Defending Democracy:
The Road to Cyber Global Governance in Safeguarding Elections

Kiana Harkema
International Affairs Program
College of Arts and Sciences
University of Colorado, Boulder

Defended March 31, 2021

Honors Thesis Defense Committee

Dr. B. Clara Park, *Primary Advisor*
Department of Political Science

Dr. Douglas Snyder, *Honors Council Representative*
International Affairs Program

Dr. Nolen Scaife, *Thesis Committee Member*
Department of Computer Science
Technology, Cybersecurity, and Policy Program

Abstract

Since Russian interference into the 2016 United States Presidential Election, the need for stronger safeguards against cyberattacks upon elections has never been more apparent. Cyberattacks transcend national borders and require international cooperation if effective deterrence measures are to be established - this means establishing acceptable and unacceptable behavior in cyberspace. While progress had been made in this endeavor, it is unclear whether nations are successful in translating the normative values they hold domestically to an international framework. My research investigates the cybersecurity practices the United States exercises, in safeguarding its election infrastructure, to understand what norms the United States internalizes and how influential those norms have been internationally. The United States has been a vocal actor in the norms formulation process, as well as one that has participated in a variety of ways thus making it an informative case study. By analyzing the extent to which the United States is successful in promoting its domestic normative values on the international stage, it may be possible to not only better understand the process of cyber norms development, but also understand where the future of cyber global governance is headed.

Acknowledgements

Thank you to the members of my committee for offering your expertise in support of my research. Thank you, Dr. Park, for helping guide my research topic from the very beginning and challenging me to think deeply about the intersection of technology and governance. Dr. Snyder, thank you for helping me articulate my ideas in a way that improved my abilities as a researcher immeasurably. All the while, your enthusiasm for my research was greatly appreciated. In spite of my unorthodox interests as a computer science student, thank you, Dr. Scaife, for being so accommodating and encouraging my interests in your class, research group, and beyond. And finally, thank you Mr. Russell for encouraging me to join your cybersecurity club when I was a freshman in high school and being a relentless advocate for me ever since. I owe my passion for cybersecurity to your continuous support - including that which you have offered in direct support of this research.

TABLE OF CONTENTS

Introduction

In 2017, the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* was published. It was a step forward in understanding how international law is applicable in an era of cyberwarfare and was lauded as being vital toward a more secure, predictable global society. By offering interpretations of how traditional international laws and norms such as sovereignty, jurisdiction, and the legal responsibility of states applied when conducting and responding to cyber operations, it appeared progress was made toward establishing deterrents to such malicious cyber activities. Of these malicious activities, digital interference and influence into a state's elections is one of particular importance and one whose progress is inexorably tied to the development of international norms in cyberspace, and not just those related to international law.

The United States' methods of election protection were forever altered by Russian interference and influence in the 2016 Presidential Elections. Discovery of activities like Russian social media accounts spreading misinformation and disinformation and the breaching of voter registration databases shook voter confidence to the core. Unfortunately, the Unites States is only one of many countries who have suffered at the hands of such cyber operations. Questions formulated regarding the best way to deter states and other actors from participating in activities that degrade the fundamental core of democracy: free and fair elections. While publications like the *Tallinn Manual* seek to address these questions, the purpose of my research is to understand the road to global governance through the lens of a nations' cybersecurity practices and its corresponding normative values.

The road to global cyber governance in safeguarding elections is paved by international organizations that are seeking to establish norms. Like the *Tallinn Manual*,

these norms are proposals for how international law should play a role in establishing conduct in cyberspace, as well as other guidelines for behavior. My research seeks to understand how effectively the United States has been in incorporating its domestic norms into an international normative framework. I argue cybersecurity practices reveal what norms the United States value and that those same norms are persistent in international bodies concerned with the creation of cyber norms, however, norms valued by the United States are not equally represented internationally. Rather, while some norms promoted by the United States are foundational pieces of cyber norms, other norms are not as observable and face obstacles to achieving legitimacy.

Chapter 1 frames the research problem and examines its relevance in establishing a mechanism of cyber global governance. In Chapter 2, I use textual analysis of key standardization documents, Congressional hearings, and other relevant statements to understand what norms the United States values in its election-oriented cybersecurity practices. The method of textual analysis is further explained below. This analysis revealed that there are three unique facets of American society that have engendered norms surrounding electoral protection: (1) election infrastructure is designated as critical infrastructure; (2) the use of electronic voting machines; and (3) private-public partnerships necessitated by disinformation campaigns meant to undermine elections. Consequently, the domestic norms arising out of these practices have been projected into international cyber norms thus demonstrating the United States' ability to have those norms legitimized. I then use Chapter 3 to analyze the United States' participation in relevant international bodies and determines the extent to which these norms found in Chapter 2 are present. I begin by developing an understanding of one of the first and most formative international cyber norm-formulation bodies: the United Nations Group of

Governmental Experts (UN GGE). The United States' extensive participation in the UN GGE since 2005 warrants a closer look at how UN GGE norms have developed since that time and culminated in the foundational 2015 UN GGE Report. I find that the United States was able to successfully project its norms within the UN GGE as it relates to its focus on protecting critical infrastructure, including election infrastructure. Furthermore, the United States' preference for voluntary standardization is observable internationally in the United States' desire to see international law upheld in cyberspace through the UN GGE. A strong desire for voluntary standardization is also especially pertinent when examining the practices surrounding critical infrastructure protection and the decentralized nature of electronic voting machine accreditation. While the translation of domestic critical infrastructure norms to international cyber norms is fairly apparent, I find that the United States has encountered obstacles in legitimizing some of its other norms within international bodies, such as a focus on Internet freedom and the applicability of certain aspects of international law.

This work analyzes the United States' cybersecurity practices surrounding election protection and identifies the normative values that are observable from such practices. The theory of organizational isomorphism suggests that entities, like cybersecurity organizations charged with the protection of electoral integrity and voting security, are subject to isomorphism because of the norms that are persistent in the industry (DiMaggio and Powell 1983; Jeyaraj and Zadeh 2020). The isomorphic nature of the cybersecurity industry means that certain terms, as discovered by Jeyaraj and Zadeh, are common nomenclature. Although these terms may be prolific across different cybersecurity organizations and nations, understanding the context of their usage is key. Per the Key-Word-in-Context (KWIC) theoretical framework, sentiment and themes can

be gleaned from work by not only understanding what keywords are used, but how they are used (Ghasiya and Okamura 2020; Ryan and Bernard n.d.). For example, American and Taiwanese cybersecurity organizations may both have a tendency to incorporate the term "critical infrastructure" in their election security standards and policies. Yet, embedded within American culture is the tendency to classify election infrastructure as critical infrastructure, while this is not the case in Taiwan. By utilizing the "keywords" derived by Jeyaraj and Zadeh and combining it with the KWIC framework, it elucidates the norms the United States values in its cybersecurity protection. Protection efforts can range from an emphasis on post-election audits that verify the success of cybersecurity measures, to persistent efforts in combatting misinformation and disinformation through private-public partnerships. Whatever these practices may be, they are indicative of what values a state holds regarding the assurance of election integrity and voting security.

The normative values extrapolated from both cybersecurity practices will be compared to those normative values that are evident in four major bodies seeking to establish global cyber norms: The United Nations Group of Government Experts (UN GGE), the United Nations Open-Ended Working Group (UN OEWG), the Global Commission on the Stability of Cyberspace, and the Paris Call for Trust and Security in Cyberspace. The way in which the United States participates in these bodies and expresses its norms will be used to evaluate whether the norms captured from the cybersecurity practices correlate with those norms valued by the GGE, UN OEWG, the Global Commission, and the Paris Call. Electoral protection was and will continue to be an important issue emphasized in these norm-setting bodies, making it a particular issue of interest as its prominence is studied throughout the historical development of cyber norms.

The UN OEWG, the Global Commission, and the Paris Call are three entities that embody the United States' struggle to solidify its norms. Nonetheless, understanding this struggle is imperative in further clarifying the domestic norms the United States hopes to solidify, as well as understanding the effectiveness of the United States' efforts to legitimize its norms. The UN OEWG was created out of Russia's discontent with the 2017 UN GGE sessions and embodies the United States' struggle to have its normative values reign supreme over Russia, including those norms that strive to uphold the international law of State responsibility and international humanitarian law, specifically the principle of Internet freedom. Additionally, the Global Commission and the Paris Call are two bodies in which the United States' private sector has chosen to articulate its norms thus adding another layer to what I characterize as the set of the United States' domestic norms. Most importantly, the private-public partnership is plagued by a disagreement over how to protect electoral integrity from disinformation campaigns.

The road to cyber global governance has an uncertain future, however, by focusing on the United States' process in establishing its domestic norms on the international stage, it is possible to develop a better understanding of what that future may look like. As this work will reveal, that future will inevitably bring the debate over electoral protection to the forefront of the cyber governance process. Studying the efforts to protect elections from cyber threats provides valuable insight into the development of international cyber norms and its assurance is key in the defense of democracy. Chapter 1 begins by providing context surrounding the process of creating global cyber norms, including its relationship with existent literature, and the methodology utilized in studying this process from a domestic and international standpoint.

CHAPTER 1: Framing the Research Problem

My research necessitates an understanding of current cyber threats posed to elections and the international bodies that are seeking to establish cyber norms. The American cybersecurity practices surrounding electoral protection are responses to the current threats that stem from Russian interference into the 2016 United States Presidential Election. Therefore, understanding the general threats that exist to elections will help in understanding how Russian activity exacerbated such threats and thus largely influenced the United States' responses and normative values. Chapter 2 examines the nature of these responses and norms on a domestic level. Furthermore, the United States has unique institutional tools in combatting cyber threats to elections and requires an understanding of such institutions. The institutions not only characterize American cybersecurity practices but demonstrate the severity with which certain cyber incidents are treated with. Uniquely, the United States has a tendency to utilize militaristic institutional tools in combatting cyber threats, specifically those that can affect elections. Chapter 3 then seeks to understand how successful the United States is in projecting its norms on an international level, both intentionally and not. For example, while critical infrastructure protection is certainly a norm that the United States explicitly wanted represented in the UN GGE, the fractured nature of private-public partnerships in the United States is one that unintentionally affects the United States' ability to engage internationally in formulating cyber norms. Due to the nature of Chapter 3, it is also necessary to understand how nations traditionally engage with international law and norms.

Section 1.1: Background

Subsection 1.1.a) Threats to the Electoral Process

The sanctity of the electoral process is dependent upon the assurance of two elements: election integrity and voting security. Election integrity is generally defined as being a culmination of a nation's politics, society, and economy that all contribute toward free and fair elections. Voting security is the protection of election infrastructure, with election infrastructure being defined as pieces of critical infrastructure that are used to maintain voter registration databases, manage election results, and assist in the process of voting (Henschke, Sussex, and O'Connor 2020).

In order to understand voting security, it is first necessary to understand election infrastructure and its variances. Typically, election infrastructure consists of electronic systems for voter registration and the actual act of casting votes, if electronic voting machines are in use. This involves the usage of hardware and software that may be exposed to the Internet and thus serves as a potential attack vector. Particular vulnerability results from the fact that voter registration and information related to vote casting is not stored in a central location and can rather be decentralized based upon the location in question. While these two components are the most alluring target for threat actors, other components such as poll books, vote tabulation systems, election night reporting systems, and auditing systems are additional components in the election ecosystem that may be vulnerable to cyberattacks. Corruption that undermines voting security can clearly be accomplished by, not just changing votes, but also by exposing and exfiltrating vital election information that is capable of degrading trust in the democratic system. Whether it be by targeting voter registration information or election night reporting applications, there are several points of failure in the electronic election ecosystem (McFaul 2019; Reichenbach 2020). Although voting security and election integrity are defined relatively coherently throughout literature, there is notable

divergence in regard to what constitutes an attack on one or the other, and the severity associated with such.

In some cases, foreign influence upon elections is regarded as being attempts by a foreign entity to influence voters on a massive scale, rather than participating in discrete targeting of political officials or infrastructure. Foreign interference stands in contrast as it targets voting security (i.e. the underlying election infrastructure) (Henschke, Sussex, and O'Connor 2020; DOD Has Enduring Role in Election Defense n.d.; Hsaio et al. n.d.). Broadly, foreign interference may fall under election fraud, defined, as a criminal concept, as being the cause of substantive irregularity as it relates to the act of voting, including the cyber corruption of election results (Alvarez, Hall, and Hyde 2008). In other cases, foreign interference is recognized as a category of influence rather than a separate entity. Influence is defined as any attempt to undermine democratic institutions, whether that be from misinformation campaigns or the hacking of election infrastructure. This stems from a belief that attacks upon voting security, in the form of foreign interference serves a dual purpose, of not only disrupting election infrastructure, but also sowing distrust in an election system and thus undermining the democratic institutions in the way a mass misinformation campaign would (Chertoff and Rasmussen 2019; Dutta et al. 2020; Waldemarsson 2020).

The distinction between foreign interference and influence is telling in that their definitions are ambiguous; nations use the terminology "interference" and "influence" in unique ways. For example, the United States will often characterize a cyber incident as "interference" when it wishes to demonstrate the severity of the action, and thus justify an equally severe response that reflect the consequences of violating international law. On the other hand, "influence" is a term the United States utilizes when it wants to

simultaneously demonstrate the seriousness of a cyber incident that, however, falls short of violating international laws or norms. This kind of flexibility is pertinent in the United States' preference for international laws' applicability in cyberspace, as further discussed in Chapter 3.

Subsection 1.1.b) State of International Law and Cyber Norms

The international discourse on governance in cyberspace has largely grappled with questions concerning the applicability of international law in this area, as well as what norms should be established regarding how the international law is applicable in cyberspace. Because of the lack of guidance States currently receive, from the international community on how to characterize cyber-attacks upon their electoral process, they are consequently unable to determine an internationally acceptable course of action that adheres to international law. For example, the act of undermining election integrity and/or voting security has not been universally agreed upon as a violation of sovereignty (Fidler 2016; Ohlin 2017). The relatively recent emergence of cyber activities has meant that the proliferation of norms has been met with varying reactions, ranging from optimism with progress made, to frustration with a lack of unity regarding these issues. Several international organizations have risen to prominence for their role in shaping cyber norms and positioning them within an existing framework of international law. The United Nations' current framework of cyber governance is based upon the work produced by Governmental Groups of Experts (GGE). The GGE began grappling with the role of information and communications technologies (ICTs) within the international community in 2004. The GGE started with representatives from fifteen states and grew to twenty-five representatives by 2017. Six working groups have been formed since then and produced varying degrees of substance in its outcomes. Between 2004 and 2009,

progress did not produce norms, but rather constructive progress that eventually led to the 2013 working group, which GGE participants recognized as being the most successful working groups up to that point. In 2013, members agreed international law was applicable in cyberspace and started to enact confidence building measures. By 2015, the GGE produced a report recognizing eleven voluntary norms in cyberspace, grounded in existing international law and norms (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015). The set of norms produced in 2015 provide the most concrete progress in both establishing the sets of international law that are of concern in cyberspace, as well as the importance of protecting critical infrastructure. These norms are provided in Appendix A.

Despite progress made during the 2015 working group, in 2017, the GGE was unable to produce a report. Contention, predominately from Russia, surrounding the applicability of international humanitarian law, right of self-defense in the event of a cyberattack, and whether states could invoke the law of countermeasures[1] in responding to cyberattacks impeded progress (Henriksen 2019). However, the UN General Assembly established a new path forward in establishing another GGE Resolution. Per this resolution, another GGE was established in 2019 and mandated to submit a final report in 2021 (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015). Despite the setback, the GGE established a 2019-2021 working group along with the UN Open-Ended Working Group (OEWG).

[1] In being subjected to the wrongful act of another State, an "injured" state may engage in a unilateral method, that may threaten the legal order, but may be used as a method of redress in the wrongdoing.

While the GGE is limited to 25 members, as of 2019, the UN OEWG is an open forum for all UN members to participate. Following the failure of the GGE to produce a report in 2017, the Russian Federation led the effort to create a new entity responsible for developing the rules, norms, and principles States should abide by in cyberspace. The OEWG began meeting in 2019 and with its most recent meetings beginning in July 2020 and set to conclude in March 2021. A pre-draft of 2020 OEWG report reiterates the role of international law and norms established by the GGE: states have an obligation to abide by international law and the norms produced by the GGE are meant to provide guidance specific to governance in cyberspace in forms of confidence-building measures (Report of OEWG Developments on in the Field of Information and Telecommunications in the Context of International Security 2020). While the GGE and OEWG seemingly work in conjunction in one another to build upon existing international law, it is important to note the OEWG is the direct product of Russia's effort to replace a United States-led call for an additional GGE meeting. The OEWG and GGE are still young entities and thus there is potential for the two to diverge more significantly in ideals in the future.

The Global Commission on the Stability of Cyberspace provides an additional framework for developing norms and, rather than nations, is comprised of individual commissioners brought together by two think tanks: the Hague Center for Strategic Studies and EastWest Institute. Building upon work produced by the GGE, the 2019 Advancing Cyberstability Report called for four guiding principles, development of norms, adherence to international law, confidence building measures, capacity building, and widespread adoption of specific technical standards (Advancing Cyberstability 2019).

The Paris Call for Trust and Security in Cyberspace also advocates for the development of norms heavily influenced by the GGE and OWEG rather than introducing

its own norms. It is notable for its broad base of support that includes 1,000 signatories representing States, companies, and civil society organizations. Additionally, the Paris Call Community on Countering Election Interference was created to expand upon one of the original Paris Call norms that called for the identification and building of the capacity needed to combat foreign interference in the election process (The Paris Call of the 12 November 2019 — Paris Call 2019).

The GGE, the OEWG, the Global Commission, and the Paris Call highlight some of the most influential entities in the development for norms of behavior in the cyberspace. Notably, they draw significant inspiration from the original norms established by the GGE. However, they differ in their participants, signatories, and overall ideals that are shaping the discourse on how the global community should interact with international law and norms when dealing in cyberspace. The purpose of this work is to understand how domestic institutions meant to protect electoral processes shape that discourse and how it aligns, or does not align, with the ideals presented by these international frameworks. Specifically, I conduct an analysis of the intuitions that comprise the United States election ecosystem.

Subsection 1.1.c) The United States' Institutional Methods of Protecting Elections

At the core of the United States' election protection process is the Department of Defense (DOD) and intelligence community at large. The Election Security Group is a collation of governmental agencies including National Security Agency (NSA) and United States Cyber Command (CYBERCOM) who also work closely with the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS). The group was established in the wake of the 2018 US Midterm Elections and has a primary objective of generating insights on foreign adversaries in order to improve defenses and inflict

punishment upon those who choose to interfere (DOD Has Enduring Role in Election Defense n.d.). In order to understand how United States institutions, such as the Election Security Group, understand cyberattacks upon the electoral process, it is important to note the complex relationships with international law and norms in a cyberspace originating with the Obama administration.

During the Obama administration, three instruments of cyber deterrence were attempted: deterrence by denial, deterrence by norms, and deterrence by punishment. Deterrence by denial functions by denying adversaries benefits sought from cyber operations while deterrence by norms seeks to shape norms against engaging in cyber operations that harm the electoral process. Research has indicated a frustration with the ineffectiveness of international law in deterring cyberattacks pushed the Obama administration to pursue deterrence by punishment (Fidler 2016; Segal n.d.). Despite being a driving force behind several conferences and treaties meant to negotiate international law and norms, the United States has moved away from being tied to these ideas in pursuit of a deterrence by punishment strategy. As noted by scholars, the Obama administration took care in distinguishing between international law and norms, emphasizing that a statement released by the President Obama characterized the Russian hacks upon the 2016 United States Presidential Election as being a violation of norms, not international law. (Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment 2016). Yet, there is disagreement on whether norms were actively established by the administration and whether the assertion of norm violation is warranted. Consequently, it signaled an increasing shift away from an attempt to shape international law and norms that continues with the Trump administration. The institutions charged with election protection, contained within the Election Security

Group, embody this ideal. The Election Security Group has stated a dedication to working with private partners to further protection of the electoral process that, as discussed below, has yet to come to fruition.

In addition to the federal agencies listed about, the Election Assistance Commission (EAC) is another important agency that is charged with safeguarding the electoral process. The EAC was established in 2002 to act as a bipartisan, independent commission charged with helping American votes. The EAC's efforts serve two purposes: to assist election officials and voters. To assist election officials, the EAC publishes voting system guidelines, accredits electronic voting systems, and acts a clearinghouse for best practices regarding the security of election infrastructure. In assisting voters, the EAC coordinates mail-in voter registration forms and provides up-to-date information on the best practices to vote privately and securely. The long-established nature of the EAC along with its provision of trusted cybersecurity guidelines made it valuable resources in this research. By analyzing the standards provided by the EAC, it helped to elucidate the themes that arise out of United States domestic cybersecurity practices.

In 2018, the United States established the Cybersecurity and Infrastructure Agency (CISA) under DHS to combat foreign influence and interference, including misinformation and disinformation campaigns and attacks on physical infrastructure. Similarly to the EAC, CISA was established to provide local jurisdictions with the resources necessary to safeguard their election infrastructure and provide accurate information regarding election procedures to the general public. CISA provides cybersecurity assessments, detection and prevention technology, information sharing capabilities, and training. The election infrastructure CISA is charged with protecting is decentralized. States and other local jurisdictions have sole control over key aspects of the

electoral process. Voter registration databases are centralized at the state level while vote-casting systems are managed at the county-level. While counties have the option to use electronic machines for tabulation and the voting process, this is not a universal feature (McFaul 2019). CISA in conjunction with the EAC also provided insight into the themes arising out of United States domestic cybersecurity practices, including a focus on protecting critical infrastructure and a preference for decentralization.

