017). *Chinese cyber diplomacy in a new era of uncertainty* (Aegis Paper

Series No. 1703). Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new "digital divide": Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. *Stanford Journal of International Law, 50,* 119–184. Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity Symposium 50 Stanford Journal of International Law 2014 (heinonline.org)

Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Business Law Journal, 16*(2), 217–256. BLJ-16.2-Shackelford-Russell-Haut.pdf (ucdavis.edu)

Shackelford, S. J., Sulmeyer, M., Deckard, A. N. C., Buchanan, B., & Micic, B. (2017). From Russia with love: Understanding the Russian cyber threat to U.S. critical infrastructure and what to do about it. *Nebraska Law Review, 96*(2), 320–338. From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It (unl.edu)

Shaffer, G. C., & Pollack, M. A. (2009). Hard vs. soft law: Alternatives, complements, and antagonists in international governance. *Minnesota Law Review, 94,* 706–790. Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance 94 Minnesota Law Review 2009-2010 (heinonline.org)

Shah, R. (2015). Law enforcement and data privacy—A forward-looking approach. *Yale*

Law Journal, 125(2), 543–558. Law Enforcement and Data Privacy: A Forward-Looking Approach (yale.edu)

Shakarian, P., Lei, H., & Lindelauf, R. (2014). Power grid defense against malicious cascading failure. In A. Lomuscio, P. Scerri, A. Bazzan, & M. Huhns (Eds.), *Proceedings of the 13th international conference on autonomous agents and multiagent systems* (pp. 813–820). International Foundation for Autonomous Agents and Multiagent Systems. http://www.dtic.mil/dtic/tr/fulltext/u2/a603639.pdf

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach.* Syngress.

Shanghai Cooperation Organization. (2009). *Yekaterinburg declaration of the heads of the member states of the Shanghai Cooperation Organization.* http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t569701.shtml

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review, 1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

Shibo, J. (2014). War by internet: Cyber attack and the application of law of war. *International Law Review of Wuhan University, 4,* 43–70.

Simmons, N. (2014). A brave new world: Applying international law of war to cyber-attacks. *Journal of Law & Cyber Warfare, 4*(1), 42–108. A Brave New World on JSTOR

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6,* 1–22. download (psu.edu)

Slack, C. (2016). Wired yet disconnected: The governance of international cyber relations. *Global Policy, 7*(1), 69–78. https://doi.org/10.1111/1758-5899.12268

Sobaih, A. E. E., Ritchie, C., & Jones, E. (2012). Consulting the oracle?: Applications of modified Delphi technique to qualitative research in the hospitality industry. *International Journal of Contemporary Hospitality Management, 24*(6), 886–906. https://doi.org/10.1108/09596111211247227

Sood, A., & Enbody, R. (2014). *Targeted cyber attacks: Multi-staged attacks driven by exploits and malware.* Syngress.

Statement for the record: Worldwide threat assessment of the U.S. intelligence community, U.S. Senate Armed Services Committee, 114th Cong. (2015) (testimony of J. Clapper). https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Statement for the record: Worldwide threat assessment of the U.S. intelligence community, U.S. Senate Armed Services Committee, 114th Cong. (2016) (testimony of J. Clapper). https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Statement for the record: Worldwide threat assessment of the U.S. intelligence *community, U.S. Senate Select Committee on Intelligence, 115th Cong.* (2018) (testimony of D. Coats). https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Statement for the record: Worldwide threat assessment of the U.S. intelligence community, U.S. Senate Select Committee on Intelligence, 116th Cong. (2019) (testimony of D. Coats). https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Statement for the record: Worldwide threat assessment of the U.S. intelligence community, U.S. Senate Select Committee on Intelligence, 117th Cong. (2021) (testimony of A. Haines). ATA-2021-Unclassified-Report.pdf (dni.gov)

Stevens, T. (2017, January 10). Cyberweapons: An emerging global governance architecture. *Palgrave Communications, 3,* 16102. https://doi.org/10.1057/palcomms.2016.102

Stockburger, P. Z. (2016). Known unknowns: State cyber operations, cyber warfare, and the jus ad bellum. *American University International Law Review, 31*(4), 545–591. Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum (american.edu)

Sumsion, T. (1998) The Delphi technique: An adaptive research tool. *British Journal of Occupational Therapy 61*(4), 153-156. https://doi.org/10.1177/030802269806100403

Sutton, V. (2015). *Emerging technologies law.* Vargas Publishing.