Section 1.2: Theoretical Framework and Literature Review

Subsection 1.2.a) Domestic Engagement with International Law and Cyber Norms

This work seeks to understand how the domestic norms surrounding electoral protection influence the United States' interaction with international law and norms in cyberspace and how pervasive these domestic norms are within an international context. This relies upon the assumption that States have an interest in complying with international law - a sentiment that is largely shared by scholars, yet faces challenge in how this process specifically manifest (Koh et al. 1997). Therefore, it is important to understand why and how nations, such as the United States, engage with international law and norms. It is also important to note that international law and norms work in a unique way in cyberspace. Although international law exists, there are few international laws that specifically govern activity in cyberspace. Consequently, nations develop norms concerning when and how international law is applicable in cyber space; these norms are often the points of contention in establishing a framework for cyber global governance. Nonetheless, it is necessary to understand the process of international law engagement.

Several theories regarding why States choose to engage with international law, and consequently seemingly internalize certain norms, have been offered. International law and norm creation can be thought as an iterative process in which State choose to engage

in continuous discourse thus involving them in regimes in which there is pressure to comply (Chayes and Chayes 1995; Koh et al. 1997). Historically, this has been interpreted as a "procedural" argument as to why nations choose to engage with international in a way that signals obedience. Other scholars have argued for a more "philosophical" approach as to why States choose to obey international law and norms by attributing a moral compass to States when making their decisions (Finnemore and Hollis 2020; Franck 1998; Posner 2003).

While this is useful for understanding long-standing international agreements within some subject areas, international law and norms as they relate to cyberspace, specifically protection of election integrity and voting security, can trace its most arguable, significant influence to as recently as the 2015 establishment of GGE norms - from which many subsequent agreements and norm building procedures have built their work upon. The question becomes how to ascertain a State's commitment to international law and norms when the "procedural" and "philosophical" creation has only begun.

Many have turned to domestic institutions as producers of indicators in the form of rhetoric in the wake of cyberattacks. "Naming and shaming" has been a popular method stemming from domestic institutions in the wake of foreign attacks on the electoral process, including within the United States. However, there has been a noticeable lack of invocation of international law and norms when nations have elected to do so. For example, the 2016 hacking of electoral infrastructure during the United States Presidential Election was, as previously noted, did not invoke any mention of international law's violation (Finnemore and Hollis 2020; Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment 2016). Rather than relying upon international law to dissuade malicious actors, States elect to use a

unilateral tool - a direct accusation in which the State responsible for an attack is named. This seemingly remains ineffective as cyberattacks only continue to rise indicating a weakness in the "shaming" aspect. Despite the lack of invocation of international law, States, including the United States, still participate in entities meant to shape cyber norms. "Naming and shaming" can thus be used as a method of evaluating the norms held by domestic organizations and comparing it to the norms produced by international entities they participate in.

The Key-Word-in-Context (KWIC) theoretical framework is another mechanism for analyzing domestic cyber norms and is used in this research. KWIC is used based upon the assumption that keywords are powerful tools in understanding the themes emerging out of text. In addition to identifying these keywords, the KWIC framework insists that equally important is the context in which these keywords are used (Ghasiya and Okamura 2020; Ryan and Bernard n.d.). Keywords are defined in this research as being the most important terms cybersecurity organization use and is derived from the theory of isomorphism. DiMaggio and Powell developed the idea of organizational isomorphism, which is the philosophy that over time organizations are susceptible to becoming similar to one another as a set of organization arises as a field rather than disparate cooperation. This is borne out of rationalization and bureaucratization (DiMaggio and Powell 1983). Cybersecurity organizations are no different. Jeyaraj and Zadeh proposed that not only are cybersecurity organization subject to the same isomorphic pressures, but that this isomorphic posture can be represented by the most frequently used keywords within standardization and other technical documents (Jeyaraj and Zadeh 2020). My research develops upon this idea by analyzing the frequency of keywords, discovered by Jeyaraj and Zadeh, within standardization documents regarding the cybersecurity of election

infrastructure. Next, I invoke the KWIC theorical framework to not only identify the most frequently used keywords, but how they are specifically being used and what norms are being revealed.

Subsection 1.2.b) Private-Public Partnerships in Safeguarding Elections

In the United States, private-public partnerships are most evident in efforts to combat misinformation that seek to undermine electoral integrity. Understanding the pre-existing obstacles to achieving successful private-public partnerships is imperative in understanding the unique challenges the United States faces that ultimately culminates in a fractured multi-stakeholder framework, evident both domestically and internationally. At the heart of the partnership is information sharing. Private entities often hold specialized knowledge of ICT. For example, according to the Federal Emergency Management Agency, 85% of critical infrastructure is privately-owned. This results in a "market-driven" approach in which the private sector is expected to provide information that is pertinent to national security, while existing in a commercial ecosystem where that kind of information sharing may not be viable for a business. This results in a partnership in which the two entities are motivated by different goals and raises questions regarding the efficacy of such a relationship - one that is held together by a weak notion of "loyalty" to one another (Carr 2016; Christensen and Petersen 2017).

Despite the more pessimistic view regarding private-public partnerships, the private sector still has had a role in shaping cyber norms as they relate to election integrity and voting security. Microsoft became an industry leader in private sector-led norm creation with their involvement in the Paris Call. In 2019, the Alliance for Securing Democracy and Microsoft established the Paris Call Community on Countering Election Interference: a multi-stakeholder organization dedicated to building capabilities within

Principle 1 of the Paris Call: defense of the electoral process. This initiative strives to advance thinking on topics such as what constitutes foreign interference, understanding of the tools used in cyberattacks upon the electoral process, and developing best practices in the case of an attack (Frank 2019a; Maurer et al. 2020; The Paris Call of the 12 November 2019 — Paris Call 2019). The private sector has, therefore, not only been increasing their engagement with policy and prevention measures in reaction to cyberattacks upon the electoral process, but actually leading the charge on electoral protection. Representatives from the private sector continue to offer a voice within organizations like the Paris Call and the Alliance for Security Democracy (including Transatlantic Commission on Election Integrity).

Returning to the "marketized" view of private-public partnerships, the market ecosystem has pushed the private sector to provide technological capabilities that support free and fair elections in the absence of government sponsored solutions. One of the most pressing issues is the private sector's newfound role in providing a platform for information: one voters rely upon when deciding who and what to vote for on Election Day. As social media becomes a breeding ground for misinformation and disinformation, there has been concern how private entities are assuring that misleading information does not become a driving force behind the decisions voters inevitably make.[2]

The private-public partnership model has been underscored by governmental pressure upon the private sector to consider national security, including as it relates to electoral protection. States' governments have brought issue with the ways in which social media platforms decide to label and/or remove content regarding the election; politicians

[2] For further information on the ways in which private organizations have taken steps to address misinformation on their platforms, see Appendix O.

will suggest the presence of an algorithmic bias against a particular party when suggesting content to users or simply question whether the private sector is doing enough to stop the spread of misinformation and disinformation. In defense, some social media corporations will insist they are not the arbiter of truth, which is a favored defense by Facebook CEO Mark Zuckerberg. However, other states, such as Russia, have been the subject of scrutiny for seemingly curbing free speech and using electoral protection as justification. In addition to tensions of this kind, the private-public relationship has been continuously tainted by a series of scandals regarding the abuse of data and questionable breaches of user privacy. (Business et al. 2018; Chertoff and Rasmussen 2019; Feldstein 2020; Government Responses to Disinformation on Social Media Platforms 2019; McFaul 2019).

Section 1.3: Methodology

This work examines how the United States expresses its normative preferences in the international cyber norm formulation, and what influences its decisions to either engage or not engage in particular international regimes by analyzing cybersecurity practices (Finnemore and Hollis 2016; Maurer et al. 2020; Prince and Lacey 2018). Using the Key-Words-in-Context (KWIC) methodology, I conduct thematic analysis upon standardization documents that provide best cybersecurity practices for securing election technology, including non-voting infrastructure and electronic voting machines. I then identify if and to what extent these themes are existent in the international bodies the United States engages with and the rhetoric used in relation to those bodies.

Section 1.3.a) Key-Words-in-Context (KWIC) Analysis

The United States Election Assistance Commission (EAC) was used as a resource for gathering information on guidelines pertaining to the proper security of election infrastructure, including non-voting infrastructure. In addition to providing its own

guidelines, the EAC also provides external resources meant to guide local election officials in securing their infrastructure from cyberattacks. Among these resources, and as used in this analysis, are documents provided by the Center for Election Innovation and Research, the MITRE[3] Corporation, the Brennan Center for Justice, and the Center for Internet Security[4]. I used these documents both for their legitimacy in the eyes of EAC, as well as their broad representation. These documents are sourced from non-profits, research centers both private and federal, as well as academic institutions. These standards are meant to elucidate overall themes in American cybersecurity practices and were intended to be as representative of the election cybersecurity industry as possible while being limited enough to allow for thorough analysis of the documents.

Additionally, the EAC is responsible for developing election guidelines in accordance with federal accessibility requirements as established by the Help Americans Vote Act (HAVA) of 2002 and providing federal accreditation over voting systems. Therefore, the EAC was also used as a resource for federal voting machine security standards; the documents included in this portion of the analysis are the EAC Testing and Certification Program Manual and the Voluntary Voting System Guidelines Volumes I and II.

Jeyaraj and Zadeh identified 177 keywords that characterize the isomorphic nature of the cybersecurity industry in general. By calculating the frequency of Jeyaraj's and Zadeh's keywords across the studied documents and identifying the most frequently used keywords, I limit the scope of the cybersecurity concepts to those that specifically dominate electoral integrity and voting security efforts. I created a script using Python

[3] The MITRE Corporation is not-for-profit organization that oversees research efforts in support of US government agencies
[4] See Appendix B regarding the nature of these organizations and the relevance of the content of their publications to this analysis

3.7.4 and imported the Regular Expression Operation library to count the frequency of the keywords across the studied documents.[5] This script ignored capitalization and punctuation; additionally, organizational names and their respective acronyms were not counted as separate entities.

The keyword frequencies were grouped according to their association with either non-voting security or voting security. Any keywords that appeared in either of these two categories with a frequency of less than 0.5% were excluded in order to captures overarching themes rather than nuances of individual documents. The most frequently identified keywords were grouped thematically and served as the foundation for the following thematic analysis.

Section 1.3.b) Thematic Analysis

The thematic analysis focuses on practices that rose in prominence post-2016 as Russian interference and influence upon the 2016 US Presidential Election was responsible for spurring an unprecedented series of policies, organizations, and new perspectives on cyber protection (Ohlin 2017; Segal 2016; Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment 2016). To accomplish this, I first categorized the most frequently used keywords based upon the context in which they are used to identify themes within the cybersecurity practices. For example, the theme *Election Infrastructure as Critical Infrastructure* was identified after noting that the most frequently used keywords were used in the context of protecting critical infrastructure. Themes were also specifically tied to their association with either non-voting infrastructure or voting infrastructure.

[5] The Regular Expression Operations library is a third-party tool used in creating patterns and words that are of certain interest within text. In this research, this library was used to properly format the keywords of interest so that they could be properly identified within the studied documents. More information on this library can be found here: https://docs.python.org/3/library/re.html.

I emphasize cybersecurity practice and ideals implemented post-2016 by examining how the themes, identified from KWIC analysis, manifested in Congressional hearings and other governmental statement during that time period. It is one thing to identify these themes within cybersecurity practices that are often technical in nature, however, identifying them within the rhetoric of political figures, who often contribute to the domestic norm-creation, further solidifies their validity. To collect information on relevant hearings, I used the ProQuest Congressional Legislative and Executive Documents database and identified "election security" as the subject within the search criteria. I then limited inclusion of results to only those hearings that took place after December 31, 2015.[6] In cases in which I was looking for specific themes and/or keywords, I utilized the more granular functionality provided by ProQuest to search for the themes and/or keywords of interest within the provided hearing transcripts.

I then identified those most frequently used terms and categorized them into themes that correlate with changes that would be expected after the 2016 United States Presidential Election. Based upon this analysis, I compared the emergent United States' themes to those that have come out of international discourse on electoral integrity and voting security. International discourse was analyzed in the context of the following international bodies: the UN Group of Governmental Experts, the UN Open-Ended Working Group, the Global Commission on the Stability of Cyberspace, and the Paris Call for Trust and Security in Cyberspace. As these bodies were primarily prevalent starting in 2015, analysis was limited to the discourse taking place after this time.

[6] Although all Congressional hearing documents were dated after the 2016 United States Presidential Election, I expanded the search criteria to include the months leading up to the election in order to have a basis for comparison regarding security practices before and after the election.

The norms embodied in the UN GGE served as the foundation for the remaining three bodies, specifically the report published in 2015 in which international norms were agreed upon as being applicable in cyberspace (Grisby 2015; Marks 2015). I began my analysis by taking note of the themes arising out of the norms published in the 2015 report and noting similarities to the previously identified United States domestic cybersecurity practices. Upon taking note of emerging themes, I then turned my attention to statements the United States had made in regard to the UN GGE process in order to identify additional norms and take note of those that the United States are particularly concerned about. For example, while the UN GGE norms enumerate the importance of applying international humanitarian law to cyberspace, the United States specifically published statements highlighting the need for these practices to be utilized in the context of protection Internet freedom. Furthermore, I relied upon additional American documents published to the UN to clarify norms the United States have been continuous advocates for, even if they are not as obvious within the four bodies studied. The United States mission to the UN was used as the source for gathering these relevant statements.

Although the United States is not a participant in the UN OEWG process, the highly contentious nature of its inception, as led by Russia, made it is useful context to clarify United States norms. The United States published statements leading up to the UN resolution responsible for creating the UN OEWG. In noting its opposition, the United States made clear its own normative values. Additionally, I relied upon statements made by Russia in proposing the resolution to create the UN OEWG to frame the ongoing debate between the United States and Russia. Although the UN OEWG report has yet to be published, pre-reports have been published which Russia has provided commentary on.

The United States public primarily contributes in the UN GGE and UN OEWG. In order to provide insight into private sector norms, I also focused on discourse within the Global Commission on the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace. The Global Commission and the Paris Call are both groups led by the private sector and civil sector and in which the United States federal government is not officially involved. Similar to the action of the public sector, private sector actors within these international organizations have published their own statements. I relied upon these statements in clarifying norms as well as taking note of how the public and private sector were cooperating, or not cooperating in formulating these norms.

Analysis of how the United States public and private sector engage in the UN GGE, UN OWEG, the Global Commission, and the Paris Call were used to determine which norms translated from a domestic level to an international one. Additionally, it illustrated the extent to which norms were present. Analyzing this through the context of electoral protection helped in exemplifying a specific topic affected by cyber norms and showed how it may be present within future norms.

CHAPTER 2: Analysis of Election Cybersecurity Practices

This chapter analyzes the themes emerging out of the United States' domestic cybersecurity practices, specifically surrounding electoral protection. KWIC analysis showed the existence of the following important themes that in turn gave rise to specific norms: (1) election infrastructure is designated as critical infrastructure; (2) electronic voting machines' usage requires security considerations; and (3) private-public partnerships are used in combatting misinformation and disinformation. Each theme emerged as a result of the frequent usage of certain keywords across standardization documents; the keywords that justify the inclusion of each theme are included within each

theme's respective section. Each theme is elaborated upon to specifically articulate the relevant domestic norms. In order to further clarify how these norms are represented domestically, I also rely upon Congressional hearings and additional statements issued on behalf of the United States.

The documents used in this analysis, and as described above in *Section 1.3: Methodology,* were provided by the Election Assistance Commission (EAC), Center for Election Innovation and Research, the MITRE Corporation, the Brennan Center for Justice, and the Center for Internet Security. All these documents outline the ideal environment in which election infrastructure should exist in to protect against cyberattacks. Results of keyword analysis is depicted below in *Table 1.*[7] For further explanation on how keywords were reconciled in producing thematic meaning, see Appendix K.

[7] Keywords that had a frequency of <.50% were excluded from analysis in order to focus on overarching themes across election infrastructure rather than nuances of individual documents

Keywords	Frequency	Percentage
Security	609	44.68%
Systems	305	22.38%
National Institute of Standards and Technology (NIST)	93	6.82%
Cyber	76	5.58%
Backup	65	4.77%
Authentication	52	3.82%
Logging	50	3.67%
Cybersecurity	42	3.08%
Reporting	41	3.01%
Backup	39	2.86%
Access Control	38	2.79%
Monitoring	64	4.70%
Audits	29	2.13%
Disable	29	2.13%
Authentication	27	1.98%
Sensitive Data	26	1.91%
Sensitive Information	26	1.91%
Firewall	26	1.91%
Testing	24	1.76%
Cybersecurity	22	1.61%
Encryption	21	1.54%
Policies	20	1.47%
Plans	20	1.47%
Firewall	19	1.39%
Open Web Application Security Project (OWASP)	16	1.17%
Encryption	12	0.88%
Ransomware	11	0.81%
Assessment	11	0.81%
Compliance	10	0.73%
Programs	9	0.66%
Security Controls	9	0.66%
Mulifactor Authentication	14	1.03%
Center for Internet Security (CIS)	7	0.51%
Security Training	7	0.51%

Table 1 Keyword frequency across security documents concerned with election infrastructure security. Keywords that appeared frequently were used as the basis for the thematic analysis.

Section 2.1: Theme 1 (T1) - Election Infrastructure as Critical Infrastructure

When the United States elected to designate election infrastructure as critical infrastructure, it demonstrated the existence of keys norms the United States holds: (1) the importance of standardization across electoral cybersecurity practices that adhere to a critical infrastructure security framework and (2) the need to integrate risk management into cybersecurity practices that align with the National Institute of Standards and Technology Cybersecurity Framework. DHS defines critical infrastructure as infrastructure "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health

or safety, or any combination thereof" (Critical Infrastructure| DHS n.d.). Therefore, when American cybersecurity policies refer to the security of election infrastructure, they are considering the security of a system that can have profound negative effects upon society, including loss of life if compromised. It makes sense that norms, as outlined in these documents, would reflect the seriousness of this task.

In order to understand the cybersecurity norms that shape the security of election infrastructure, it is necessary to understand what norms dictate the security of critical infrastructure as a whole. The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA as a protectorate of the DHS and the new duties bestowed to the agency are indicative of what it means within the United States to protect critical infrastructure. Accordingly, the terms that frequently occurred in American standards documents can be attributed to the following norms that surround critical infrastructure:

T1a) Standardization of Election Cybersecurity Practices

NIST is frequently referenced within these documents in regard to best practices for securing election infrastructure and reflects norms that are imbedded within the risk management framework it provides in protecting critical infrastructure.[8] It is notable that despite NIST not providing information specific to the security of election infrastructure, but rather critical infrastructure, NIST is among the most frequently invoked keywords within the studied documents. This is indicative of the current posture of election infrastructure cybersecurity practices: a proclivity toward standardization, especially as it relates to critical infrastructure.

The use of the NIST Cybersecurity Framework indicates two key points: (1) The value American cybersecurity practices hold for voluntary standardization as a means of

[8] See Appendix C for more information regarding the content of the NIST Cybersecurity Framework

assessment and (2) The extent to which the United States treats election infrastructure as critical infrastructure. The NIST Cybersecurity Framework is specifically presented as being a set of voluntary guidelines that are not to be used by an organization in any one mandated way.

"To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio."

The NIST Cybersecurity Framework Executive Summary (National Institute of Standards and Technology 2018)

The regard the United States holds for standardization is evident across federally funded research and testimony from Congressional hearings. A 2018 consensus study report[9] by the National Academies of Science, Engineering, and Medicine[10] delved into the current state of election infrastructure in the United States and provided recommendations for enhancing security. In all of its recommendations regarding these three areas, the National Academies emphasizes the need for standardization and adherence to best security practices. Specifically, NIST and the EAC are called upon to develop security standards for validating the information within electronic pollbooks, and ballot design is to be standardized by the EAC as well. The National Academies report

[9] The National Academies defines its consensus report as being a evidence-based consensus on the best practices for securing future election as decided upon by an appointed committee of experts
[10] See Appendix D for more information regarding the content of the 2018 National Academies consensus report

calls upon Congress to "authorize and fund the National Institute of Standards and Technology, in consultation with the United States Election Assistance Commission, to develop security standards and verification and validation protocols" (Securing the Vote: Protecting American Democracy 2018).

The preference for standardization, stemming from the critical infrastructure designation, is also observed in Congressional hearings. Since 2016, there have been thirty-nine hearings[11] regarding election security in which witnesses before the respective committees called for standardization across voting and non-voting infrastructure security, misinformation and disinformation, and regarding the protection of other assets of election infrastructure.[12] From 2012-2015, no hearings regarding the state of electoral integrity and voting security included a noticeable call for standardization in cybersecurity practices. Rather, standardization became a topic of discussion most frequently following the events of the 2016 United States Presidential Election and in the lead up to the 2020 United States Presidential Election. As depicted in *Figure 1* below, there was a noticeable increase in hearings regarding the role of standardization in election security in 2017. 2017 was also the year in which DHS designated election infrastructure as critical infrastructure thus making norms of critical infrastructure protection applicable to election infrastructure protection specifically.