Taddeo, M. (2014). Information warfare: The ontological and regulatory gap. *APA Newsletter on Philosophy and Computers, 14*(1), 13–20. apa-cyberwarfare-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

Task Force on National and Homeland Security. (2020). *A call to action for America: Task force on national and homeland security, secure the grid coalition, and other partners* (Document No. AD17-8–000). A-Call-to-Action-for-America-Revised-on-6-11-2020-1.pdf (emptaskforce.us)

Theodoulou, S. Z., & Cahn, M. A. (2012). *Public policy: The essential readings* (2nd ed.). Pearson.

Theohary, C. A., & Rollins, J. W. (2015). *Cyberwarfare and cyberterrorism: In brief.* Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R43955/4

Tiernan, A., & Burke, T. (2002). A load of old garbage: Applying garbage-can theory to contemporary housing policy. *Australian Journal of Public Administration, 61*(3), 86–97. https://doi.org/10.1111/1467-8500.00287

Tikk, E. (2016). International cyber norms dialogue as an exercise of normative power. *Georgetown Journal of International Affairs, 17*(3), 47–59. https://doi.org/10.1353/gia.2016.0036

Tikk, E. (2018). Will cyber consequences deepen disagreement on international law? *Temple International & Comparative Law Journal, 32*(2), 185–194. 32.2_Tikk_Article07-header-deleted.pdf (temple.edu)

Trautman, L. J. (2016). Is cyberattack the next Pearl Harbor. *North Carolina Journal of*

Law & Technology, 18(2), 233–289. Is Cyberattack the Next Pearl Harbor? (unc.edu)

Troelsen, J. (2007, March 4). *Idaho National Laboratory—Operation Aurora* [Video file]. https://www.youtube.com/watch?v=bAWU5aMyAAo

Tullos, K. E. (2012). From cyber attacks to social media revolutions: Adapting legal frameworks to the challenges and opportunities of new technology. *Emory International Law Review, 26*(2), 733–744. From Cyber Attacks to Social Media Revolutions: Adapting Legal Frameworks to the Challenges and Opportunities of New Technology (emory.edu)

United Nations. (1972). *Convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction.* https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.37_conv%20biological%20weapons.pdf

United Nations. (1981). *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, UNGA A/RES/36/103, December 9, 1981.* http://www.un-documents.net/a36r103.htm

United Nations. (2001). *Draft articles on responsibility of states for internationally wrongful acts.* http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

United Nations. (2004). *Convention on Jurisdictional Immunities of States and their Property.* https://treaties.un.org/doc/source/RecentTexts/English_3_13.pdf

United Nations. (2011). *International code of conduct for information security UNGA*

Doc A/66/359. United Nations General Assembly. http://cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf

United Nations. (2013). *Group of governmental experts on developments in the field of information and telecommunications in the context of international security A/68/156.* http://undocs.org/A/68/156

United Nations. (2015a). *Group of governmental experts on developments in the field of information and telecommunications in the context of international security A/70/174.* (2015). https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

United Nations. (2015b). *International code of conduct for information security UNGA Doc A/69/723.* (2015). United Nations General Assembly. http://undocs.org/A/69/723

United Nations. (1970). *Declaration on principles of international law concerning friendly relations and co-operation among states in accordance with the charter of the United Nations, UNGA A/RES/25/2625, October 24, 1970.* http://www.un-documents.net/a25r2625.htm

United Nations. (2018). *Resolution on advancing responsible state behavior in cyberspace in the context of international security, A/RES/73/266, December 22, 2018.* https://undocs.org/en/A/RES/73/266

United Nations. (2019). *Resolution on advancing responsible state behavior in cyberspace in the context of international security, A/RES/74/28, December 12,* *2019*. https://undocs.org/en/A/RES/74/28

U.S. Department of Defense. (2011). *Department of defense cyberspace policy report: A report to congress pursuant to the national defense authorization act for fiscal year 2011, section 934*. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf

U.S. Department of State. (2016). *International cybersecurity strategy: Deterring foreign threats and building global cyber norms* (testimony of Christopher Painter before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy). https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm

U.S. Supreme Court. (1900). *The Paquete Habana, 175 U.S. 677* (1900). https://supreme.justia.com/cases/federal/us/175/677/case.html

U.S. v. Morenets, Serebriakov, Yermakov, Malyshev, Badin, Sotnikov, Minin, No. 18-263 (W.D. Pa. filed October 3, 2018). https://www.justice.gov/opa/page/file/1098481/download

U.S. v. Netyksho, Antonov, Badin, Yermakov, Lukashev, Morgachev, Kozachk, Yershov, Malyshev, Osadchuk, Potemkin, Kovalev (2018). No. 18-215 (D. D.C. filed July 13, 2018). https://www.justice.gov/file/1080281/download

U.S. v. Wang Dong, Sun Kailiang, Wen Zinyu, Huang Zhenyu, Gu Chunhui. (2014) No. 14-118 (W.D. Pa. filed May 1, 2014). https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf

U.*S. v. Zhu Hua and Zang Shilong* (2018). No. 18-891 (S.D. Ny. filed January 17, 2018).

https://www.justice.gov/opa/press-release/file/1121706/download

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Oxford University Press.

van Creveld, M. (2000). Through a glass, darkly: Some reflections on the future of war. *Naval War College Review, 53*(4), 25–44. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2644&context=nwc-review

van der Meer, S. (2015). Enhancing international cyber security. *Security and Human Rights, 26*(2–4), 193–205. https://doi.org/10.1163/18750230-02602004

van Dunk, J. (2020). The threat of terrorism to power grids: Effects of electromagnetic pulses to the United States. *Liberty University Journal of Statesmanship & Public Policy*, *1*(1), 7. The Threat of Terrorism to Power Grids: Effects of Electromagnetic Pulses to the United States (liberty.edu)

van Eeten, M. J., & Mueller, M. (2013). Where is the governance in internet governance? *New Media & Society, 15*(5), 720–736. https://doi.org/10.1177/1461444812462850

van Zolingen, S. J., & Klaassen, C. A. (2003). Selection processes in a Delphi study about key qualifications in Senior Secondary Vocational Education. *Technological Forecasting and Social Change, 70*(4), 317–340. https://doi.org/10.1016/S0040-1625(02)00202-0

Vasiu, I., & Vasiu, L. (2017). Malicious cyber activity distribution, attribution, and retribution. In I. Vasiu & F. Streteanu (2017). *Advanced Cyberlaw and Electronic Security* (pp. 9–19). https://ssrn.com/abstract=2966010 von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. *International Law Studies, 89*(1), 123–156. https://www.hsdl.org/?abstract&did=734369

von Heinegg, W. H. V. (2015). *International law and international information security: A response to Krutskikh and Strelsov* (Tallinn Papers, No. 9). NATO Cooperative Cyber Defense Center of Excellence.

Wallach, W. (2015). *A dangerous master: How to keep technology from slipping beyond our control.* Basic Books.

Watkin, K. (2013). The cyber road ahead: Merging lanes and legal challenges. *International Law Studies, 89*(1), 472–511. viewcontent.cgi (usnwc.edu)

Watts, S. (2015). Low-intensity cyber operations and the principle of non-intervention. *Baltic Yearbook of International Law Online, 14*(1), 137–161. https://doi.org/10.1163/22115897-90000125

Waxman, M. (2013). Self-defensive force against cyber attacks: Legal, strategic and political dimensions. *International Law Studies, 89*(1), 109–122. viewcontent.cgi (usnwc.edu)

Waxman, M. C. (2017). *Cyber strategy & policy: International law dimensions* (SSRN Scholarly Paper ID 2926099). Social Science Research Network. https://papers.ssrn.com/abstract=2926099

Waz, J., & Weiser, P. (2012). Internet governance: The role of multistakeholder organizations. *Journal on Telecommunications and High Technology Law, 10,* 331–349. Internet Governance: The Role of Multistakeholder Organizations

(colorado.edu)

Weiler, R. M. (1995). Determining consensus: Applying Kendall’s coefficient of concordance. *Health Values: The Journal of Health Behavior, Education & Promotion, 19*(2), 53–56. Determining consensus: Applying Kendall's coefficient of concordance. - PsycNET (apa.org)

Weiss, M. & Weiss, M. (2019). An assessment of threats to the American power grid. *Energy, Sustainability & Society, 9*(1), 1-9 . https://doi.org/10.1186/s13705-019-0199-y

Westerburger, S. (2014). *Cyber conflict in the 21st century. The future of war and security in a digitalizing world*. [Unpublished master’s thesis] Radboud University.