[11] See Appendix E for more information regarding the nature of these studied hearings and their relevance to the research

[12] Information collected using ProQuest's database of Congressional Legislative and Executive Documents *Limited data was available regarding the 2020 Congressional Session due to the timing of this research, as well it being an election year with most preparation being accomplished prior and follow-up being conducted in 2021

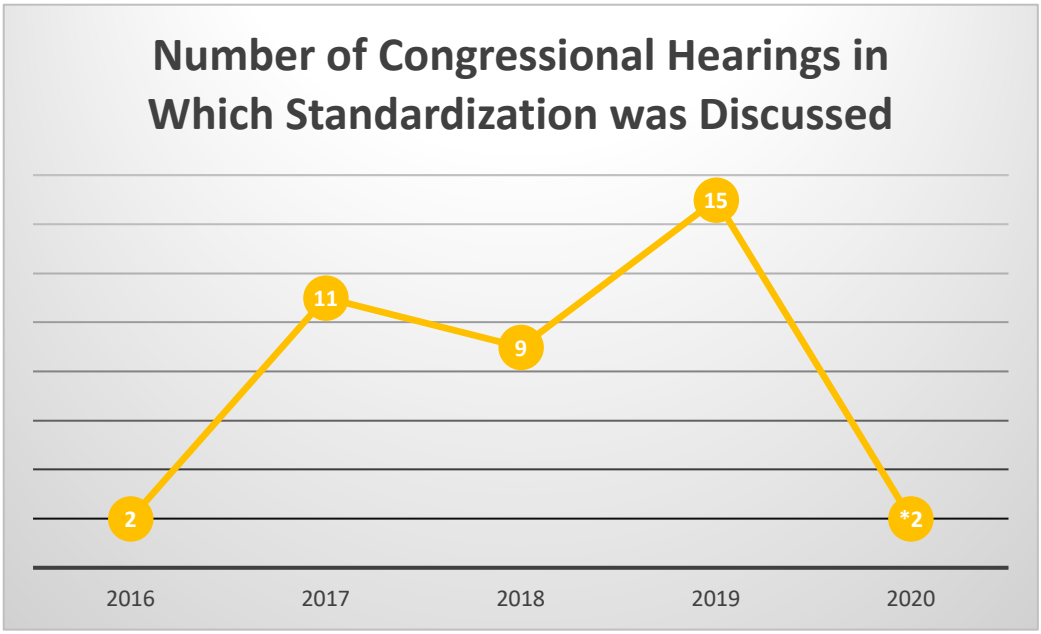


Figure 1 Change from 2016-2020 in number of congressional hearings that included the need for standardization in electoral integrity and voting security. Russian interference into the 2016 United States Presidential Election occurred in 2016 and explains the sharp rise in calls for standardization in electoral protection.

This sentiment regarding the necessity of standardization was shared across government, academia, civil sector, and the private sector - for example, as documented in The Road to 2020: Defending Against Election Interference hearing before the House Subcommittee on Cybersecurity Infrastructure Protection and Innovation.[13]

Francis Taylor, board member of United States CyberDome[14], testified to his experience as a security professional and made recommendations for defending election infrastructure in the 2020 United States Presidential Election. Taylor justified his call for mandated, minimum cybersecurity standards for political campaigns by stating

[13] The House Subcommittee on Cybersecurity Infrastructure Protection and Innovation was created prior to the meeting of the 112th Congress and, since the designation of election infrastructure as critical infrastructure in 2017, has heard testimony regarding the current state of cybersecurity in safeguarding election.

[14] US CyberDome is a non-profit entity that provides cybersecurity expertise to presidential campaigns in order to protection against foreign interference

"campaigns may have greater incentive to spend efforts and funds on cybersecurity if they know their competitors are obligated to the same expenditures".[15]

Calls for standardization are not restricted to cybersecurity practices that affect physical election infrastructure, they are also a common proposed solution in regulating misinformation and disinformation. Richard Stengel, former Under Secretary of State for Public Diplomacy and Public Affairs, testified that direct government intervention is not needed, but rather action is needed that sets standards for private organizations in how they combat misinformation and disinformation (private-public partnerships and how they manifest in the United States will be further discussed below).

Traditionally, standards in cybersecurity have been regarded as those similar to the NIST Cybersecurity Framework: a set of guidelines that information technology professionals should abide by when configuring their systems. The private sector, however, has also advocated for standardization in the form of multi-stakeholder engagement that sets international norms of behavior in cyberspace, thus deterring nation-states from engaging in cyberattacks upon electoral infrastructure. Ginny Badanes, director of strategic projects for Microsoft's Defending Democracy[16] program, advocated for this approach stating that while the technical hygiene that Microsoft provides is valuable, equally important is the federal government's role in "culture-setting" an environment in which cybersecurity is a top priority. Badanes specifically refers to and endorses the norms presented by the UN GGE and the Paris Call, lauding their approaches to standardizing behavior in cyberspace through multi-stakeholder

[15] Taylor went further and suggested there be a federally supported threat sharing network in order to create these standards. Such information sharing networks are the cornerstone of critical infrastructure protection programs operated by CISA.

[16] Defending Democracy was launched in order to assist political campaigns in improving their cybersecurity posture. To date, the program has provided security tools, training, and threat monitoring capabilities to political campaigns.

engagement. Both these organizations have been fundamental norm-setting bodies for acceptable and unacceptable behavior in cyberspace (The Road to 2020: Defending Against Election Interference 2019).

Calls for standardization of election infrastructure security emerged prominently with the designation of election infrastructure as critical infrastructure. However, as apparent in this hearing and others, the desire for standardization has proven to be one that takes many forms, from the traditional adherence to a given cybersecurity framework to a call for participation in international norm-setting bodies that subsequently gives rise to standards.

T1b) Risk Management and the National Institute of Standards and Technology (NIST) Cybersecurity Framework

The NIST Cybersecurity Framework is an assessment tools used by agencies such as CISA to evaluate the current state of an organization's cybersecurity posture. Accordingly, it is a useful tool for understanding the risk management measures that election protection entities are implementing in upholding this posture. Risk management is defined by the NIST Cybersecurity framework as "the ongoing process of identifying, assessing, and responding to risk" (National Institute of Standards and Technology 2018). From a high-level, risk management necessitates five functions: Identify, protect, detect, respond, recover[17]:

a) **Identify:** Develop an organizational understanding of the assets, individuals, systems, data, and capabilities that comprise a system in order to understand the inherent risks

[17] Further elaboration on these functions is provided in Appendix C

b) **Protect:** Insatiate appropriate safeguards against attacks that would compromise the delivery of critical services

c) **Detect:** Develop tools and activities that are capable of detecting cybersecurity events

d) **Respond:** Develop a plan in the event of a cybersecurity incident

e) **Recover:** Develop tools and activities to recover critical capabilities or services in the event they are compromised during a cybersecurity incident

This theme of risk management is inexorable from the framework provided by NIST, especially when discussing it in the context of critical infrastructure security. With this in mind, I will be exploring this theme by understanding how the keywords of interest are used in the context of identifying risk, protecting from risk, detecting risk, responding to risk, and recovering from the effects of an exploited risk. This also allows us to understand what assets are of particular concern when it comes to protecting election infrastructure. *Table 2* categorizes the frequently identified keywords in accordance with the related NIST Cybersecurity Framework function.

Identify	Protect	Detect	Respond	Recover
(Risk) Assesment	Authentication	Logging	Reporting	Backup
	Access Control	Monitoring		
	Disable	Audit		
	Firewall			
	Encryption			

Table 2 Frequently identified keywords that have been grouped with the NIST Cybersecurity Framework functionalities they correspond to. This demonstrates the importance of the NIST Cybersecurity Framework in electoral protection as well as the most import functionalities.

The Framework identifies through the development of an understanding of the various systems, people, assets, data, and capabilities that define an organization. While

this is an important function in cybersecurity planning, it was found to not be as prominent within election infrastructure security planning. Risk identification can be achieved in several ways; within the analyzed documents, risk assessment was specifically concerned with the supply-chain structure of election infrastructure. When handling information, such as voter registration information, it is common within the United States to corroborate information with in-state government agencies. For example, The Help Americans Vote Act (HAVA) and the National Voter Registration Act of 1993 (NVRA) mandates that voter registration information is verified with a motor vehicle authority via a driver's license. Furthermore, there is the need to facilitate out-of-state government data transfer, such as when the USPS "Change of Address" service is used to inform a jurisdiction that a registered voter has moved. The decentralized nature of American election infrastructure coupled with the need for constant communication between jurisdictions necessitates risk assessment of various parts of the supply chain, such as the federal and state level (Casey et al. 2019).

The analyzed documents exhibit a strong focus on actually protecting the assets that support election infrastructure. These are presented predominantly as "security control" measures that can be implemented to mitigate risk to various assets. A vital component of this risk mitigation strategy is granting network access and capabilities to those that absolutely need it. Furthermore, analysis revealed the most important aspect in need of protection is voter registration information.[18] When illustrating the severity of the compromise of sensitive information, the Russian influence upon the 2016 US Presidential Election is often used as motivating example in US rhetoric:

[18] For further information on how the "protect" functionality is utilized in American cybersecurity practices, see Appendix L

"Russian intelligence operatives and their thinly-disguised proxies stole and leaked sensitive information from political campaigns and employed hundreds of operatives in "troll farms" to spread and amplify toxic content on social media, and to orchestrate divisive political rallies on American soil"

Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School; former Chief of Staff to the Secretary of Defense
and Assistant Secretary of Defense for Homeland Defense and Global Security (Burr et al. 2018)

The security control measures associated with the "detect" functionality of the NIST Cybersecurity Framework, within the studied documents, are predominantly focused on implementing tools within election infrastructure that keep continuous records on network activity. Monitoring and logging tools allow information technology to verify the presence of unauthorized activity. Once again, this is explored within the reports as being important in the context of securing voter registration databases.[19]

Reporting is an important piece in critical infrastructure recovery efforts in the event of a cyber incident and is a vital component in ensuring the "respond" functionality. This is primarily accomplished within information sharing networks, which are a cornerstone of the critical infrastructure effort. Information sharing networks consist of "federal, state, local, territorial, and private sector partners" that communicate with one another via the CISA-managed Homeland Security Information Network, Infrastructure Protection Gateway, and National Infrastructure Coordinating Center (Election Infrastructure Security | CISA n.d.). When a partner within this threat-sharing network identified a threat, these platforms are used to disseminate information as quickly as

[19] For further information on how the "detect" functionality is utilized in American cybersecurity practices, see Appendix M

possible regarding the threat to other critical infrastructure stakeholders. Another important piece of effective reporting, as highlighted in the examined documents, is effective employee training. Employees, such as poll workers, are highly recommended to be trained in identifying indicators of a cyber incident and having clear direction as to who to report the incident to.

In addition, regular backups have the capability to restore information lost in the event of a cyberattack and enable the "recovery" functionality. In these reports, there is a focus on keeping backups of electronic pollbooks in physical forms, transaction log reports, and voter registration database information. As will be observed in the themes surrounding electronic voting machine security, having physical as well as electronic backups of information is increasingly becoming more important in an era where technology is often seen as the best solution to complex problems. The security surrounding electronic voting machines has also given rise to additional norms.

Section 2.2: Theme 2 (T2) - Securing Electronic Voting Machines

The United States Election system is unique in its usage of electronic voting machines which has given rise to the following norms: (1) a preference for decentralized accreditation and (2) a growing movement to become less dependent on software in determining the accuracy of the votes it records. Many nations have prohibited the use of electronic voting machines, citing the inherent insecurity of these systems. The same controversy that has prohibited its usage in other nations has cultivated debate regarding the use of electronic voting machines in the United States. Opposition opinions range from advocating for stricter practices in managing electronic voting to banning electronic voting all-together. The spectrum of opinions will be analyzed in this theme and will be specifically focused on how the idea of software independence shapes norms. As a result,

the United States has taken particular steps to standardize voting machine security through standardization efforts facilitated by the EAC. The EAC Testing and Certification Program Manual 2.0 took effect in 2015 and contains the criteria the EAC applies to grant certification of electronic voting machines used within the United States. The EAC Manual guides certification authorities in how to utilize the Voluntary Voting System Guidelines (VVSG) in determining whether or not to grant accreditation. Although EAC has the sole federal authority to certify and decertify voting machines, EAC certification is not required for electronic voting machines to operate within a state. However, thirty-eight states use some aspect of this federal certification program in certifying the voting machines used at a state level (National Conference of State Legislatures 2018; Root et al. 2018). Within this theme, I will analyze how this decentralized accreditation system has created certain norms, most notably a preference for voluntary standardization that is also a feature of the NIST Cybersecurity Framework as discussed in the previous theme. As done in the previous theme, thematic analysis will be aided by the KWIC methodology and the data collected depicted in *Table 3*:

Keyword	Frequency	Percentag
Systems	1295	32.52%
Testing	1177	29.56%
Security	294	7.38%
National Insitute of Standards and Technology (NIST)	243	6.10%
Compliance	145	3.64%
SOC	94	2.36%
Regulations	91	2.29%
Evaluation	87	2.18%
Reporting	72	1.81%
Access Control	50	1.26%
Programs	49	1.23%
Assessment	49	1.23%
Audit Trail	45	1.13%
Plans	36	0.90%
Disable	27	0.68%
Audits	22	0.55%
Monitoring	21	0.53%

Table 3 Keyword frequency across security documents concerned with electronic voting machine security.[20] The most frequently used keywords served as the basis for thematic analysis, most importantly those relating to software independence and other technical specifications.

T2a) Decentralized Accreditation

Federal standardization is prolific across all states in how they choose to evaluate electronic voting machines used in their respective jurisdictions. However, they are not all used in the same way. *Figure 2* shows the diverse ways in which states use federal certification guidelines and thus demonstrates another way in which the United States has demonstrated its preference to adhere to voluntary standards:

[20] Keywords that had a frequency of <.50% were excluded from analysis in order to focus on overarching themes across election infrastructure rather than nuances of individual documents

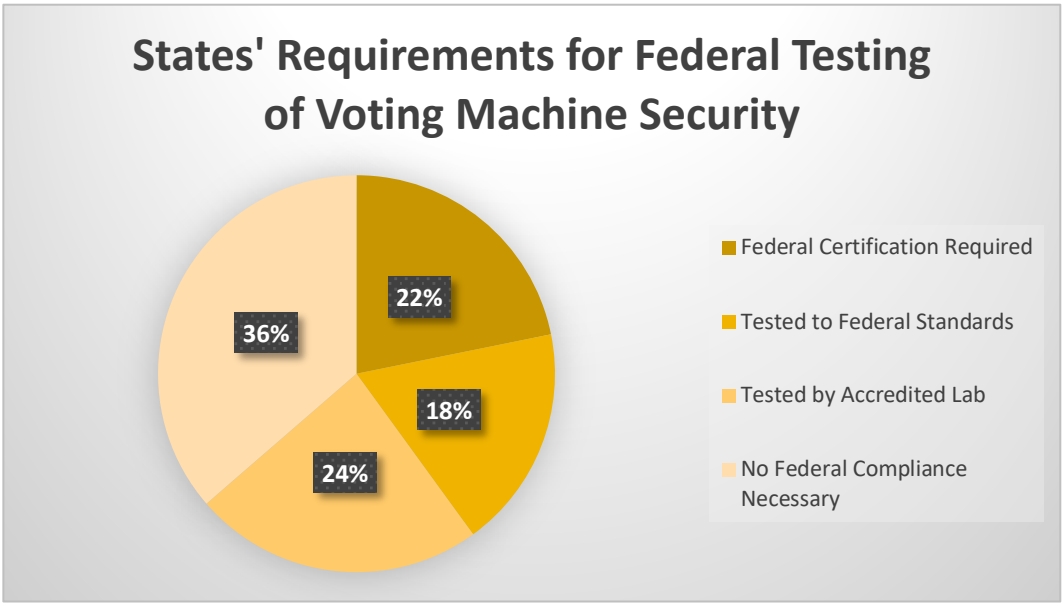


*Figure 2 Degrees of federal testing an electronic voting machine must undergo before being used statewide.[21] This demonstrates the diverse ways in which state choose to utilize federal guidelines in evaluating the security of electronic voting machines. *Includes the District of Columbia*

The EAC established the VVSG in order to provide a level of rigor in assessing how electronic voting machines are tested before being used in elections. However, not all states use these guidelines in the same way. The manners in which states used the VVSG, and as utilized in Figure 2, are described below (State Requirements and the Federal Voting System Testing and Certification Program 2009)[22]:

a) **Federal Certification Required:** Electronic voting systems utilized within the state must be certified by the EAC

b) **Requires Testing to Federal Standards:** State statues require testing to some federal standard, including those provided by the EAC, Federal Election Commission, and NIST

c) **Requires Testing by a Federally Accredited Laboratory:** Voting systems must be tested by a federally accredited laboratory

[21]From EAC State Requirements and the Federal Voting System Testing and Certification Program
[22]The level of federal compliance required by each state is included in Appendix F

d) No Federal Compliance Required: State regulations make no mention of any federal authority in testing of its voting systems

In order to understand the norms that arise out of a decentralized structure such as this, I evaluate the themes that emerge based upon which category of federal regulations states abide by. I analyzed the EAC Testing and Certification Program Manual 2.0 along with its source material, the VVSG Volumes I and II. KWIC analysis revealed frequent usage of the following terms as depicted in *Table 4*:

Keyword	Frequency	Percentag
Systems	1295	32.52%
Testing	1177	29.56%
Security	294	7.38%
National Insitute of Standards and Technology (NIST)	243	6.10%
Compliance	145	3.64%
SOC	94	2.36%
Regulations	91	2.29%
Evaluation	87	2.18%
Reporting	72	1.81%
Access Control	50	1.26%
Programs	49	1.23%
Assessment	49	1.23%
Audit Trail	45	1.13%
Plans	36	0.90%
Disable	27	0.68%
Audits	22	0.55%
Monitoring	21	0.53%

Table 4 Keyword frequency across documents concerned with the security of voting systems. The most frequently used keywords were used as the basis for a thematic analysis regarding how states use federal accreditation standards.

As expected, many of the terms were related to the concept of testing for security vulnerabilities. The EAC and VVSG, and by extension the federal standardized, approach to securing voting machines covered the following concepts: security, accuracy, error

recovery, integrity, system audit, election management systems, vote tabulation programs, ballot counters, telecommunications, and data retention.[23]

States that require electronic voting machines to be federally certified before being operated within the state embody norms that reflect federal guidelines and thus those included in the NIST Cybersecurity Framework; Colorado is one of these states. Following a history of implementing audit policies in line with federally guidelines, Colorado became the first state to mandate risk-limiting post-election audits upon voting machines (Root et al. 2018). Colorado Secretary of State Jena Griswold emphasized the importance of audit policies in electronic voting stating that, "In Colorado, voting machines are not connected to the internet, and each vote has a paper record. Ballot envelope signatures are verified and results of the elections are audited, and a team of bipartisan judges monitors in-person voting" (Griswold 2019).

States that do not require federal certification, but do require testing in line with federal standards, often leave certification authority to their respective Secretary of States. As a result, many of the normative standards that are upheld in the federal certification process are prominent, however, it is a state authority who declares the final certification or revokes certification (State Requirements and the Federal Voting System Testing and Certification Program 2009). Additionally, state regulations encourage collaboration with state universities in conducting testing upon electronic voting machines. Connecticut, one of the states that mandates compliance with federal testing standards, but not federal certification, funded the establishment of the University of Connecticut Center for Voting Technology and Research (VoTeR Center) to advise the Secretary of State in the

[23] For further information regarding how electronic voting machine security is related to the NIST Cybersecurity Framework, see Appendix N

certification process. In establishing the importance of state institutions in the voting system security testing process, Dr. Alexander Shvartsman, director of the VoTeR Center, stated "Looking toward the future, we are hoping to improve the methodology of electronic voting, and we will most likely be involved in the prospective upgrades of this system" (UConn Team Ensures Election Integrity 2010). The importance of relying upon state authorities and knowledge is an important theme for states that abide by these guidelines, however, ultimately, they still invoke federal standards as a benchmark of credibility. For example, the primary function of the VoTeR Center is to conduct and establish credible policies in post-election audits, a prominent theme in all federal accreditation guidelines.

Within states that require testing by a federally accredited laboratory, state participation in the accreditation process is lessened when compared to practices in states like Connecticut. State subject to these guidelines tend to still involve state authorities in the certification decision process. In Alabama, the Alabama Electronic Voting Committee may send experts as selected by the committee to aid in testing at the federal level (Alabama: Examination and Certification of Equipment 2008). State testing authorities can also be involved prior to federal accreditation, such as in Illinois (Illinois: Application for Approval of Voting Systems 2009). However, in these states the state authority is only able to certify those voting machines that have been tested and certified within a federally accredited laboratory.

States that do not require federal accreditation nor testing by a federally accredited laboratory retain the most power when it comes to determining the security of electronic voting machines. In these states, it is common practices for state authorities to both develop state-specific standards and determine adherence to said standards. Of course,

this does not prohibit those state standards from taking significant influence from federal standards. In Alaska, a state not requiring federal accreditation nor testing, still relies on DHS in the development of security assessments, information sharing, and training. In a 2018 statement, Alaska's Division of Elections justified its partnership with DHS by stating "we are only as good as our understanding of the threat, and information sharing is a key tool for staying ahead of the bad guys" (Bahnke and Krebs 2018). Even in states where it is explicitly stated that sole power to establish accreditation standards is vested to state authorities, all voting systems certified within the state are accredited by the EAC.

The only two accredited voting systems in Florida, Dominion Voting Systems and Election Systems and Software, LLC., are EAC accredited vendors. Regardless, Florida Voting System Standards makes clear that "Qualification [granted by a federally accredited laboratory] will not satisfy requirements for Florida Certification. It is imperative that applicants for Florida Certification notify the independent testing authorities that the ITA [independent testing authority] test plans are to include specifications for the Florida Voting Systems Standards" (Hood 2005). As noted below in *Table 5,* KWIC analysis conducted on the Florida Voting Systems Standards revealed that while it shared similar concerns and norms to those present in federal standards, there is a clear lack of other technical specifications. *Table 5* shows the most frequent keywords are those that are general ways of describing components of cybersecurity, rather than how to actually secure those components.

Keyword	Frequency	Percentage
Systems	134	41.23%
Testing	66	20.31%
Audit	33	10.15%
Compliance	22	6.77%
Reporting	14	4.31%
Programs	11	3.38%
Security	8	2.46%
Evaluation	7	2.15%
Disable	6	1.85%
Regulations	5	1.54%
Plans	4	1.23%
Instrumentation	3	0.92%
Authorizaion	2	0.62%
Destroy	2	0.62%

Table 5 Keyword frequency within Florida voting system guidelines. Despite Florida leaving accreditation authority solely to state powers, its accreditation guidelines are extremely similar to federal accreditation guidelines.

Overall, the influence of EAC and other federal standards across this decentralized accreditation system is unable to be ignored. Whether a state requires full federal accreditation or creates its own standards, the normative values and themes persistent in federal standards are the foundation for all state accreditation processes. The desire for control a state wishes to have over the accreditation process appears to more of a motivating factor for varying accreditation processes than a true disregard for federal standards. As a result, the United States' cybersecurity practices demonstrate a normative desire for voluntary standardization that allows jurisdictions to have flexibility in cyberspace. This desire for flexibility extends beyond a domestic level as the United States has sought to establish the applicability of international law in cyberspace, which would allow for flexibility in determining when and how certain laws are applicable.

T2b) Software Independence

Software independence was a term coined by Dr. Ron Revest and John Wack of NIST and, above all, demonstrates a growing normative distrust of the election results recorded by software and thus necessitating a need for physical auditing measures. The researchers proposed that software independence be a global characteristic of voting technology: a purely technological problem, originating with voting software, should not be capable of going undetected in the election as a whole. Practically, this means that there should always be some human-performed checking measures in place to verify the integrity and accuracy of election results (Human Factors and Privacy Subcommittee and Security and Transparency Subcommittee n.d.). NIST's profound impact on voting technology security practices has ensured the prominence of software independence and warrants its inclusion in this thematic analysis. The VVSG 2.0 is awaiting publication and one of the new guidelines is that all voting system technologies demonstrate software independence. Although this is an important norm domestically, it was not as apparent internationally when comparing it to those norms that manifested in relation to critical infrastructure protection.

Calls for software independence have been renewed partially in response to proposed technological solutions in auditing election results. Blockchain technology is one such solution and has received criticism. [24] The National Academies report comments on why software independence and blockchain are not compatible, noting that "Software is required to examine postings on blockchain. If such software is corrupted, then verifiability may be illusory. Software independence is not, therefore, achieved through posting ballots on a blockchain: as ballots are represented electronically, software

[24] The proposed solutions surrounding blockchain technology advocate for the blockchain acting as a "virtual electronic ballot box". Blockchain is meant to be immutable - for every ballot cast, results would be recorded in the blockchain and can only be appended to, not altered, but a specific set of managers.

independence may be more difficult to achieve" (Securing the Vote: Protecting American Democracy 2018). Simply, the experts of the National Academies are of the opinion that software independence is valuable because it allows for verifiability of electronic election results and is not subject to technical glitches. On the other hand, blockchain technology represents ballots electronically and can be subjected to such glitches and loses the value of simple verifiability.

Software independence is not just a solution that voting security researchers advocate for, but also one that is evident in federal testing standards, such as the EAC Testing Manual and VVSG as revealed by KWIC analysis. Despite guidelines not specifically calling for software independence in currently published versions, vital components of a software independent strategy were included in the EAC Testing Manual and VVSG as a focus on human-based auditing procedures. These ideas are paving the way for the inclusion of direct guidelines of software independence in future versions.

Tables 6 and 7 below demonstrates the focus that security standards, specifically concerned with voting machine security, have on these human-based auditing procedures. The tables depict the frequency of common security terms that are necessary to describe approaches to software independence. The documents analyzed for *Table 7* were concerned with non-voting infrastructure security and tend to abide by common norms in security standards, such as the NIST Cybersecurity Framework. Thus, terms such as "reporting" and "audits" and other terms associated with software independence would be expected to appear frequently. However, *Table 6* draws its analysis from documents specifically concerned with voting machine security (EAC Testing Manual and VVSG) and shows a significant increase in such terms. Not only this, but the way in which they are

used in context are related to the ideal of software independence rather than the generic audit policies in the *Table 6* documents.

Term	Frequency
Reporting	72
Audit Trail	64
Audits	22
Total	158

Table 6 Software independence terminology within reports on electronic voting machine security. Software independence terminology occurs more frequently within these documents, than those studied in Table 7, and demonstrates how reliant software independence is upon proper audit procedures.

Keywords	Frequency
Reporting	41
Audits	29
Audit Trail	1
Total	71

Table 7 Software independence terminology within reports on non-voting election infrastructure security

The VVSG specifically contains a section that details one of the most common solutions for ensure software independence: a paper audit trail. A paper audit trail is some physical record of a voter's selections on a direct-recording electronic (DRE) voting machine.[25] In order to meet the VVSG standards for a DRE voter verifiable paper-audit trail, the following functional requirements must be met:

a) A printed, paper recorded summary of the voter's ballot selection that can then be compared to the electronic ballot selections

b) Mechanism by which voter can confirm or reject recorded results

c) Ballot box to store paper recorded summaries

[25]A DRE voting machine provides an electronic voting interface for a user to make selections on with those selections then being stored in the machine's local memory for later removal and processing.

d) A paper record corresponded to each DRE

By implementing these requirements, the VVSG is advocating for a software independence approach to vote tabulation that makes assurances of voting integrity and accuracy. Officials concerned with election security have taken measures to mirror the function requirements in the VVSG to ensure software independence. The Office of State Procurement in Louisiana announced the replacement of 10,000 DRE voting machines citing the importance of the Voter Verifiable Paper Audit Trail (VVPAT) implemented int the new machines. In the quote below, the Office of State procurement is echoing a pervasive sentiment that VPPAT systems are one of the best ways to verify electronic election results:

"VVPAT system provides voters with the peace of mind that their vote is recorded accurately by allowing them to verify their vote on paper before casting their vote electronically on a voting machine. This feature will also enhance the continued accuracy of state elections by providing a mechanism for a full paper audit of each election"

Louisiana Office of State Procurement (Louisiana looking to replace entire stock of voting machines 2021)

Software independence is a response to the technological dependence that has led to proposed solutions demonstrating considerable security concerns, such as blockchain technology. The rise in its prominence, in federal standards, research, and electoral activity, has demonstrated a growing norm that values limited technological solutions to growing cybersecurity concerns in the electoral process. However, software independence has been more subtle in in international bodies, especially within the UN GGE.

Consequently, the private sector and civil society has worked to embed norms related to software independence within the Paris Call and the Global Commission. In a world in which technology is presented as solution to some of the most pressing issues, election experts are pushing back and emphasizing the importance of human-centered procedures in safeguarding elections.

Section 2.3: Theme 3 (T3) - Private-Public Partnerships in Managing Misinformation and Disinformation

The role of misinformation and disinformation management in safeguarding elections is an emerging issue stemming in large part from Russian interference into the 2016 United States Presidential Election. However, this goal is complicated by the fact that the private sector is largely responsible for managing the flow of electoral information that individuals are consuming. As a result, private-public partnerships have become a necessity in ensuring electoral management and has given rise to the following norms: (1) the hesitation to bring a multi-stakeholder model fully to fruition and (2) the importance of protecting freedom of speech on the Internet while managing misinformation. Although it is not a traditional component of cybersecurity, insofar that there are federal guidelines to regulate it, the damage misinformation and disinformation can inflict upon electoral integrity is a distinct concern within the United States and has made it a focal point of several international organizations seeking to protect elections.

Russian interference into the 2016 US Presidential Election prompted hearings to be held regarding the extent and methods of the interference. *Figure 3* below depicts the fluctuation of Congressional hearings regarding the threat misinformation and disinformation poses to electoral integrity. From 2015 to 2016, there were no hearings that specifically discussed this form of threat. Rather, as noted from *Figure 3,* it appears

that the role of misinformation and disinformation in the Russian interference campaign into the 2016 United States Presidential Election acted as a catalyst for these discussions to take place at the federal level beginning in 2017.

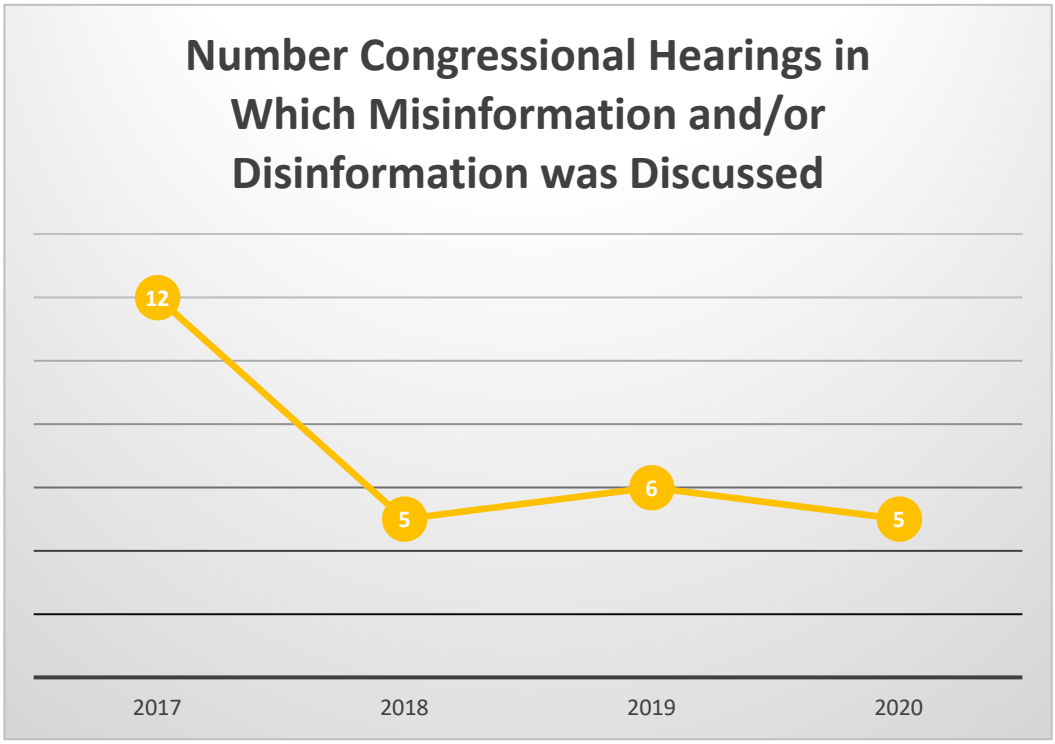


Figure 3 Number of Congressional hearings in which misinformation and/or disinformation campaigns were discussed in the context of electoral integrity. Occurrences of these kinds of Congressional hearings increased significantly following Russian interference in 2016.

The following analysis is concerned with the discourse taking place within these Congressional hearings. Thematically, it is important to understand the kind of multi-stakeholder engagement the private and public sector is advocating for in ensuring electoral integrity, as well how the United States' value for free speech is complicating the matter.

T3a) Multi-Stakeholder Engagement and Information Sharing: An Elusive Solution

Following the events of 2016, an influx of hearings, regarding the threat misinformation and disinformation poses to electoral integrity, were held and sought to establish the role the private and public sector would play in combatting it, however, these

discussions were unable to clarify what a multi-stakeholder model would look like. The ideal multi-stakeholder framework would be achieved when the public and private sector would contribute all their respective resources towards the pursuit of electoral protection. For example, the private sector would willingly provide information to the government that would assist in managing the spread of misinformation and the government would help facilitate private-sector solutions in addressing misinformation. Above all, both sectors would coordinate their goals and work toward a solution that defends the electoral system. Despite this multi-stakeholder framework being prevalent in calls for solutions to managing misinformation, little has been done to bring this framework to fruition.

It appears the private and public sector each has different ideas regarding what the ideal multi-stakeholder framework would resemble and what roles the public and private sector are to play. The private sector is frustrated by the lack of government leadership in establishing norms that control misinformation, while the public sector sees privately controlled social media platforms as breeding grounds for misinformation that are going largely unchecked. The ambiguity surrounding the private and public sector's roles in addressing cyber threats to elections, as well as general frustration with the current multi-stakeholder model, is evident from Congressional hearings following the 2016 United States Presidential Election.

The initial hearing on misinformation's role in the 2016 United States Presidential Election was held before the Senate Committee on Intelligence to examine the extent of Russia's usage of information warfare and the role of the multi-stakeholder framework. Despite Russia's historical utilization of information warfare, the private sector and civil society characterized the government sector as being unprepared and passive in combatting it. This is not due to a lack of information according to these sources, but

rather an unwillingness to remain attentive to research derived from outside the public sector. Dr. Roy Godson, Professor Emeritus of Government at Georgetown University, testified that despite awareness of historical Russian means of interference, "the attentive public and most elected officials continue to be surprised by Russia's operational behavior". To remedy this action, Dr. Godson recommended developing "rules of the road" that "both sides [Russian and the United States] follow to avoid the catastrophe neither wants". Dr. Godson's "rules of the road" solution insinuates the development of cyber norms, and specifically those related to election security, "For example, should we tolerate Russian (and other) efforts to influence the mechanisms of our election process and its outcomes, now or in the future" (Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Panel I 2017).

"Rules of the road" is rhetoric that has consistently been used to describe cyber norms, such as those established in the UN GGE, UN OEWG, the Global Commission, and the Paris Call. Ginny Badanes of Microsoft's Defending Democracy program, as discussed above in *Section 2.1 - Theme 1b,* echoed this sentiment in preparation for the 2020 United States Presidential Election; Badanes specifically invoked the Paris Call and the UN GGE as effective examples in establishing "rules of the road" that elected officials should pay attention to and facilitate meaningful contributions to.

Members of the private sector and civil society not only call for norms in cyberspace but advocate for United States leadership in establishing them. Clint Watts, senior fellow at the Center for Homeland Security at George Washington University and the Foreign Policy Research Institute, testified "It's time the United States reminds the world [...] we stand alongside our allies in defending our democratic systems of government from power-hungry tyrants" (Disinformation: A Primer in Russian Active

Measures and Influence Campaigns: Panel I 2017). In this case, the private sector and public sector sees current government efforts to establish norms as insufficient. The testimony described above comes primarily from non-partisan organizations, such as academia, research institutions, other members of civil society, and private sector entities that are all not responsible for hosting platforms where misinformation comes to fruition. As a result, the organizations discussed above present a relatively neutral understanding of the state of misinformation and disinformation, therefore, it is necessary to understand how entities actively involved in the transmission of such misinformation, such as large technology companies like Facebook, Google, and Twitter, perceive their role in this multi-stakeholder framework, as well as the role of the government.

Overall, these technology companies appear to vouch for multi-stakeholder engagement, including with the government. However, the extent to which technology companies are willing to work with the public sector to combat misinformation and disinformation is left vague. In a hearing entitled *Russian Online Disinformation Tech Solutions*, representatives from Facebook, Google, and Twitter testified and left any mention of government cooperation toward the end of their respective testimony. Colin Stretch, General Counsel for Facebook, testified "By working together, business, government, and civil society can make it much harder for malicious actors to harm us". Richard Salgado, Senior Counsel for Google, similarly stated "Google and YouTube are committed to doing our part, but as well all recognize across government, civil society, and the private sector, we will only make progress by working together to address these complex issues at their root". Sean J. Edgett, Acting General Counsel for Twitter, also included a vague statement on government cooperation: "We are resolved to continue this work in coordination with the government and our industry peers. Twitter believes that

this hearing is an important step toward furthering our shared understanding of how social media platforms, working hand-in-hand with the public and private sectors, can prevent the propagation of extremist content and disinformation both generally and, of critical importance, in the context of the electoral process" (Russian Online Disinformation Tech Solutions 2017). On the other hand, the testifying technology companies were more specific about engagement across the private sector.

In response to the spread of misinformation across Twitter, the technology company launched the Global Internet Forum to Counter Terrorism (GIFCT): a partnership between Twitter, YouTube, Facebook, and Microsoft to facilitate "information sharing, technical cooperation, and research collaboration", as noted by Edgett. Additionally, Facebook reaffirmed its commitment to "work more closely with other technology companies to share information on how to identify and prevent threats and how to respond faster and more effectively" (Russian Online Disinformation Tech Solutions 2017). The more specificity offered in working with the private sector when compared with public sector cooperation is telling. It paints a picture in which private sector organizations are hesitant to directly work with government entities in addressing these problems. However, the public sector has a different vision as to how multi-stakeholder engagement is to function.

In addition to the government's role in establishing cyber norms, the public sector has other ideas regarding its role within multi-stakeholder engagement. During the same hearing on Russian disinformation and the role of technology companies, Senator Lindsay Graham (R- South Carolina) explained, while articulating the purpose of the hearing, that "And to the extent legislation can help, we'd like to know what we could do to help. To the extent that the status quo is acceptable, we all want to go on record and

say it is not" (Russian Online Disinformation Tech Solutions 2017). The public sector calculates the extent to which it can help based upon how transparent companies are willing to be. Specifically, the public sector desires to have access to private sector information pertinent to national security, such as how social media user information is being used and accessed by third parties: a strategy used by Russian to determine which social media users would be particularly susceptible to spreading misinformation (Dutta et al. 2020). However, information sharing between the public and private sector has been limited thus pushing the public sector to bring information to the private sector in hopes that they will utilize it in combatting misinformation.

CISA's Countering Foreign Influence Task Force (CFITF) brings together actors across the federal government to identify threats linked to misinformation. Additionally, the CFITF uses the gathered information to alert social media organizations of disinformation campaigns being waged on their respective platforms. After CTITF brings threats to the attention of social media platforms, it is not clear whether there is any enforcement mechanism nor any other framework that actually addresses the misinformation. Rather, CTITF focuses on amplifying "trusted voices", including information from state and local government officials, community leaders, and associations to combat misinformation. Social media platforms are not included as "trusted voices" (CFI Task Force | CISA n.d.). The unilateral means the public sector utilizes in addressing disinformation and misinformation is another point that is in contention with a multi-stakeholder framework that focuses on information sharing.

As noted above within the literature review, this public sector ideal regarding information discourse is in contention due to the divergent motives within private-public partnerships (Carr 2016; Christensen and Petersen 2017; Prince and Lacey 2018). The

public and private sector have demonstrated a limited willingness to engage in multi-stakeholder engagement and information sharing as the information they desire, and the entities is it shared with are in contention. As a result, there is no consensus on what the ideal framework for multi-stakeholder engagement would be. Despite the lack of consensus, actors within the framework have acted upon their own preferences for multi-stakeholder framework. The government has engaged in the establishment of cyber norms, such as the intolerable nature of targeting critical infrastructure and focus on the applicability of international humanitarian law in cyberspace and is beginning to demand further transparency from private sector actors, and the private sector is engaging with multi-stakeholder on its own term - going as far as unilaterally choosing to engage in international norm-setting bodies while the public sector does not. For example, the Paris Call for Trust and Security in Cyberspace is a set of norms that addresses behavior in cyberspace and was one of the first international works to specifically include a principle on how to defend electoral processes from cyber interference and influence. While private entities such as Microsoft and Facebook have signed on as supporters, the United States as a State has not joined other nations and its private sector partners in supporting the Paris Call. The role of free speech, and more specifically the ideal of Internet freedom, is further complicating the pursuit of electoral protection. While the public and private sector have each conveyed a strong desire to protect free speech online, each has its own preferences as to how to achieve that while ensuring electoral integrity.

T3b) The Role of Internet Freedom

Pushing private technology companies to limit and/or remove information perceived as misinformation, via government regulation, has implications to free speech that has shaped the private-public relationship. Despite fears over limiting Internet

freedom, public sector representatives still call for technology companies to stem the influx of misinformation, as described above in *T3a)*, through censorship. In the process, Section 230 of the Communications Decency Act, legislation that is at the center of this debate, has come under attack.

Section 230 states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". Fundamentally, this means that social medial platforms cannot be held liable for the content posted by their users, including misinformation and violent content (Section 230 of the Communications Decency Act n.d., 23). Supporters of Section 230, notably social media companies, claim that this fosters free speech by not putting companies in a position where they are overly censoring content to avoid legal risk. Additionally, supporters appreciate being able to moderate content when addressing risks, such as incitements of violence or information meant to undermine elections, without fear of legal action being taken against them. Testifying before the Senate Committee on Commerce, Science, and Transportation, Jack Dorsey, Chief Executive Officer of Twitter, testified that "We must ensure that all voices can be heard, and we continue to make improvements to our service so that everyone feels safe participating in the public conversation--whether they are speaking or simply listening. The protections offered by Section 230 help us achieve this important objective" (Big Tech Company's Liability Shield 2020). Advocates for Section 230 invoke the importance of Internet freedom and outline their efforts to combat misinformation and other harmful content to avoid government overreach that would come with the repeal of Section 230. When discussing Section 230, public sector actors, such as members of the United States

Congress, are also consistently invoking this same principle regarding freedom of speech online, however, they see Section 230 as stifling it rather than nurturing it.