Westner, M., & Kobus, J. (2016). Ranking-type Delphi studies in IS research: Step-by-step guide and analytical extension. In *IADIS Int. Conf. Inf. Syst* (pp. 28-38) http://www.iadisportal.org/digital-library/ranking-type-delphi-studies-in-is-research-step-by-step-guide-and-analytical-extension

White House. (2011). *International strategy for cyberspace: Prosperity, security, and openness in a networked world.* https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

White House. (2018). *National cyber strategy of the United States*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Williams, P., & Fiddner, D. (Eds.). (2016). *Cyberspace: Malevolent actors, criminal opportunities, and strategic competition.* Department of the Army.

Wirtz, J. J. (2017). The cyber Pearl Harbor. *Intelligence and National Security, 32*(6), 758–767. https://doi.org/10.1080/02684527.2017.1294379

Xinbao, Z. (2017). China's strategy for international cooperation on cyberspace. *Chinese Journal of International Law, 16*(3), 377–386. China's Strategy for International Cooperation on Cyberspace | Chinese Journal of International Law | Oxford Academic (oup.com)

Yetter, R. B. (2015). *Darknets, cybercrime & the onion router: Anonymity & security in cyberspace.* [Unpublished master's thesis] Utica College.

Yin, R. K. (2017). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Yoo, C. S. (2015). *Cyber espionage or cyberwar?: International law, domestic law, and self-protective measures* (University of Pennsylvania Law School Paper No. 15-3). https://papers.ssrn.com/abstract=2596634

Zahariadis, N. (2019). The multiple streams framework: Structure, limitations, prospects. In P. A. Sabatier (Ed.), *Theories of the policy process* (2nd ed., pp. 65-92). Routledge.

Zahariadis, N. (2017). Theories of the policy process. In C. M. Weible & P. A. Sabatier (Eds.), *Theories of the policy process* (4th ed., pp. 65–92). Routledge.

Zahariadis, N. (2003). *Ambiguity and choice in public policy: Political decision making in modern democracies.* Georgetown University Press.

Zahariadis, N. (1996). *Theory, case, and method in comparative politics.* Cengage Learning.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*(1), 13–15. https://doi.org/10.4314/mmj.v27i1.4

Zeng, J. (2016). Constructing a "new type of great power relations": The state of debate in China (1998–2014). *British Journal of Politics and International Relations, 18*(2), 422–442. https://doi.org/10.1177/1369148115620991

Zeng, J., & Breslin, S. (2016). China's 'new type of Great Power relations': A G2 with Chinese characteristics? *International Affairs, 92*(4), 773–794. https://doi.org/10.1111/1468-2346.12656

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty." *Politics & Policy, 45*(3), 432–464. https://doi.org/10.1111/polp.12202

Appendix A: Participant Qualifications

Criteria	Panel Average
Doctoral Level Education	83%
Years of Professional Experience[1]	9
Professional Credentials[2]	1.7
Scholarly Writing[3]	11
Institutional Service[4]	100%
Other Qualifications[5]	100%

[1] Professional Experience - the average number of years substantially involved in international cybersecurity matters.

[2] Professional Credentials – the average number of professional licenses, certifications, or specializations relating to international cybersecurity matters.

[3] Scholarly Writing – the average number of published scholarly works regarding to international cybersecurity norms.

[4] Institutional Service – the percentage of participants with significant institutional service concerning international cybersecurity norms.

[5] Other Qualifications – the percentage of participants with recognition of significant expertise in international cybersecurity norms (e.g., honors, awards, grants).

Appendix B: Issue Definitions

Issue	Definition
Problem Nature	Democratic States (DS) consider cyberconflict a technology problem caused by incredibly complex networks of information systems that cannot be adequately secured. Authoritarian States (AS) consider it a sociopolitical problem caused by subversive information that foments civil unrest and incites revolution.
Threat Perception	DS perceive the salient cyberconflict threat as a catastrophic cyber-attack on critical national infrastructure. AS perceive their primary threat as subversive information that foments civil unrest and incites revolution.
Problem Character	DS desire limited norms to regulate cyber-attacks that produce effects analogous to conventional armed attacks. AS seek broadly applicable international cybersecurity norms that increase State control over subversive information.
Norm Selection	DS policy solutions are limited to a narrow type of destructive cyber-attack they classify as an armed attack. As a result, they advocate for norms that apply the law of armed conflict to the most dangerous type of State conduct in cyberspace. This solution mitigates the primary threat to DS without jeopardizing fundamental human rights (e.g., privacy, free speech). AS classify cyberconflict more broadly as wrongful State conduct and they advocate for norms that apply the international laws of nonintervention, sovereignty, and countermeasures to cyberconflict. AS feel this approach offers less dangerous remedies for cyber-attacks that are difficult to classify and regulates a broader spectrum of hostile conduct.
Attribution	DS seek robust international law enforcement cooperation to collect the evidence necessary to attribute cyber-attacks to responsible States and enforce norms. AS desire limited international law enforcement cooperation that safeguards their sovereign rights.
Urgency	AS enjoy the advantage of time because the primary security threat posed by cyberconflict is less urgent than that of DS. A catastrophic cyber-attack on critical national infrastructure would be invisible with near instantaneous effects. In contrast, a subversion campaign to incite