In the same hearing in which Jack Dorsey testified, Senator Roger Wicker (R-Mississippi) justified this investigation into the problems of Section 230 by stating "Reasonable observers are left to wonder whether big tech firms are obstructing the flow of information to benefit one political ideology or agenda. My concern is that these platforms have become powerful arbiters of what is true and what content users can access" (Big Tech Company's Liability Shield 2020). Individuals like Senator Wicker, acting on behalf of the public sector, are suspicious of the same moderation power that advocates for Section 230 see as necessary in mitigating harmful content. Following the events of 2016, conservative politicians in particular claimed that technology companies were moderating content in favor of liberal ideals (Bond 2020; Guynn 2020; Issac and Browning 2020). Former President Donald Trump has also stated his wishes to repeal Section 230 using the same rationale as his conservative counterparts (Hamilton 2020). Upon signing an executive order that threatened to penalize social media companies for supposedly exhibiting a bias against conservative content, former President Donald Trump justified his decision by stating "We're here today to defend free speech from one of the greatest dangers [...] In a country that has long cherished the freedom of expression, we cannot allow a limited number of online platforms to hand-pick the speech that Americans may access and convey online" (Sheth, Relman, and Gold 2020). Conservative politicians are not the only group who have advocated for the repeal, liberal politicians also see Section 230 as justification technology companies use in dodging their responsibility of moderating misinformation and other harmful content.

In his opening statement for a hearing regarding the role Section 230 plays in spreading disinformation, Representative Mike Doyle (D - Pennsylvania) stated, "And while a number of websites have used 230 for years to remove sexually explicit and overtly violent content, they have failed to act to curtail the spread of disinformation. Instead, they have built systems to spread it at scale and to monetize the way it confirms our implicit biases".

Despite holding different fundamental reasons for repealing Section 230 than conservatives, Representative Doyle still invokes the importance of free speech online: "Freedom of speech is a fundamental right upon which our democracy is built, and we must make sure these companies are now policing the free flow of speech, especially when it comes to political discussions as they continue to operate online platforms" (Hearing Disinformation Online and a Country in Crisis 2020). President Joe Biden has also advocated for the repeal of Section 230 (Lerman 2021).

From social media companies to conservatives to liberals, the importance of free speech in online communication is a constant theme in their support or opposition of Section 230, despite their varying views. Social media companies see Section 230 as a way to ensure free speech and allow for content moderation that avoids harm to the public. Conservatives fear Section 230 has curbed free speech by allowing technology companies to moderate content in accordance with certain political ideologies without fear of legal liability. Finally, liberals see Section 230 as a shield that social companies have wielded to avoid addressing harmful content and thus preventing the generation of "healthy free speech" online. While the unified goal of protecting free speech represents an important domestic norm, the debate over the protection of free speech has demonstrated a divisive multi-stakeholder model in which each sector has its own ideas of how to best achieve

electoral protection. Consequently, the idealized multi-stakeholder framework members of both the public and private sector have advocated for is yet to be realized. Domestic norms regarding Internet freedom serve an important role in what norms the United States choose to engage and not engage with. At the same time, the fractured multi-stakeholder model, largely driven by debates over that same ideal of Internet freedom, are also observable in international norm-setting bodies.

CHAPTER 3: Analysis of International Engagement

This chapter examines how the domestic norms observed in Chapter 2 have become a part of global cyber norms. Although the norms that emerged out of the previously discussed themes are present within several international contexts, they are not present to the same extent. The United States was able to successfully advocate for its normative values, related to critical infrastructure protection, on the international stage specifically within the UN GGE. As a part of critical infrastructure protection norms, the United States was able to establish the applicability of international law and thus solidify its normative desire to have voluntary standardization as a part of international cyber norms. While critical infrastructure's role in the UN Group of Governmental Experts (GGE) is the most obvious demonstration of the United States' norms being projected in international bodies, the UN Open-Ended Working Group (OEWG), the Paris Call, and the Global Commission contain United States' norms that were both purposefully advocated for, as well as those that are involuntary reflections of the United States' cybersecurity practices. The norms the United States advocated for, and are still hoping to gain international legitimacy for, are those related to the applicability of the international law of State responsibility and international humanitarian law. The Paris Call and Global Commission embody the domestic shortcoming of the multi-stakeholder

framework and demonstrate its presence in international norm-setting bodies. Furthermore, the private sector was able to push more norms with a technical focus within the Paris Call and the Global Commission, specifically those dervied from the NIST Cybersecurity Framework and principles of software independence. This chapter discusses these American norms that were elucidated in the following ways: (1) through engagement with the UN GGE; (2) through the conflict that came with the creation of the Russia-led UN OEWG; and (3) through private sector and civil society efforts to influence cyber norms in the Paris Call and the Global Commission.

The successful publication of the 2015 UN GGE Report on Developments in the Field of Information and Telecommunications in the Context of International Security solidified norms the Unites States had long fought for, among them, the recognition that international laws are applicable in cyberspace and the importance of establishing norms surrounding critical infrastructure protection (Marks 2015; Maurer et al. 2020). However, this was only the beginning in establishing norms that represented the United States' interests. As the UN GGE process progressed, electoral protection from cyberattacks would become a more pressing issue and would give rise to further norms. While norms such as critical infrastructure protection and the applicability of international law would remain prominent with regard to electoral protection, these norms would transform, and others would be included as the UN GGE continued its discussions.

The UN GGE is not the only place where we observe themes from the United States' cybersecurity practices. Despite the UN GGE being one of the first international bodies to formulate cyber norms, the UN OEWG, the Paris Call, and the Global Commission are other influential bodies in cyberspace where the United States' normative values are placed on display. Normative disagreements led to the eventual stalling of UN GGE

progress in 2017 and led to the creation of the UN Open-Ended Working Group (OEWG) as led by Russian efforts. As a result of this disagreement, more normative values of the United States became more apparent, such as an emphasis on free speech and the applicability of related international humanitarian law. Russia's interference into the 2016 United States Presidential Election also caused electoral protection and reverence for state sovereignty to become a divisive issue. The stalling of the UN GGE demonstrated the prominent role election protection plays in shaping cyber roles and how it factors into the United States' trepidation to reconcile its norms with those of States like Russia. In its opposition to a resolution put forth by Russia to counter the criminal use of information and communications technology, the United States justified its decision by stating the following:

"Given the Russian Federation's criminal misuse of information and communications technologies to undermine and violate the integrity of institutions including international organizations and sports organizations, as well as the sovereign democratic processes of UN member states, they are not the appropriate sponsor to be taking the lead of this topic."

United States Statement to the UN General Assembly (Explanation of Vote on a Third Committee Resolution on Countering the use of information and communication technologies for criminal purposes 2018). [26]

By specifically invoking Russia's history with electoral interference in "sovereign democratic processes" as justification to question the integrity of the resolution, the

[26] Additional authors on this resolution included Belarus, Cambodia, China, the Democratic People's Republic of Korea, Myanmar, Nicaragua, and Venezuela

United States demonstrated how strongly it reveres its own norms that are incompatible with Russia. In addition, the themes arising out of a complex relationship between the public and private sector would come to light in the Global Commission and the Paris Call in the form of norms that seek to demonstrate the important contributions the private sector can make to the creation of cyber global norms. This chapter shows that these norms, both those the United States has been successful and unsuccessful including in international norms, were not unexpected but are rather predictable when analyzing domestic cybersecurity practices surrounding electoral protection, as was done in Chapter 2.

Section 3.1: The United States and the UN Group of Governmental Experts

When the United States became a signatory on the 2015 UN GGE report, it was not a passive actor. The United States saw the UN GGE as an active way to push for key norms: the importance of critical infrastructure protection and the applicability of international law in cyberspace. These norms laid the groundwork for the themes that would be present in future United States participation in international norm-setting bodies, as well as the important role election protection would play in shaping the discourse.

Subsection 3.1.a) Protecting Critical Infrastructure

The 2015 UN GGE Report contains normative values that draw inspiration from those that have frequently been invoked in United States cybersecurity practices regarding critical infrastructure.[27] In its opening, the 2015 report notes critical infrastructure norms as being an important addition to the previous iteration of norms decided upon in 2013, "a state should not conduct or knowingly support ICT activity that

[27] For further information on the origin of the United States' critical infrastructure protection program, please see Appendix P

intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats" (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015).

The "measures" proposed in this report are the norms agreed upon by the signatories and bear resemblance to those present in United States cybersecurity practices, including information sharing and cooperation. Norm 13.h) states that nations should "respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious [information and communications technology] ICT acts". As discussed in Chapter 2, this kind of cooperation that transcends industry lines, or in this case national borders, is an important piece of the risk management strategy. At a domestic level, CISA-managed information sharing networks are the primary method of communicating and responding to threats across critical infrastructure stakeholders. As observed in the 2015 report, information sharing is a norm that the United States values beyond those domestic cybersecurity practices. The 2015 report goes further in establishing the importance of this norm in its Confidence-Building Measures, "States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders." Furthermore, it calls for "the development of mechanisms and processes for bilateral, subregional, regional, and multilateral consultations on the protection of ICT-enabled critical infrastructure" in Confidence-Building Measure 16.d) (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015). These are macro-level information sharing mechanisms that build upon

the ideas proposed within United States cybersecurity practices and make them applicable across international partnerships.

While information sharing is one key component of the NIST "respond" functionality, another is the normative value present related to training. The studied documents in Chapter 2 revealed that training critical infrastructure personnel, including poll workers and other election officials, in identifying threats and knowing the appropriate communication procedures is an important piece of the "respond" strategy. This theme is reflected in the 2015 report as well. International Capacity-Building Measure 21.d) states that "States should consider the following voluntary measures [...] to build capacity in securing ICTs", with one of the measures being the creation of "procedures for mutual assistance in in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance" (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015). Once again, this is a strategy employed by CISA in protecting critical infrastructure at the domestic level and is now being advocated for as an intentional norm. Risk management and critical infrastructure are, therefore, important concepts that transcend United States domestic practices. It is notable that on the international stage, there is a more of an emphasis on the "response" functionality of the NIST cybersecurity framework than is observed on the domestic level. This may be due to the fact that the "protect" functionality, which is highly featured in domestic United States cybersecurity practices, is more technical in nature and not suited to the structure of the UN GGE report, which is more focused on international partnerships. However, the technical nature of the "protect" functionality is

represented within the Paris Call and the Global Commission, which will be further discussed below.

The studied documents in Chapter 2, regarding non-voting infrastructure, draw significant influence from the NIST Cybersecurity Framework and thus critical infrastructure security guidelines at large. As a result, domestic cybersecurity practices regarding election infrastructure align with those used in critical infrastructure protection at large. The notable influence that domestic critical infrastructure practices have upon international norms indicates such themes will continue to play a role in shaping the United States' normative values on the international stage. Furthermore, critical infrastructure will not only be discussed as a field in general, but specifically invoke election infrastructure as a crucial example of critical infrastructure in need of protection. Preliminary publications that summarize the discussions surrounding the 2021 UN GGE report, point to attacks upon election infrastructure as being an emerging threat.[28] "State and non-State actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites" (Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security 2019).

Critical infrastructure themes from domestic cybersecurity practices are not only apparent in the international discourse the United States led through the UN GGE, but also indicate the growing importance of including election protection in this discussion. As observed in Chapter 2, guidelines that dictate proper election infrastructure security are extremely similar, if not completely copied, from those that concern critical

[28] The 2021 UN GGE report has yet to be published. Due to UN GGE meetings being closed to observers, information gleaned from this ongoing discussion is based upon preliminary reports published by the group and its experts.

infrastructure security at large. This means that when the United States discusses critical infrastructure, they are including election infrastructure indirectly in the discourse. The reliability with which domestic practices predict emerging themes on the international stage insinuates another outcome: election infrastructure will drive the international discussion on critical infrastructure protection and the related norms.

Subsection 3.1.b) The Applicability of International Law and Voluntary Standardization

The 2015 UN GGE report not only reinforced the United States commitment to critical infrastructure protection, but also its commitment to upholding international law in cyberspace. Michele Markoff, the United States tendered expert to the UN GGE, stated at the conclusion of the 2017 UN GGE session that "I have sought clear and direct statements on how international law applies to the States' use of ICTs, including international humanitarian law, international law governing States' exercise of their inherent right to self-defense, and the law of state responsibility, including countermeasures" (Markoff 2017). This statement demonstrates a desire to uphold these international laws in cyberspace, with a particular focus on humanitarian laws and the implications of State sovereignty: topics that have brought debates in the UN GGE to a head. The nature of this debate will be discussed in *Section 3.2*. For now, the implications of the United States' focus on international law are telling in itself.

The United States been an advocate for the applicability of international law in governing the "rules of the road" in cyberspace since the formation of the UN GGE, however, it is unclear why this is, until analyzing American domestic cybersecurity practices that exhibit a clear preference for voluntary regulation and guidelines. By

upholding international law as the governing norms rather than a formal treaty, the United States is able to exercise more freedom in how it conducts itself within cyberspace.

The relationship between international law and norms in cyberspace work in the following way: while adhering to international law, in general, can be thought of in more binary terms, as either violating or not violating some law, it is much more difficult to do so in the context of cyberspace. There are little international laws specifically concerning activities in cyberspace. Consequently, nations are left to develop norms regarding how to best interpret existing international law and make it applicable to cyber incidents.

As a result, the United States does not have to characterize cyberattacks within the framework of some binding treaty, but rather is free to interpret international law and resulting cyber norms to its discretion. This normative value of the United States is evident in several ways. As discussed in *Section 1 Subsection 1.1.b*, the Obama administration elected to not characterize the interference into the 2016 United States Presidential Election as a violation of international law. This was a normative judgement and demonstrates the freedom granted to the United States through the upholding of international law in cyberspace rather than a treaty. Additionally, this gives the United States leverage to pursue a "deterrence by punishment" strategy that has been utilized in past conflicts, such as the sanctions that were put in place after North Korean State-sponsored groups were found exfiltrating information, via cyberattacks, for their illicit weapon and missile programs (United States Department of the Treasury 2019).

Anders Henricksen, director of the Center for International Law, Conflict, and Crisis at the University of Copenhagen, characterizes the United States' dedication to upholding international law in cyberspace as a means to "maintain their superior position and to prevent other States from engaging in and what it perceives to be disruptive

activities". As demonstrated by the actions of the Obama administration, international law has been a method of the United States in maintaining flexibility and avoiding the "creation of new legal constraints" against its activities in cyberspace. As a result, the United States has managed to avoid serious discussions on adopting new treaties or new standards regarding cyberspace while imposing restrictions on other States (Henriksen 2019). The United States has solidified its position against regulations, particularly via treaties, in other areas of cyberspace including the UN resolution on *Countering the use of information and communications technologies*. The UN resolution proposed the drafting of a new treaty designed to control cybercrime to which the United States responded "despite intense debate, there is absolutely no consensus among Member States on the need or value of drafting a new treaty. Undertaking work on such an important issue through a divisive and non-inclusive process will not achieve a successful outcome or improve international cooperation". The response continued by reiterating the United States' lack of regard for this treaty: "any such treaty will be no more than a stack of paper without the endorsement of those Member States that are most frequently the recipients of requests for electronic evidence and international cooperation in cybercrime cases, including the United States" (Mack 2019).

The 2015 UN GGE report endorses the United States' desire to maintain flexibility via international law by stating that "The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible, and peaceful ICT environment" (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015).

As a leader in this UN GGE process and an advocate for international law in cyberspace, the United States is demonstrating ideals that can be traced back to its own cybersecurity practices. The NIST Cybersecurity Framework is the foundation of critical infrastructure security, and by extension, electoral protection. Despite the reverence cybersecurity professionals have for these standards, they remain voluntary. The Framework states the role of NIST is to "identify and develop cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators" in order to allow for "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" to cybersecurity professionals (National Institute of Standards and Technology 2018). The strength of the NIST Cybersecurity Framework lies in its ability to be adaptable, and that means presenting its best security practices as voluntary guidelines rather than requirements. This kind of flexibility is once again reflected specifically in domestic cybersecurity practices regarding electoral protection. Again, the NIST Cybersecurity Framework contains the guiding principles for securing electoral infrastructure due to its designation as critical infrastructure. Additionally, this flexibility is extended to electronic voting machine security. The decentralized accreditation system, as discussed above in *Theme 2a)*, allows states to remain flexible in how they integrate the EAC Accreditation Standards into its own state-wide practices. Some states require full federal accreditation, while others require none and instead rely upon standards developed within the state.

The norm of flexibility in domestic cybersecurity practices is also witnessed within the UN GGE as the United States pushes for the upholding of international law as a means of obtaining this flexibility in an international context. Domestic cybersecurity practices, especially as they relate to the foundational, voluntary NIST Cybersecurity Framework,

reveal the norms that will manifest on an international stage, as well as how electoral protection will play an important role. It likely the United States will continue advocating for norms and participating in international bodies that grant it the flexibility it is accustomed to domestically. Furthermore, the issue of electoral protection will continuously be one that the United States will desire to have autonomy over and will benefit from international law's applicability in cyberspace. When a foreign adversary electronically interferes in elections, the United States does not want to be bound to a treaty, but rather be able to punish as it sees fit. These norm and ideals observed domestically are once again observable on the international stage. Although the United States was successful in establishing its normative values surrounding critical infrastructure, it faced opposition to its other norms with the creation of the UN OEWG.

Section 3.2: Tensions with Russia - Electoral Interference and the UN Open-Ended Working Group

The norms that have caused tensions, and ultimately led to the stalling of the UN GGE and creation of the Russian-led UN OWEG, center upon differing interpretations and applicability of the international law of State responsibility and international humanitarian law in cyberspace.[29] United States Expert to the UN GGE Michele Markoff's statement detailing the failure of the UN GGE to come to a consensus in 2017 notes contention arose regarding "certain bodies of international law, including the *jus ad bellum*, international humanitarian law, and the law of State responsibility" (Markoff 2017). The clash between United States and Russian ideals elucidates norms held by the United States and shows that the domestic cybersecurity practices analyzed in *Chapter 2* were predictive of the norms that ultimately led to this divisiveness.

[29] The norms articulated in the UN OEWG are contained in Appendix I

Subsection 3.2.a) International Law of State Responsibility and Cyber Attacks as "Armed Attacks"

The international law of State responsibility is articulated in the Articles on the Responsibility of States for Internationally Wrongful Acts, adopted in 2001 by the International Law Commission. The Articles contain the principles governing when and how States are held responsible for breaches of international obligations (Responsibility of States for Internationally Wrongful Acts 2008). The United States maintains it position that cyberattacks can warrant a state of *jus ad bellum:* the conditions under which a state may respond to a breach of international responsibility, as defined by the Articles, with armed force or other activities usually barred by international law. Thus, this implies that the United States believes it is justifiable in the proper instances to respond to cyberattacks with armed attacks and/or retaliatory cyberattacks, especially when it targets systems so vital to society as critical infrastructure (Grisby 2015; Henriksen 2019; UN GGE on Cybersecurity n.d.). Markoff articulates this norm in her statement:

"A report that discusses the peaceful settlement of disputes and related concepts but omits a discussion of the lawful options States have to respond to malicious cyber activity they face would not only fail to deter States from potentially destabilizing activity, but also fail to send a stabilizing message to the broader community of States that their responses to such malicious cyber activity are constrained by international law"

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 (Markoff 2017)

Markoff emphasizes the importance of the "lawful options" (i.e., armed counterattacks that would normally be breaches of international law) afforded to states in an environment of *jus ad bellum* in order to provide stability in cyberspace and constrain malicious activity, such as cyber election interference and influence.

In order to understand what the United States' norms, it is also necessary to understand the views they are reacting to, namely those of Russia. The norms Russia upholds are reflected in is participation in the UN OEWG. In its commentary on the "Pre-draft" of the UN OEWG Final report, to be published at the end of 2021, Russia makes clear its objection to cyberattacks being contextualized as a tool in warfare as the United States has seemingly done in stating. In Russian's commentary, it justifies it stance by stating it is "potentially dangerous [...] to impose the principle of full and automatic applicability of [international humanitarian law] to the [information communication technologies] ICT environment" (Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the UN OEWG 2019).[30] Russia and the United States fundamentally disagree on whether or not cyberattacks are instruments of warfare, and whether such acts are consequently subject to international law that governs activities of war. The United States' domestic cybersecurity activities indicated as much with the significant emphasis it places on critical infrastructure protection.

The establishment of critical infrastructure, and its cybersecurity practices, as a prevalent component of American society demonstrates how the United States perceives cyberattacks upon critical infrastructure: an action that can be treated as an act of war. The cybersecurity practices discussed in Chapter 2 reflect the severity with which the

[30] International humanitarian law includes principles related to *jus ad bellum* and the law of State responsibility as well as those related to freedom of information and communication; the latter will be covered below in *Subsection 3.2.b)*

United States treats attacks upon its critical infrastructure and its mission to protect against those attacks. As noted previously, the risk management structure used to secure critical structure is one that spans several federal agencies, has been adopted in federal standardization documents, and has been deployed on a level as granular as election infrastructure protection. Calls for critical infrastructure security are so pervasive in American society, that those security polices, originally specific to critical infrastructure as contained within the NIST Cybersecurity Framework, provide the most revered standards in cybersecurity beyond critical infrastructure.[31]

The conflict between the United States and Russia, regarding the UN GGE and UN OEWG division as well Russia's interference into the 2016 United States Presidential Election, emphasizes the United States' normative judgement that cyberattacks can be perceived as an extension of warfare. The value the United States holds in its ability to respond to cyberattacks as if they were the traditional definitions of armed attacked, as defined in international law, stems from its cybersecurity practices. The concern over critical infrastructure security has warranted an image of cybersecurity within the United States that Russia has characterized as the unjust militarization of cyberspace. For its part, the United States has upheld the practices as discussed in Chapter 2 and continues to seemingly live up Russia's perception that the United States sees cyberspace as a potential military zone and is interested in applying the appropriate international laws. The United States intelligence and defense community play an active role in safeguarding election infrastructure, and critical infrastructure at large. At the center of these norms, election security is continuously serving as a motivating example that all parties on the

[31] A Russian state-sponsored campaign to compromise critical infrastructure illustrates the severity with which the United States treats attacks upon its critical infrastructure and how it might equate such an event to a justification of *jus ad bellum*. This incident is described in Appendix Q.

international stage are concerned with. In addition to being key in United States' norms on the law of state responsibility, the issue of safeguarding elections from cyber threats has manifested in another source of conflict between the United States and Russia: the balance between free speech and security.

Subsection 3.2.b) International Humanitarian Law and Internet Freedom

The applicability of international humanitarian law was another point of disagreement cited in Markoff's statement. As such, it represents another important norm valued by the United States: the significance of Internet freedom. Although the United States does not specifically invoke the importance of Internet freedom in Markoff's statement, the reference to international humanitarian law is particularly concerned with this aspect, as evidenced from additional studies of United States ideologies throughout the international norm formulation process and Russia's contrasting norms. In 2012, the United States demonstrated its dedication to preserving Internet freedom at the Internet Telecommunication Union's World Conference when it refused to sign treaty amendments to the 1998 International Telecommunications Regulations for fear of over-government regulation in cyberspace. If adopted, the amendments would have allowed governments to restrict the proliferation of online content that threatens state stability, specifically that stemming from foreign governments (Henriksen 2019).[32]

The 2015 UN GGE report signed by the United States also emphasized the inexorable tie that human rights have to Internet freedom and reaffirmed an international obligation to uphold the preservation of this freedom. The Human Rights Council resolutions mentioned are discussed in further detail within Appendix R:

[32] Henricksen characterizes the West's proclivity for Internet freedom's inclusion in international humanitarian law by stating that, in the West, "cyberspace is considered an important tool for spreading - and at times even securing - human rights, such as freedom of expression."

"States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression".

(Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015).

Russia has framed Internet freedom's role, not within the field of cybersecurity, but rather as an issue of information security centered around State sovereignty. The free flow of information is thought of as a tool of political subversion in Russia. Consequently, discussion allowing for this free flow of information is equated as threats to Russia's sovereignty (Ford 2010; Henriksen 2019). While the 2017 UN GGE's failures to produce a consensus report was partially attributed to differing norms between the United States and Russia regarding Internet freedom's applicability through cyber norms, it has also caused problems for Russia within the UN OEWG. Russia, in its belief that international humanitarian law (specifically concerned with Internet freedom) is unfairly being made applicable through cyber norms, commented on the pre-draft of the UN OEWG report that, "Considerable number of questions, which are not directly related to the problem of ensuring international peace and security (issues of the UN First Committee) are unreasonably included in the “pre-draft” of the report". The statement goes further in characterizing references to the protection of human rights as "redundant" (Commentary of the Russian Federation on the Initial “Pre-Draft” of the Final Report of the UN OEWG 2019). Through this comment, Russia conveys that, issues of human rights, among others,

are best left to other international bodies not concerned with cyberspace. Russia also made clear its disdain for the inclusion of Internet freedom, and larger humanitarian concerns', in its competing 2017 UN GGE. There, it affirmed the "right and duties of states to combat, within their constitutional prerogatives the dissemination of false and distorted news, which can be interpreted as interference in the internal affairs of other states as being harmful to the promotion of peace, cooperation and friendly relations among states and nations." In response, the United States issued its resolution that strongly emphasized "the necessity of an open, interoperable, reliable and secure information and communication technology environment, consistent with the need to preserve the free flow of information" (De Tomas Colatin 2018).

The conflict regarding Internet freedom's role in regulation cyberspace via norms not only highlights important themes in the United States' engagement on these issues, but also can again be tied back to domestic cybersecurity practices. Specifically, cybersecurity practices regarding electoral protection are pertinent as the strong desire to uphold Internet freedom has been exemplified through United States' domestic discussion on misinformation and disinformation during elections. As discussed in *Chapter 2*, Internet freedom has been at the center of the debate regarding one of the most discussed threats to the democratic process: misinformation. Vying opinions regarding how to best regulate misinformation spread on large social media platforms has become significant in election security debate. However, despite different solutions being advocated on behalf of the private and public sector, there remains a deep concern with protecting freedom of speech online. It is telling that despite differing political parties, industry affiliations, and ways in which misinformation has affected their respective sectors, the public and private sector both still affirm their devotion to maintaining

Internet freedom. The United States upholds its devotion to Internet freedom throughout the international norms-formulation process as strongly as it does on a domestic level. Consequently, it become a divisive enough issue to warrant the creation of the UN OEWG. As the UN GGE and UN OEWG continue their respective processes, it is possible that the deep ties that misinformation and disinformation regulation have to electoral protection will ensure the issue of election integrity maintains its importance in the cyber norm creation process. Therefore, electoral protection from cyberattacks will not only continue to be a critical issue in the international cyber norms process, but also demonstrates the prevalence of its cybersecurity practices in elucidating United States' norms. With that being said, tensions with Russia are not the only obstacles the United States faces in pushing a cohesive normative agenda as its own private sector and civil society have pursued other means of getting its norms noticed.

Section 3.3: The Private Sector and Civil Society in Norm Development - A Fractured Multi-Stakeholder Framework

Domestically, the United States has struggled to introduce a multi-stakeholder framework that effectively involves the public sector, the private sector, and civil society in the electoral protection process resulting in the same fractured multi-stakeholder framework is evident on an international level. While it is telling in itself that the multi-stakeholder framework is not effective internationally, the unilateral manners in which the public sector, the private sector, and civil society choose to advocate for their own preferences reveals additional norms that are also evident within the United States' domestic cybersecurity practices. The private sector and civil society have chosen in engage in the Global Commission and the Paris Call to exercise unilateral power in norm-formulation processes, especially those that allow the private sector to establish norms

that require its technical expertise. Through the Global Commission, these non-state actors are able to assert the importance of their role in cyber global governance through the norms they produce. Furthermore, the Paris Call has been an organization in which the private sector and civil society can generate widespread participation and proliferate norms. On the other hand, the public sector within the United States advocates for its normative preferences within the UN GGE by not seeking to engage the private sector and civil society within this body and instead using the UN GGE to push state-held normative values, such as those pertaining to critical infrastructure protection.

Despite the inability to produce a consensus report in 2017, the UN GGE is still the primary group the United States government choses to engage with in both shaping cyber norm and responding to opposing norms arising out of the UN OEWG. However, the private sector and civil society have not been engaged within the UN GGE. Only after the failure of the 2017 UN GGE to reach a consensus report was there serious discussion on involving groups outside the public sector (Hinck 2018). By analyzing private sector and civil society involvement in the Global Commission and the Paris Call, the following domestic norms became observable in an international setting: (1) a stated desire for collaboration with the United States government, with no private sector action to support this ideal; (2) a recognition of non-state actors' importance in shaping and upholding cyber norms due to the technical services they provide; and (3) an emphasis on the implications cyber norms have for ensuring electoral protection. I discuss these norms in the context of the Paris Call and the Global Commission.

Subsection 3.3.a) The Paris Call for Trust and Security in Cyberspace

The Paris Call was largely spearheaded by Microsoft after expressing frustration with the lack of consensus between state actors and the hope of fostering more wide-

spread cooperation. Despite American private sector participation, the United States is one of the few Western nations to not sign the Paris Call.[33] Microsoft Vice President for UN Affairs, John Frank, characterized the Paris Call as an effort meant to bring together supporters who are "committed to working together in a multi-stakeholder model, with governments, industry, academia and civil society collaborating to protect our cyberspace from nation-state threats, including attacks on our democratic processes" (Frank 2019b). Nicklas Lundbald, a Google Vice President, also affirmed this belief stating that, "Strong security is the cornerstone of everything we do at Google. We support the Paris Call for Trust and Security in Cyberspace, because as security threats evolve, continuous collaboration with the industry and with governments is the best way to protect users and help create a more secure Internet for everyone" (Beavers 2018). Domestically, the private sector has also called upon government partnerships in addressing issues surrounding cyber norms. However, as also observed domestically, private sector and public sector partners have yet to establish a framework in which they can cooperate with one another despite rhetoric indicating their desire to do so.

Additionally, private sector involvement in the Paris Call has exemplified the emerging role of electoral protection in international discourse. The importance of protecting elections from cyber threats has quickly become not only a vital aspect of cyber norms but a motivating factor behind the creation of international bodies including the Paris Call. Microsoft President Brad Smith stated the Paris Call represents a "watershed moment, bringing together stakeholders from around the globe to protect our electoral processes, not just governments, but the leading institutions that collectively represent the fabric of the world's democracies" (Beavers 2018). The focus on electoral protection

[33] For further information on why the United States may not have signed the Paris Call, see Appendix S

has caused the emergence of two commissions related to the Paris Call: The Transatlantic Commission on Election Integrity and Microsoft's Alliance for Securing Democracy. Both of these commissions are collaborative efforts meant to inform election officials of the electronic tools used to conduct interference into elections and what can be done to protect against these attacks. Electoral protection's role in cyber norms is solidified in Principle 3 of the Paris Call: Defend the Electoral Process. Principle 3 urges its signatories to "strengthen its capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities" (The Paris Call of the 12 November 2019 — Paris Call 2019).

The salience of norms surrounding electoral protection within the Paris Call demonstrates the inevitable focus that will be devoted to the prevention of cyberattacks that threaten democratic processes. In the domestic analysis of cybersecurity practices, cyber threats to elections have been insinuated as an emerging topic, while on the international stage this future is undeniable. The unilateral effort by the private sector to effect change on this issue embodies an additional domestic norm: the private sector's belief that it has a key role in protecting Internet freedom. In this case, Internet freedom is inexorably tied to the ability of all Americans to participate in elections freely and fairly. The private sector, in its view, has the best technical tools in combatting the misinformation that threatens this ideal of free and fair elections. Additionally, it has decided that it has not only a technical role to play in this endeavor, but a duty to participate in governance as well. Participation in the Global Commission exemplifies the norms discussed in this section, while also focusing on particular nuances that arise out of more significant participation from civil society. As a result of civil society's more active

role in the global commission, there is a focus on restraining non-state actor behavior in addition to endorsing the norms evident within the Paris Call and the UN GGE.

Subsection 3.3.b) The Global Commission on Stability in Cyberspace

The origins of the Global Commission, coupled with its commissioners predominately being representatives from civil society, introduces new nuances to the norms it endorses including emphasizing the important role non-state actors have in securing cyberspace and the need for more technical specifications being incorporated in cyber norms. Despite the new norms advocated for, the Global Commission still explicitly endorses the norms included in the 2015 UN GGE report and, most importantly, accepts the applicability of international law in cyberspace and the significance of protecting critical infrastructure. While the private sector may not have as active as a role in the Global Commission, their norms and preferences are evident, nonetheless. Microsoft and Google are funders of the Global Commission indicating private sector actors are still interested in seeing these specific norms upheld. As evidenced by participation in the Paris Call, private sector actors endorse norms that communicate the dominance of non-state actors in cyberspace as well as those that focus on electoral protection - norms that are also endorsed by the Global Commission (Maurer et al. 2020).

Civil society and the private sector converge upon a common acknowledgement in the Global Commission: the substantial role non-state actors have in upholding stability in cyberspace. The private sector uses this acknowledgment to justify its belief that assurance of cyber norms on their platforms, such as managing misinformation that threatens electoral integrity, is a task it is well-equipped to handle without government intervention. In Chapter 2 of this thesis, the private sector conveyed its preference for non-government intervention in the context of Section 230 of the Communications

Decency Act. Per Section 230, the private sector can more easily moderate content in order to cultivate free speech that is not sullied by disinformation efforts. Civil society comes to a different conclusion upon acknowledging non-state actors' undeniable role in cyberspace: norms need to specifically standardize control over non-state actors if stability is to be achieved.

In its final report, the Global Commission makes clear the distinction between the norms proposed by the UN GGE and its own norms by stating the differences lies in the Global Commission's belief that, "responsibilities should be imposed on non-state actors as well, as they must exercise restraint or take affirmative steps to ensure the stability of cyberspace." Norm 8 in the Global Commission's final report clarifies this ideal in stating, "Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur" (Advancing Cyber Stability: Final Report 2019). Civil society made clear its preference for salient norms, that are endorsed by the federal government, when it advocated for normative solution to electoral protection within Congressional hearings as previously noted. Leaders in the civil sector continuously advocated for global norms that acknowledged the importance of cooperation between the public and private sector.

The Global Commission also built upon UN GGE norms through its inclusion of technical norms.[34] While the UN GGE norms are more general in their scope, the norms proposed by the Global Commission include more concrete, technical steps organizations can take to promote cyber stability that are derived from American domestic practices related to the NIST Cybersecurity Framework and the principle of software independence.

[34] The Global Commission's norms are included in Appendix H

The technical norms are inspired by the recognition that the Internet contains the public core of society since it ensures widespread communication society depends upon. The Global Commission defines the public core as being "critical elements of the infrastructure of the Internet as packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers". In other words, the technological elements that allow the general population to reliably and safely use the Internet comprise the public core.

As such Norm 1, is entitled "Non-Interference with the Public Core" and states that no actor should facilitate activity that "substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace" (Advancing Cyber Stability: Final Report 2019). Safeguarding the Internet and all the vital activities it facilitates reveals norms that were evident within the United States' cybersecurity practices: the need to "identify", "protect", and "report" in protecting from Internet-enabled cybersecurity attacks.

The risk management framework that is foundational in United States' domestic cybersecurity practices noted that to "identify" in a network structure is to take note of the assets within that structure and its capabilities in order to understand the threat posed to the organization overall; this is in accordance with the highly influential NIST Cybersecurity Framework. The Global Commission recognizes the vital role the public core of the Internet plays while simultaneously acknowledging the malicious activities that can be facilitated via the Internet. Hence, the Global Commission seeks to identify the possible points of attack within the Internet that stem from a supply chain structure. In the supply chain, the public core is only able to support communications and other activities through third party communication tools, which often host vulnerabilities that

can be exploited and thus threaten the public core of the Internet. For example, the 2015 Russian cyberattack upon Ukraine's power grid exploited the supervisory control and data acquisition (SCADA) system to deprive over 235,000 people of power (Zetter 2016). The Global Commission characterizes this as violation of Norm 3 as the power outage exploited and rendered infrastructure inoperable that consequently affected access to the public core of the Internet. Furthermore, it was accomplished via third party tool. (Advancing Cyber Stability: Final Report 2019).

As additionally observed in *Chapter 2*, cybersecurity postures that detail technical specifications focus on the "protect" functionality of the NIST Cybersecurity Framework. The Global Commission norms are no different. In striving for the protection of the public core, the Global Commission advocates for the protection measures that specifically target packet routing and forwarding technologies, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers. Protection mechanisms specified in the Global Commission's *Advancing Cyber Stability* report bear similarity to those that are advocated for on a domestic level within the United States. For example, KWIC analysis conducted in *Chapter 2* revealed that proper authentication and role-based privileges are prevalent priorities in domestic cybersecurity practices, meaning that individuals should have their identity properly authenticated and have that be used in determining what information is accessible. Norm 1 echoes this norm in stating that the cryptographic keys used to identify users and the underlying equipment comprise the public core and thus entities have an obligation to do all in their power to protect these assets form exploitation.

Norm 5 of the Global Commission's report articulates the "report" functionality the NIST Cybersecurity Framework describes. In pursuit of the protection of the public core

and recognition of the underlying interconnectedness, Norm 5 urges States to create "procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities". Although Norm 5 recognizes disclosure can be detriment to state security, it nonetheless asserts that "the default presumption should be in favor of disclosure" (Advancing Cyber Stability: Final Report 2019). Cybersecurity practices within the United States revealed a particular interest in best reporting practices that are tied to transparent auditing procedures. For example, the principle of software independence has continuously been used to justify the need for paper-based auditing systems in verifying elections results. Software independence asserts that software has a tendency to be non-transparent and susceptible to technical mishaps that can go unnoticed. Furthermore, the Global Commission recognized the United States' leadership in endorsing this practice through its Vulnerability Equities Processes (VEP), a framework used in determining whether the United States government disclose the presence of zero-day vulnerabilities: those vulnerabilities that are largely unknown by the entities it could affect until the vulnerability has been exploited. Norm 5, while arguing for this transparency, once again notes its particular importance given the supply chain structure that defines the public core: an undisclosed vulnerability in one facet of the supply chain has the potential to compromise the general population's ability to use the Internet.

The nuances introduced by the Global Commission are included among norms that are familiar in the international norms-formulation process. Among these familiar norms are those that recognize the private sector's vital role in shaping and upholding cyber norms concerned with electoral protection. On the latter norm, the Global Commission, like the Paris Call, introduces Norm 2 that states no actor should "support or allow cyber

operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites." The Global Commission does not make any affirmative claims whether attacks upon electoral infrastructure are breaches of international law, however, it states that "election interference is intolerable whether it is considered to be a violation of international law or not"(Advancing Cyber Stability: Final Report 2019). The dedication to electoral protection, through the Global Commission, further demonstrates the highly influential role that elections play in forming norms. Additionally, regardless of the private sector and civil society's disagreement over the exact extent of the private sector's role in cyber norms development, the role of the non-state actor is an emerging norm that has inspired new international bodies.

Conclusion

Analysis of domestic cybersecurity practices revealed the norms that the United States values. Most prominently, the cybersecurity culture surrounding critical infrastructure security divulged key norms that dominate the domestic and international cyber norms landscape. The United States has a preference for standardization across critical infrastructure that extends to the issue area of electoral protection. An important caveat to the nature of standardization in the United States is that it is valued insofar as it is voluntary. The voluntary nature of standardization translated to the United States' desire to see international law upheld in cyberspace, not because of the strict guidance it offers, but rather the flexibly it allows in interpretation. Consequently, the United States feels it still has the ability to respond to cyber conflict in a way it best sees fit. Furthermore, the risk management strategy associated with critical infrastructure protection elaborated upon the specific technical elements the United States has an interest in protecting from cyberattacks. By designating election infrastructure as critical infrastructure, the key

facets of critical infrastructure security became applicable to electoral protection, including those related to standardization and the United States' preferred risk management framework.

The United States was most effectively able to implement norms it holds in relation to critical infrastructure security on the international stage. The 2015 UN GGE Report contained norms that were nearly identical to those the United States uses to ensure critical infrastructure security. Additional third-party research also corroborated this finding that the 2015 UN GGE Report reflected the United States' success in gaining recognition for norms regarding the importance of protecting critical infrastructure. While the normative values extracted from critical infrastructure domestic practices were the most salient, other norms were evident on the international stage.

Norms related to the United States' unique usage of electronic voting machines were pervasive. The decentralized nature of voting machine accreditation highlighted once again how much the United States values the voluntary nature of standardization, and by extension, the ability to interpret international "standards" to best suit the circumstances. The rising norm regarding software independence also highlighted the rising importance of transparency that is not dependent solely upon software. In pursuing this norm, the United States demonstrated its normative desire for verifiable results that technology was or was not subjected to cyber interference. The international norms that stem from software independence, however, were not as evident from a public sector perspective, but rather a private sector one.

The theory behind software independence inspired the private sector to apply this ideal and make it relevant on the international stage, within the Global Commission, by incorporating specific technical norms that called for the physical auditability of cyber

systems. This normative desire, however, was only one of many norms that the private sector chose to pursue. In attempting to legitimize its own normative preferences, the private sector revealed important norms that would not be as apparent if I were to only focus on public sector actions. For example, there is the fragmented nature of the multi-stakeholder framework. Despite public and private sector actors advocating for multi-stakeholder engagement on a domestic level, that ideal has yet to come to fruition. Instead, on a domestic level, the private and public sector disagree were observed disagreeing and ultimately have been unable to come to a consensus as far as what each actor should be doing to protect electoral integrity - specifically, what each actor should be doing to combat misinformation. The multi-stakeholder framework remains an elusive solution on the international stage as well, as evidenced by private sector and civil society participation in the Global Commission and the Paris Call that engenders unilateral action. Through the Global Commission and the Paris Call, the United States private sector has demonstrated its devotion to building cyber norms that specifically ensure electoral protection, a desire for the acknowledgement of non-state actors' roles in the assurance of cyber norms, and consequently, the establishment of cyber norms that leverage the private sector's technical expertise to achieve security. The disconnect between public and private sector actors' methods of shaping cyber norms are not the only sources of conflict in solidifying global norms.

Conflict arising out of the UN OEWG's formation has impeded the United States' ability to legitimize its norms. As a result, the normative values that uphold the applicability of international humanitarian law (specifically the ideal of Internet freedom) and the international law of State responsibility are yet to be solidified in far-reaching normative bodies. It is important to recognize this barrier in understanding the future of

cyber global governance. Not only does the conflict exemplify the United States' attempt to gain international recognition of its norms, but it also represents a hurdle to achieving cyber global governance. The United States and Russia are major cyber powers that lead two of the most influential norm-development bodies and have yet to recognize one other as a potential partner. Rather, major world powers have spent political capital asserting the superiority of one set of norms over another. The path to cyber global governance is complicated further by the fractured multi-stakeholder model that exists between the public and private sector.

Despite the apparent lack of cooperation, cyber norms continue to proliferate and remain an undeniable tool in assuring stability in cyberspace. The stakes are high, as the future of electoral protection and the defense of democracy relies upon the successful implementation of cyber norms. This work demonstrated the up-and-coming role that electoral protection has played in influencing the development of cyber norms. Electoral interference in the 2016 United States Presidential Election spurred unprecedented action. Safeguarding elections is such an important goal in cyberspace that it is not only invoked as motivating example in the UN GGE and the UN OEWG but has also warranted the creation of cyber norms specific to the protection of electoral integrity. The road to cyber global governance can lead to the further assurance of free and fair elections, however, this is only one of many implications. Actors from all sectors and nations have interest in seeing cyber norms established and this work means to show that understanding how we as an international community reach that point is vital if we are to protecting our democratic institutions.