	revolution would be visible with effects that manifest over time. Thus, the primary threat to DS is more acute, and their need for international cybersecurity norms is more urgent, than that of AS.
Significance	Intellectual property obtained via cyberespionage has fueled rapid economic growth in some AS. Therefore, unregulated cyberconflict provides AS an enormous economic advantage. In contrast, the corresponding economic loss to DS is nearing a trillion dollars annually.
Asymmetry	Unregulated cyberconflict provides AS an asymmetric means to counter the economic and military advantages of DS. Cyberconflict is a low cost and low risk means to create effects far exceeding what could be produced with the conventional capabilities of AS. Therefore, DS need international cybersecurity norms to maintain their economic and military advantages.
Cyberpower	DS maintain a dominant position in cyberspace through indirect control of non-governmental organizations that regulate critical internet functions. This enables DS to control norms that serve their interests. In contrast, AS require a redistribution of cyberpower to create new norms that further their national security interests (i.e., increased surveillance and information control).

Issue	Definition
Problem Nature	Democratic States (DS) consider cyberconflict: a technology problem caused by incredibly complex networks of information systems that **by design lacks security; and an international law problem caused by disagreement over and lack of compliance with pre-existing international law norms.** Authoritarian States (AS) consider it: a sociopolitical problem caused by subversive information that foments civil unrest and incites revolution; **and a structural problem caused by DS control of most international cyber mechanisms.**
Threat Perception	No change.

Problem Character No change.

Norm Selection DS policy solutions **focus heavily on a** narrow type of destructive cyber-attack they classify as an armed attack. As a result, they **emphasize advocacy** for norms that apply the law of armed conflict to the most dangerous type of State conduct in cyberspace. This solution mitigates the primary threat to DS without jeopardizing fundamental human rights (e.g., privacy, free speech). AS classify cyberconflict more broadly as wrongful State conduct and they **emphasize advocacy** for norms that apply the international laws of nonintervention, sovereignty, and countermeasures to cyberconflict. AS feel this approach offers less dangerous remedies for cyber-attacks that are difficult to classify and regulates a broader spectrum of hostile conduct.

Attribution DS seek robust international law enforcement cooperation to collect the evidence necessary to attribute cyber-attacks to responsible States and enforce norms. AS desire limited international law enforcement cooperation that safeguards their **control and autonomy with respect to cyber actions.**

Urgency The issue was removed from the list.

Significance Intellectual property obtained via cyberespionage has fueled rapid economic growth in some AS. **Such intellectual property theft provides AS discount imports through which the victim entity generally cannot seek retribution.** Therefore, unregulated cyberconflict provides AS an enormous economic advantage. In contrast, the corresponding economic loss to DS is nearing a trillion dollars annually.

Asymmetry Unregulated cyberconflict provides AS an asymmetric means to counter the economic and military advantages of DS. Cyberconflict is a low cost and low risk means to create effects far exceeding what could be produced with the conventional capabilities of AS. Therefore, DS need international cybersecurity norms to maintain their economic and military advantages. **In the interim, DS require greater defensive/offensive deterrent capabilities.**

International Cyberpower	DS maintain a dominant position in cyberspace **through heavy influence over sympathetic** non-governmental organizations that regulate critical internet functions. This enables DS to control **international** norms that serve their interests. In contrast, AS require a redistribution of **international** cyberpower to create new norms that further their national security interests (i.e., increased surveillance and information control).
Workforce	**AS enjoy a faster and more consistent ability to proportionally increase its work force with cybersecurity and offensive cyber capabilities given the style of government and greater control over the educational systems at all levels. DS cannot replicate or increase such a workforce at the same speed. Instead, DS must rely on incentive-based efforts to increase the technology proficient workforce.**