Bibliography

Advancing Cyber Stability: Final Report. 2019. The Global Commission on the Stability of Cyberspace. http://cyberstability.org/report/ (March 6, 2021).

Alabama: Examination and Certification of Equipment. 2008. 17–23 17.

Alvarez, R. Michael, Thad E. Hall, and Susan D. Hyde. 2008. *Election Fraud: Detecting and Deterring Electoral Manipulation*. Washington DC, UNITED STATES: Brookings Institution Press. http://ebookcentral.proquest.com/lib/ucb/detail.action?docID=472668 (November 24, 2020).

Anderson, Brian, and John Mutch. 2011. *Preventing Good People From Doing Bad Things: Implementing Least Privilege*. Apress. https://ucblibraries.skillport.com/skillportfe/main.action?assetid=RW$45523:_ss_book:43819#summary/BOOKS/RW$45523:_ss_book:43819 (January 31, 2021).

Bahnke, Josie, and Christopher Krebs. 2018. "Your Vote Is Safe: How Alaska Is Partnering with DHS to Protect Elections."

Beavers, Olivia. 2018. "US Tech Companies Back Paris Cyber Agreement Opposed by Trump Administration | TheHill." *The Hill*. https://thehill.com/policy/cybersecurity/416465-us-tech-companies-back-paris-cyber-agreement-that-us-wont (March 1, 2021).

Big Tech Company's Liability Shield. 2020. (Senate).

Bond, Shannon. 2020. "Conservatives Flock To Parler App, Claim Censorship On Facebook And Twitter : NPR." *National Public Radio*. https://www.npr.org/2020/11/14/934833214/conservatives-flock-to-mercer-funded-parler-claim-censorship-on-facebook-and-twi (February 14, 2021).

Brown, Matthew. 2020. "Fact Check: Georgia 'suitcase' Video Is Missing Context." *USA TODAY*. https://www.usatoday.com/story/news/factcheck/2020/12/14/fact-check-georgia-suitcase-video-missing-context/3892640001/ (February 2, 2021).

Burr, Richard et al. 2018. "SELECT COMMITTEE ON INTELLIGENCE." : 104.

Business, in News et al. 2018. "The Fight Against Disinformation in the U.S.: A Landscape Analysis." *Shorenstein Center*. https://shorensteincenter.org/the-fight-against-disinformation-in-the-u-s-a-landscape-analysis/ (October 6, 2020).

Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92(1): 43–62.

Casey, Carter et al. 2019. *Recommended Security Controls for Voter Registration*. MITRE.

"CFI Task Force | CISA." https://www.cisa.gov/cfi-task-force (February 23, 2021).

Chayes, Abram, and Antonia Handler Chayes. 1995. *The New Sovereignty: Compliance with International Regulatory Agreements*. Cambridge, Mass: Harvard University Press.

Chertoff, Michael, and Anders Fogh Rasmussen. 2019. "The Unhackable Election: What It Takes to Defend Democracy - ProQuest." https://search-proquest-com.colorado.idm.oclc.org/docview/2161593917/3E13F22C778B4F36PQ/7?accountid=14503 (September 9, 2020).

Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. 2017. "Public–Private Partnerships on Cyber Security: A Practice of Loyalty." *International Affairs* 93(6): 1435–52.

"Commentary of the Russian Federation on the Initial 'Pre-Draft' of the Final Report of the UN OEWG." 2019.

De Tomas Colatin, Samuele. 2018. "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace." https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/ (February 14, 2021).

DiMaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2): 147–60.

Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Panel I. 2017. (Senate).

Dutta, Upasana et al. 2020. "Analyzing Twitter Users' Behavior Before and After Contact by the Internet Research Agency." *arXiv:2008.01273 [cs]*. http://arxiv.org/abs/2008.01273 (October 12, 2020).

"Election Infrastructure Security | CISA." https://www.cisa.gov/election-security (January 14, 2021).

"Explanation of Vote on a Third Committee Resolution on Countering the Use of Information and Communication Technologies for Criminal Purposes." 2018. *United States Mission to the United Nations*. http://usun.usmission.gov/explanation-of-vote-on-a-third-committee-resolution-on-countering-the-use-of-information-and-communication-technologies-for-criminal-purposes/ (February 26, 2021).

"Facebook, Twitter CEOs to Be Pressed on Election Handling." 2020. *AP NEWS*. https://apnews.com/article/facebook-twitter-ceos-election-congress-68489486894db6fd552611fa76775887 (December 3, 2020).

Feldstein, Steven. 2020. *How to Tackle Europe's Digital Democracy Challenges*. Carnegie Endowment for International Peace.

https://carnegieendowment.org/2020/10/15/how-to-tackle-europe-s-digital-democracy-challenges-pub-82960 (October 20, 2020).

Fichera, Angelo. 2020. "Video Doesn't Show 'Suitcases' of Illegal Ballots in Georgia." *FactCheck.org*. https://www.factcheck.org/2020/12/video-doesnt-show-suitcases-of-illegal-ballots-in-georgia/ (February 2, 2021).

Fidler, David P. 2016. "The U.S. Election Hacks, Cybersecurity, and International Law Symposium on Cybersecurity and the Changing International Law of Data." *AJIL Unbound* 110: 337–42.

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110(3): 425–79.

———. 2020. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." *European Journal of International Law*. https://academic.oup.com/ejil/advance-article/doi/10.1093/ejil/chaa056/5904502 (December 1, 2020).

Ford, Christopher A. 2010. "The Trouble with Cyber Arms Control." *The New Atlantis*. http://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control (February 28, 2021).

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018. Gaithersburg, MD: National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (January 30, 2021).

Franck, Thomas M. 1998. Fairness in International Law and Institutions *Fairness in International Law and Institutions*. Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198267850.001.0001/acprof-9780198267850 (December 1, 2020).

Frank, John. 2019a. "Paris Call: Growing Consensus on Cyberspace." *Microsoft (Blog)*. https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/ (December 3, 2020).

2019b. "Paris Call: Growing Consensus on Cyberspace." *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/ (March 5, 2021).

"Georgia Election: Trump Voter Fraud Claims and Others Fact-Checked." 2021. *BBC News*. https://www.bbc.com/news/55561877 (February 2, 2021).

Ghasiya, Piyush, and Koji Okamura. 2020. "Comparative Analysis of Japan and the US Cybersecurity Related Newspaper Articles: A Content and Sentiment Analysis Approach." In *Advanced Information Networking and Applications*, Advances in Intelligent Systems and Computing, eds. Leonard Barolli et al. Cham: Springer International Publishing, 431–43.

"Government Responses to Disinformation on Social Media Platforms." 2019. https://www.loc.gov/law/help/social-media-disinformation/uk.php (October 6, 2020).

Grisby, Alex. 2015. "The 2015 GGE Report: Breaking New Ground, Ever So Slowly." *Council on Foreign Relations*. https://www.cfr.org/blog/2015-gge-report-breaking-new-ground-ever-so-slowly (February 11, 2021).

Griswold, Jena. 2019. "Colorado's Secretary Of State On Election Security." https://www.kunc.org/show/kuncs-colorado-edition/2019-10-21/colorados-secretary-of-state-on-election-security (February 15, 2021).

"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :" 2015. http://digitallibrary.un.org/record/799853 (October 14, 2020).

Guynn, Jessica. 2020. "Donald Trump Supporters Claim They're Censored but Dominate Facebook." *USA Today*. https://www.usatoday.com/story/tech/2020/11/30/donald-trump-facebook-twitter-censor-censorship-conservatives-election/6349142002/ (February 14, 2021).

Hamilton, Isobel Asher. 2020. "The Georgia Runoffs Could Decide the Fate of Section 230 – along with the Future of Big Tech." *Business Insider*. https://www.businessinsider.com/what-biden-administration-means-for-section-230-2020-11 (February 14, 2021).

Hearing Disinformation Online and a Country in Crisis. 2020. (House).

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5(1). https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865 (November 24, 2020).

Hinck, Garrett. 2018. "Private-Sector Initiatives for Cyber Norms: A Summary." *Lawfare*. https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary (March 5, 2021).

"Homeland Security Presidential Directive 7 | CISA." 2003. https://www.cisa.gov/homeland-security-presidential-directive-7 (February 20, 2021).

Hood, Glenn. 2005. *Florida Voting System Standards*. Florida Department of State.

https://www.cisa.gov, Cybersecurity and Infrastructure Security Agency: 2020. "Election Infrastructure Security Resource Guide: Cybersecurity and Infrastructure Security Agency U.S. Department of Homeland Security." *Homeland Security Digital Library*. https://www.hsdl.org/?abstract&did= (January 19, 2021).

Huergo, Jennifer. 2014. “NIST Releases Cybersecurity Framework Version 1.0.” *NIST*. https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10 (February 20, 2021).

Human Factors and Privacy Subcommittee and Security and Transparency Subcommittee. “Software Independence and Accesibility.”

“Human Rights Council Resolution 20/8.” 2012.

Illinois: Application for Approval of Voting Systems. 2009. 204.50 26.

Issac, Mike, and Kellen Browning. 2020. “Lawmakers Drill down on How Facebook and Twitter Moderate Content. - The New York Times.” *The New York Times*. https://www.nytimes.com/2020/11/17/technology/lawmakers-drill-down-on-how-facebook-and-twitter-moderate-content.html (February 14, 2021).

Jeyaraj, Anand, and Amir Zadeh. 2020. “Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach.” *Journal of Organizational Computing and Electronic Commerce* 30(4): 361–80.

Johnston, Roger. 2011. *Suggestions for Better Election Security*. Argonne National Laboratory.

Koh, Harold Hongju, Abram Chayes, Antonia Handler Chayes, and Thomas M. Franck. 1997. “Why Do Nations Obey International Law?” *The Yale Law Journal* 106(8): 2599.

Lerman, Rachel. 2021. “Social Media Liability Law Is Likely to Be Reviewed under Biden.” *Washington Post*. https://www.washingtonpost.com/politics/2021/01/18/biden-section-230/ (February 14, 2021).

“Louisiana Looking to Replace Entire Stock of Voting Machines.” 2021. *KTBS*. https://www.ktbs.com/news/arklatex-politics/louisiana-looking-to-replace-entire-stock-of-voting-machines/article_50c89548-6156-11eb-a398-eb992fbb9342.html (February 7, 2021).

Mack, Jacob. 2019. “Statement on Agenda Item 107 ‘Countering the Use of Information and Communications Technologies for Criminal Purposes.’” *United States Mission to the United Nations*. http://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/ (February 26, 2021).

Markoff, Michele. 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 Tele.” *United States Mission to the United Nations*. http://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/ (February 11, 2021).

Marks, Joseph. 2015. “U.N. Body Agrees to U.S. Norms in Cyberspace.” *POLITICO*. https://politi.co/2TUiiUi (February 11, 2021).

Maurer, Tim, Wyatt Hoffman, Ducan Hollis, and Christian Ruhl. 2020. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.” *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110 (October 26, 2020).

McFaul, Michael. 2019. *SECURING AMERICAN ELECTIONS*. Stanford University.

Nakashima, Ellen. 2021. “Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader.” *Washington Post*. https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html (February 27, 2021).

National Conference of State Legislatures. 2018. “Voting System Standards, Testing and Certification.” https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx (February 5, 2021).

Ohlin, Jens David. 2017. *Did Russian Cyber-Interference in the 2016 Election Violate International Law?* LawArXiv. preprint. https://osf.io/3vuzf (September 13, 2020).

Posner, Eric. 2003. “Do States Have a Moral Obligation to Obey International Law?” *Stanford Law Review* 55(5).

Prince, Daniel, and Mark Lacey. 2018. “Securitization and the Global Politics of Cybersecurity.” : 19.

Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. 2019. The United Nations.

Reichenbach, Dominique. 2020. “Taiwan’s Electoral System Puts the US to Shame.” *The Diplomat*. https://thediplomat.com/2020/02/taiwans-electoral-system-puts-the-us-to-shame/ (November 24, 2020).

Report of OEWG Developments on in the Field of Information and Telecommunications in the Context of International Security. 2020. United Nations.

“Responsibility of States for Internationally Wrongful Acts.” 2008. In *International Documents on Environmental Liability*, Dordrecht: Springer Netherlands, 323–31. http://link.springer.com/10.1007/978-1-4020-8367-9_22 (February 27, 2021).

Root, Danielle, Liz Kennedy, Michael Sozan, and Jerry Parshall. 2018. “Election Security in All 50 States.” : 245.

Russian Online Disinformation Tech Solutions. 2017. (Senate).

Ryan, Gery W., and H. Russell Bernard. *Techniques to Identify Themes in Qualitative Data*. http://www.analytictech.com/mb870/readings/ryan-bernard_techniques_to_identify_themes_in.htm (January 9, 2021).

Sanger, David E. 2018. “U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks.” *The New York Times*. https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html (March 5, 2021).

“Section 230 of the Communications Decency Act.” *Electronic Frontier Foundation*. https://www.eff.org/issues/cda230 (February 14, 2021).

Securing the Vote: Protecting American Democracy. 2018. National Academies of Sciences, Engineering, and Medicine. https://www.nap.edu/download/25120# (January 21, 2021).

Securing U.S. Election Infrastructure and Protecting Political Discourse. 2019. (House) https://congressional-proquest-com.colorado.idm.oclc.org/congressional/result/congressional/congdocumentview?accountid=14503&groupid=96122&parmId=176CB869257&rsId=176CB85E058#0 (February 2, 2021).

Segal, Adam. 2016. “Do U.S. Efforts to Deter Russian Cyberattacks Signal the End of Cyber Norms?” *Council on Foreign Relations*. https://www.cfr.org/blog/do-us-efforts-deter-russian-cyberattacks-signal-end-cyber-norms (October 14, 2020).

Shanton, Karen L. 2020. “The U.S. Election Assistance Commission: Overview and Selected Issues for Congress.” : 30.

Sheth, Sonam, Eliza Relman, and Ashley Gold. 2020. “Trump Signs Executive Order Threatening Penalties to Twitter, Facebook.” https://www.businessinsider.com/trump-signs-executive-order-threatening-twitter-facebook-conservative-bias-2020-5?r=eo-landing (February 23, 2021).

State Requirements and the Federal Voting System Testing and Certification Program. 2009. Election Assistance Commission.

“Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment.” 2016. *whitehouse.gov*. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (October 14, 2020).

Swenson, Ali. 2020. “Surveillance Tape Breeds False Fraud Claims in Georgia.” *AP NEWS*. https://apnews.com/article/election-2020-donald-trump-georgia-media-social-media-e9a73462e39e7aa39683f0f582a6659e (February 2, 2021).

"The Paris Call of the 12 November 2019 — Paris Call." 2019. https://pariscall.international/en/call (November 30, 2020).

The Road to 2020: Defending Against Election Interference. 2019. (House of Representatives) https://congressional.proquest.com/congressional/result/congressional/congdocumentview?accountid=14503&groupid=96122&parmId=176972BA518#0 (January 23, 2021).

"UConn Team Ensures Election Integrity." 2010. *School of Engineering News*. https://news.engr.uconn.edu/uconn-team-ensures-election-integrity.php (February 6, 2021).

"UN Charter (Full Text)." 2016. https://www.un.org/en/sections/un-charter/un-charter-full-text/ (February 27, 2021).

"UN GGE on Cybersecurity: The End of an Era?" https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (February 14, 2021).

"United Nations General Assembly Resolution 68/167 The Right to Privacy in the Digital Age." 2014.

United States Department of the Treasury. 2019. "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups | U.S. Department of the Treasury." https://home.treasury.gov/news/press-releases/sm774 (February 21, 2021).

Volume I: Voting System Performance Guidelines. 2015. Election Assistance Commission.

Volume II: National Certification Testing Guidelines Summary. 2015. Election Assistance Commission.

Volz, Dustin. 2018. "U.S. Spending Bill to Provide $380 Million for Election Cyber Security." *Reuters*. https://www.reuters.com/article/us-usa-fiscal-congress-cyber-idUSKBN1GX2LC (February 3, 2021).

Wilson, Aaron, Mike Garcia, and Philip Langlois. 2019. *Security Best Practices for Non-Voting Election Technology*. Center for Internet Security.

Zetter, Kim. 2016. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED." *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (March 6, 2021).

Appendix A

Norms from the 2015 UN GGE Report

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

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

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

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law
that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Appendix B

Election infrastructure security in the United States is primarily composed, broadly, of two components: non-voting and voting infrastructure. The Election Assistance Commission recommends best practices for security in both of these areas. Using that information provided by the EAC, I identified the best reports to gain an understanding of the cybersecurity landscape as it relates to non-voting security. I later focus on voting infrastructure security, specifically as it relates to electronic voting machines. The organizations and their respective reports used in my research, as well as justification for their inclusion, are outlined below. All the reports utilized were published following the events of the 2016 United States Presidential Election and thus reflect a response to such interference. This selection was intentional in order to keep the 2016 United States Presidential Election as a continuous focal point throughout my research:

Voter Registration Database Security, Center for Election Research and Innovation (CEIR)

The CEIR is a not-for-profit organization and was founded in 2016 by David Becker, a former attorney in the Voting Section of the Department of Justice's Civil Rights division, in order to respond to a historic decline in voter turnout and combat foreign interference. The CEIR is a non-profit, nonpartisan organization and its work was selected for use in my research for its minimal bias evident its work with both Republican and Democratic Secretaries of State. Upon receiving requests from election officials, the CEIR will provide technical tools and planning to maintain accurate voter lists and mitigate vulnerabilities in election infrastructure.

Voter Registration Database Security is a research report produced by CEIR in September 2018 and includes findings that are drawn from discussions with experts from technical organizations, the Department of Homeland Security, the Election Assistance Commission, and others. The findings are meant to articulate threats that exist in the prevention, detection, and mitigation of vulnerabilities within voter registration database and offer guidance in improving existing practices.

Recommended Security Controls for Voter Registration, The MITRE Corporation

The MITRE corporation is a not-for-profit organization that specializes in conducting research focused on emerging technologies at the federal, state, and local

government level, in the private sector, and in academia. While the MITRE corporation is comprised of several centers, I was concerned with work being published from the National Cybersecurity federally funded research and development center (FFRDC) that is operated in conjunction with NIST. The MITRE corporation does not have to compete or have to reconcile interests between industry, owners, or shareholders. Rather, their clients are sourced from a variety of sectors.

Recommended Security Controls for Voter Registration provides security controls for a technical audience charged with securing voter registration systems. Of these security controls, this report specifically highlights the importance of understanding the supply-chain model of the infrastructure that underlies voter registration infrastructure in order to secure these assets from exploitation. Furthermore, the report is concerned with making sure communication between the various parts of the supply-chain model are properly protected.

Better Safe Than Sorry: How election officials can plan to get ahead to protect the vote in the face of a cyberattack, Brennan Center for Justice

The Brennan Center for Justice is housed in New York University School of Law and is a nonpartisan law and policy institute that conducts research meant to help in protecting the core components of democracy. The Brennan Center has worked with grassroot groups, advocacy organizations, and governments officials and its work was selected for its nonpartisan ideology.

In response to the 2016 United States Presidential Elections acts of foreign interference that exposed weaknesses in then existing cybersecurity planning, *Better Safe Than Sorry* provides recommendations to prevent cybersecurity incidents as well as respond to them. *Better Safe Than Sorry* focuses on those vulnerabilities that can be exploited within voter registration databases by virtue of this database being both a long-term storage mechanism, as well as a resource that is needed instantaneously by election officials on election day.

Security Best Practices for Non-Voting Election Technology, Center for Internet Security (CIS)

The Center for Internet Security is a not-for-profit organization that focuses on providing cybersecurity standards to the information technology community. CIS is best known for its production of CIS Controls and CIS Benchmarks that provide standardization recommendations organizations can use to evaluate their cybersecurity posture. Furthermore, CIS houses the Elections Infrastructure Information and Sharing Center (E-ISAC) that provides nonpartisan cybersecurity services to United States federal, state, local, and territorial entities.

Security Best Practices for Non-Voting Election Technology is a set of best practices IT professionals are recommended to abide by when deploying non-voting systems, such as voter registration databases. CIS's best practices are meant to help election officials and IT professionals prioritize assets to protect and actions to take

specifically in the context of non-voting election technology. The report goes into detail regarding best practices for each aspect of non-voting election technology.

Appendix C

Further Explanation on the NIST Cybersecurity Framework

The NIST Cybersecurity Framework Version 1.0 was published in 2014 to guide critical infrastructure operators in how to best secure the systems that underlie critical infrastructure. In 2018, Version 1.1 was released and is the version that was utilized in my research. Feedback from Version 1.0 prompted NIST to adapt the framework in order to address the following needs: emphasizing that "compliance" that there is not strict compliance with the Framework, but rather helps organizations develop their own versions of "compliance"; expanding guidance on how to conduct security self-assessments; adding explanations as to how best protect against attacks that target supply-chain structures; refining authentication, authorization, and identity proofing measures; better explaining how different pieces of the Framework work together; and adding guidance as to how to navigate the vulnerability disclosure process.

The Cyber Resilience Review (CRR) is a CISA assessment tool meant to evaluate maturity of an organization's cybersecurity practices across various domains. The NIST Cybersecurity Framework was the backbone of the CPR evaluation methodology and thus serves as a common denominator in CISA's security practice, and consequently critical infrastructure security at large (https://www.cisa.gov 2020). The use of the NIST Cybersecurity Framework was intended to specifically guide best practices in securing critical infrastructure.

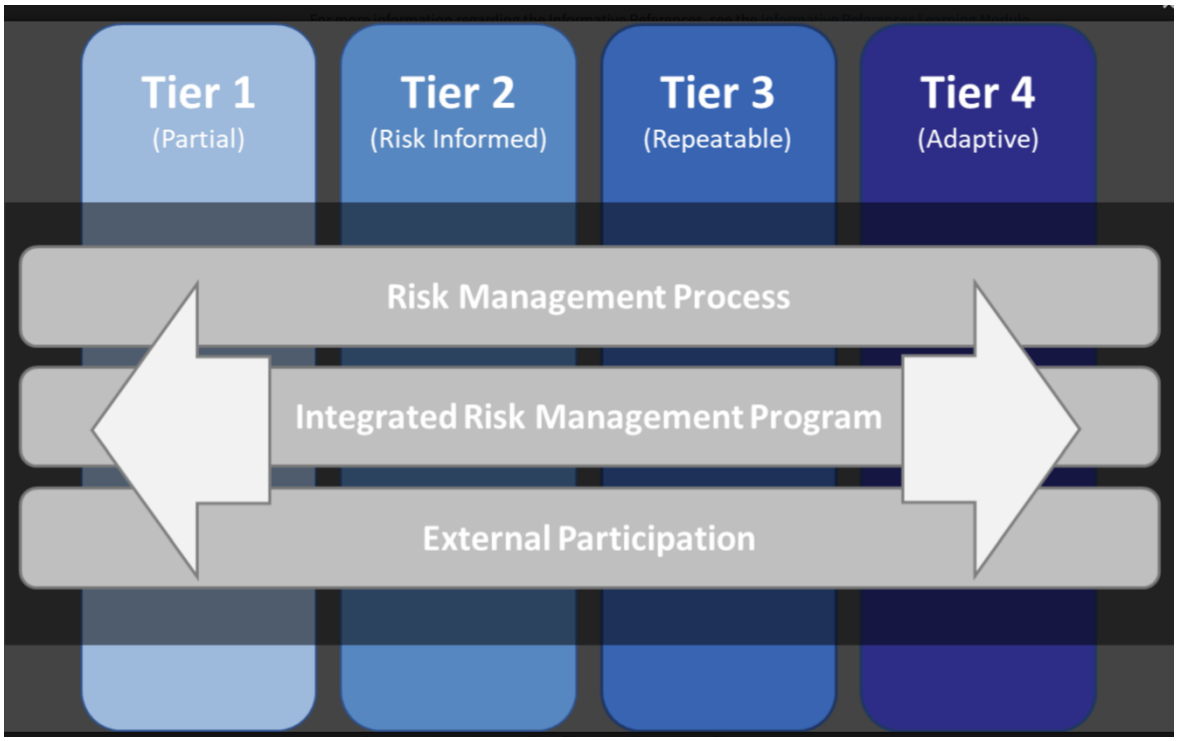
CISA, as the DHS entity charged with critical infrastructure protection, is primarily a provider of resources local election officials can use to pursue an "election infrastructure as critical infrastructure" security posture. In pursuit of this posture, the standards produced by the previously mentioned entities are used as *assessment tools* by CISA in evaluating the effectiveness of local election cybersecurity infrastructure. The established and respected nature of the NIST Cybersecurity Framework has made it a particularly favored tool in the security of election infrastructure, hence its frequent use in the studied documents.

My research focused on the functionalities of the Framework; functionalities are activities that should be undertaken to improve a cybersecurity posture and comprise the Framework core. The Framework Core is expanded to elaborate on more specific functions that be taken in regard to the functionalities of "identify", "protect", "detect", "respond", and "recover". Elaboration upon these functions is included in the table below, sourced from the NIST Cybersecurity Framework:

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Upon determining the extent to which an organization achieves the functions stated above, organizations can then determine how sophisticated their cybersecurity postures is. The figure below depicts four tiers that organizations can choose to strive for with each representing varying levels of rigor, integration of cybersecurity-based decision into larger decisions, and information sharing practices. Based upon the tier, organizations can create the cybersecurity profile they wish to have and improve or otherwise change the execution of the five functionalities listed above.



Appendix D

Securing the Vote: Protecting American Democracy

The National Academies is comprised of the National Academy of Sciences, the National Academy of Engineering, and the National Academy of Medicine. The National Academies serve as independent bodies meant to provide input on governmental decisions relating to scientific matters. Although each of the National Academies publish their own reports, reports in which each body provides input are categorized as consensus reports. *Securing the Vote: Protecting American Democracy* is, therefore, a consensus report. Reports of this nature undergo rigorous review from each of the bodies and represent the evidence-based findings that supports the ultimate recommendations of the National Academies.

Securing the Vote based its recommendations upon the ultimate finding that the greatest threat to electoral systems is not the increasingly complex technological nature of those systems that lend themselves to problems, but rather pointed attempts to undermine electoral integrity and voting security. The Academies recommend steps in light of this observations that strive to improve security in the following areas: infrastructural components of voting systems, such as voter registration databases and electronic voting machines, electoral integrity as it relates to the proliferation of disinformation, and hierarchical organizations. Due to the respected and independent nature of the National Academies, it was used as reliable evidence in supporting the themes arising out of the United States' domestic cybersecurity practices.

Appendix E

Congressional Hearings

Congressional hearings were used to clarify the United States' domestic norms as well as provide concrete examples of how these norms are expressed through rhetoric. Hearing transcripts were acquired through ProQuest's Congressional Legislative and Executive Documents database. The thematic focus of my research was upon those norms that arose out of Russian interference into the 2016 United States Presidential Election, therefore I relied upon hearings that took place after 2016. To further narrow the scope of relevant hearings, I utilized ProQuest's search engine to specify "election security" as the subject matter. Furthermore, I read through the summaries of hearings that matched this criterion in order to determine their relevance to the research. In cases where hearings did not specifically concern electoral integrity or voting security, these hearings were not used to contextualize the research. This process yielded the thirty-nine hearings that were quoted from and used to support my findings.

Appendix F

U.S. Election Assistance Commission

Categories of State, Territory, and District of Columbia Participation in Federal Voting Standards
Last Updated 4/30/2009

1.) *No Federal Requirements*	2.) *Requires Testing to Federal Standards*	3.) *Requires Testing by a Federally Accredited Laboratory*	4.) *Requires Federal Certification*
20	**10**	**13**	**12**
AK	CT	AL	CA
AS	DC	AZ	CO
AR	IN	IL	DE
FL	KY	IA	GA
GU	MN	LA*	ID**
HI	NV	MA	NC**
KS	NY	MD	ND
ME	OR	MO	OH
MI***	TX	NM	SC
MS	VA	PA	SD
MT		RI*	WA
NE		UT*	WY
NH		WI*	
NJ			
OK			
PR			
TN			
VT			
VI			
WV			

* Statutes/regulations require testing by an independent testing authority or NASED accredited laboratory according to standards adopted by either the FEC or EAC.

** Statute allows for either NASED or EAC certification.

*** Statutes/regulations prescribe testing by an independent testing authority accredited by NASED, with no mention of Federal standards.

State Requirements and the Federal Voting System Testing and Certification Program. 2009. Election Assistance Commission.

Appendix G

The Paris Call Norms/Principles

Principle 1: Protect individuals and infrastructure

Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure. Emergency services: the European Emergency Number Association provides cybersecurity guidelines to ensure the safety of citizens. Recent cyberattacks around the world, including against hospitals, remind us about the need to be better prepared. Public safety organizations are not exempt from these ever-evolving cyber risks. When emergency call centers suffer cyberattacks, interference with first response from rescue organizations can result in the death of individuals.

The European Emergency Number Association (EENA) believes that, for the safety of citizens, it is essential to ensure public safety services remain uninterrupted. To protect critical infrastructure and sensitive information, emergency services must implement appropriate and effective safeguards.

After the WannaCry ransomware attacks in 2017, EENA launched its Cybersecurity Working Group to help share best practices and develop a set of concrete, specific recommendations for emergency response organisations. The group held a dedicated webinar and published cybersecurity guidelines. The importance of this issue has been highlighted at the annual EENA Conference for several years and during the EENA Members Workshop 2018. Recommendations include the need to include cybersecurity as part of general risk assessment, train employees, implement technological solutions, and perform vulnerability tests and cyber incident exercises.

Principle 2: Protect the Internet

Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.

Protecting the Domain Name System: French company Nameshield ensures identity integrity and resilience

Protecting the availability and the integrity of the public core of the Internet requires close cooperation between different types of actors, including non-profit organization ICANN (Internet Corporation for Assigned Names and Numbers) and private companies such as Nameshield. An independent French company, Nameshield ensures identity integrity and resilience on the Internet with its own caste-based, resilient DNS infrastructures.

Cornerstone of the Web, the Domain Name System (DNS) serves as the Internet directory. This protocol translates a domain name into an IP address, based on a database

distributed on thousands of machines. If the DNS falls because of data corruption or a denial of service attack, websites and emails become inaccessible.

It is crucial to guarantee the protection and availability of DNS. A new protocol, DNSSEC, has thus been developed with the support of ICANN to address vulnerabilities in the DNS. Other solutions can help ensure identity resilience, such as Registry Lock or SSL certificates. By protecting data on domain name identity cards and providing a high availability service, Nameshield contributes to the second principle of the Paris Call and protects the public core of the Internet.

Public Core CoI: the Hague Centre for Strategic Studies will lead a community of interest on protecting the public core of the Internet

Responding to threats against the core protocols and services of the global Internet requires the cooperation of the full range of stakeholders. Most of the infrastructure, services, and products underpinning it are privately-owned, or governed and maintained by the civil society functioning as a technical community.

Whilst the idea of protecting the core Internet functions has a longer history, the notion only recently became the subject of various norm proposals, most notably by the Global Commission on the Stability of Cyberspace (GCSC), which was initiated by the The Hague Centre for Strategic Studies (HCSS). Building on the GCSC Report "Advancing Cyberstability" which calls for the adoption of specific "Communities of Interest", HCSS will lead a "Community of Interest on Protecting the Public Core of the Internet" (Public Core CoI). This concerted multistakeholder initiative will gather committed supporters for the general principle of protecting the public core in a regular working group.

This group will likely examine the need to further refine the concept, discuss propagation, and explore options for implementation and monitoring of the principle as well as related norms. It will convene key stakeholders to raise awareness of the threats against the core Internet protocols and functions, develop best practices and policy proposals for adoption and implementation, and advance common understandings of violations of the principle. Organizations interested in joining the Public Core CoI can write to cyber@hcss.nl.

Principle 3: Defend electoral processes

Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

Protecting the integrity of democratic elections: The Transatlantic Commission on Election Integrity (TCEI) helps advancing solutions

Election interference is a major threat to the universal right of people to take part in the democratic process. Still, democratic governments and technology companies around the world are scrambling to meet the challenges of the latest election meddling tactics and technologies. This is a global phenomenon, with instances of election interference

seen in countries from Mexico to North-Macedonia, Ukraine to Kenya, Taiwan to Turkey.

Yet, attacks and coordinated manipulation are no longer coming from foreign malign powers alone: increasingly, the cross-border disinformation playbook is used by domestic actors trying to sow division and polarization in both authoritarian and democratic contexts.

The TCEI brings together committed and eminent persons from different backgrounds with one shared goal: to ensure people decide freely, based on independent information, who should represent them. Transatlantic and bipartisan in nature, the TCEI seeks to share best practice between decision-makers and institutions across the democratic world, raise public awareness about the risks of interference while applying on the ground new models and technologies to empower civil society and governments to defend democracy. The TCEI is an initiative of the Alliance of Democracies Foundation founded by Anders Fogh Rasmussen in 2017.

Countering election interference: Microsoft and the Alliance for Securing Democracy partner to prevent malign interference by foreign actors

Microsoft and the Alliance for Securing Democracy are building a community of partners to counter election interference, which will bring together representatives from government, industry and civil society in order to strengthen the capacity to prevent malign interference by foreign actors in electoral processes.

Recognizing that the growing challenge that cyber threats pose to electoral processes is part of a broader, multifaceted threat to democratic institutions, Microsoft and the Alliance for Securing Democracy, together with a government partner, have chosen to formalize their collaboration by partnering in a community dedicated to these topics.

Together, the two organizations will work to raise global awareness of the threat cyberattacks pose to elections and democratic institutions and convene key stakeholders to advance thinking on what constitutes foreign interference in elections, track the tools and tactics used to undermine democratic institutions and processes, and develop best practices and policy responses to secure elections and other democratic processes from cyber-enabled threats. Microsoft and the Alliance for Securing Democracy will also assist likeminded partners in capacity building by developing mechanisms to facilitate information sharing on emerging trends, driving industry collaboration to support smaller organizations that lack resources to develop their own capabilities, and conducting threat simulation exercises designed to produce actionable solutions.

Principle 4: Protect Intellectual Property

Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.

Protecting software distributed under open source licenses: the Linux Foundation supports communities that share their knowledge

In a world whose dynamics are based on sharing of knowledge, the free software model and the application of free software licenses become increasingly important. Open source software is equipped with legal tools such as copyleft to frame the involvement on a cooperative basis and a reciprocal gift-giving logic, to produce highly performing software and to prevent private appropriation of codes or theft of intellectual property, since what is voluntarily shared cannot be re-appropriated.

The open source software model offers a way to reconcile private individual interest and collective efficiency: it is not a question of abandoning intellectual authorship, but to allow reuse of the free software created under the condition that any new version can also circulate freely. Hence intellectual property shared under such licenses spreads more quickly in the industrial fabric and benefits from network effects, which support the push for creating standards that evolve around it and its promoters.

With over 1,000 corporate members worldwide, The Linux Foundation provides strong support to open source communities through financial and intellectual resources, infrastructure, services, events, and training. Working together, the Linux Foundation and its projects form one of the most ambitious and successful investments in the creation of shared technology: the collective value of the code in Linux Foundation projects is estimated at roughly US$16 billion.

Balancing between protection and access in face of new digital threats: the Center for Internet & Society India participates in international negotiations on intellectual property

Managing intellectual property (IP) in the cyberspace raises numerous challenges. It is necessary for companies and authors to protect IP in the digital world, which fuels innovation, differentiation and revenue. Copyrights, patents and trademarks are an important part of the digital landscape.

As malware and malicious practices develop, companies and individuals may suffer loss due to IP theft or infringement and need to develop more sophisticated protection systems. At the same time, access to information plays an important role in terms of education and innovation. The evolving information infrastructure and new threats may upset the balance between the two.

In India, the Center for Internet and Society defends the position that the balance between protection and access must be re-calibrated in the cyberspace. As such, the Center has participated in negotiations taking place at regional and international levels through the Regional Comprehensive Economic Partnership agreement (RCEP) and the World Intellectual Property Organization Standing Committee on Copyright and Related-rights (WIPO-SCCR). In addition, the Center conducts its own empirical research on IP and ICT.

Principle 5: Non-proliferation

Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.

Fighting malware at the roots: YesWeHack organises Bug Bounty programmes to disclose and correct vulnerabilities before malicious tools get in

Bug Bounty programmes reward individuals who report security vulnerabilities. Participants who discover insufficiencies in hardware or software report to the organising entity ("the vendor") so that corrective measures can be taken.

By bridging the gap between vulnerability discoverers and vendors, Bug Bounty programmes allow the structuration of a Coordinated Vulnerability Disclosure (CVD) process. It prevents state and non-state actors from stockpiling vulnerabilities and limits the development of vulnerability-oriented black markets. In turn, it curbs the proliferation of malicious ICT practices and tools which feed on vulnerabilities.

YesWeHack, Europe's Bug Bounty leader, promotes proactive vulnerability disclosure by organising public and private Bug Bounty programmes. It also offers such programmes to NGOs and civic tech associations to improve the security of their infrastructures. By mobilising a community of ethical hackers and contributing to a harmonious CVD approach, YesWeHack limits entry points available to malicious ICT tools.

Principle 6: Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.

ICT/OT supply chain integrity: Carnegie Endowment for International Peace presents government and corporations with recommendations

The Carnegie Endowment has released a report on ICT supply chain integrity authored by Ariel E. Levite. It calls for urgent action to arrest the current trends undermining trust in digital products and services and fracturing the global ICT supply chain.

Strengthening the security of digital products and services throughout their supply chain is a key principle of the Paris Call as malicious actors can threaten governments, industry and individuals by attacking the weakest point on the chain, with negative consequences in terms of geopolitics, espionage, trade, and consumer protection. Cooperative efforts are needed to restore confidence in the integrity of supply chains.

In particular, the new report underscores the importance of complimentary governmental and corporate actions to enhance the integrity of the ICT/OT supply chain through a combination of commission and omission, elaborating on practical obligations both should undertake toward that end. It sets up comprehensive objective criteria for qualification of Trustworthy Suppliers, and proposes mechanisms to verify compliance with the trustworthiness criteria and an incentive structure to reward those who assume and fulfill their commitments.

Charter of Trust: member companies strengthen cybersecurity along the entire supply chain of their products and services

The digital world is changing everything. Today, billions of devices are connected through the Internet of Things. While this creates great opportunities, it also harbors great risks. To make the digital world more secure, partners from industry have joined forces with the Charter of Trust.

The Charter of Trust is a unique initiative now gathering 16 leading global companies – with a cooperation that has reached significant milestones toward cybersecurity and has ambitious goals for the future.
The Charter calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

After two years of work, members have achieved a lot, especially regarding the security of digital processes, products and services. In their businesses, they successfully strengthened cybersecurity along the entire supply chain and established "Security by Default" as a must-have product feature. The Charter of Trust provides its members with an aligned view on security along the digital supply chain and has defined 12 baseline cybersecurity supply chain requirements.

Members of the Charter of Trust are committed to build capacity on this important matter, as well as on other principles outlined in the Paris Call. They commit not only to providing advanced training for their workforce but also for business and society. They also continue to firmly anchor cybersecurity on the agenda at the highest political level –locally and globally.

Global Transparency Initiative: cybersecurity and anti-virus provider Kaspersky implements a unique approach for higher transparency and verifiable trust in cybersecurity

Users need to know that their data will be protected and that they can trust the security of the digital products and services they purchase – whether it is a smartphone, a laptop, a mobile application, or a cybersecurity solution. In order to earn their customers' trust, companies need to constantly improve their transparency and accountability in the cyberspace.

Kaspersky's Global Transparence Initiative (GTI) puts into effect a set of clear verification and risk-minimization measures to increase users' confidence and ensure that cybersecurity solutions meet and exceed corporate data security and protection standards.

Measures implemented by Kaspersky range from data care (relocation of data processing and data storage to Switzerland for the utmost data protection and security) to verification (secure and reliable engineering practices confirmed through independent third-party assessment) and vulnerabilities management (responsible cooperation with security researchers through Kaspersky's Bug Bounty Program with awards of up to $100k for the most critical security flaws).

The GTI also puts into place Transparency Centers, dedicated security facilities for greater confidence in and knowledge of cybersecurity products through Kaspersky's specifically

developed 'three-layer' approach to security briefings and external reviews of the company's source code, software updates and threat detection rules.

Principle 7: Cyber hygiene

Support efforts to strengthen an advanced cyber hygiene for all actors.

Seguros en la red: the Equatorian Cybersecurity Association promotes cyber hygiene to kids in Ecuador

Children and adolescents study, play and interact for hours online. But like every new world to discover, the cyberspace presents a series of risks that they need to know about.

The Ecuadorian Cybersecurity Association (AECI) launched the "Seguros en la Red" ("Secure on the net") project to teach children about responsible use of ICTs and associated risks. AECI created playful characters, who give girls and boys a minimum level of education in order to nurture, foster and promote a culture of digital security. Named "Cyber" and "Alerto", these fictional characters introduce children to cyberspace with its resources and opportunities but also its dangers.

Awareness, culture and prevention are the three pillars around which AECI aims at creating an ecosystem of digital security programs, in conjunction with educational institutions, public and private organizations.

Principle 8: No private hack back

Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.

Hack-back, active defense, and countermeasures: the Cybersecurity Tech Accord starts a conversation on definitions and best practices

As the frequency and severity of global cyber threats grow, defenders are investing in new and innovative techniques to protect themselves. However, not all measures being developed are purely defensive: increasingly talk has been around more intrusive "active defense" techniques – with hack back the most prominent example.

The Cybersecurity Tech Accord signatories strongly supported the decision to include Principle 8 in the Paris Call, which rightly introduces a general prevention on hacking back for non-state actors. However, this is an area fraught with ambiguity, and they believe further elaboration is needed to set clear boundaries around intent, authority, and intrusiveness before government and private actors can implement it.

It is particularly critical to ensure the prohibition does not capture positive cybersecurity techniques, such as penetration testing. To this end, the Tech Accord signatories are committed to working together to support effective implementation of the Paris Call principle on hack back, including by highlighting potential definitions and best practices.

They will start the discussions with a meeting at the Internet Governance Forum in Berlin, where they hope to gather views of not just industry, but civil society on this critical topic. Organizations interested in participating in this effort can send an email to info@cybertechaccord.org.

Principle 9: International Norms

Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

Selecting a contact point (POC) in each State to exchange information on ICT-related incidents: along with other countries, France operationalizes confidence-building measures within the OSCE

The Organization for Security and Co-operation in Europe tackles various cyber threats including cybercrimes and the use of the Internet for terrorist purposes. A key focus is on the development of confidence building measures (CBM) between participating states to reduce the risks of conflict. Sixteen CBMs have been adopted, which aim at enhancing interstate cooperation, transparency and predictability to reduce risks of misperception and escalation.

One of these measures requires that participating States nominate a contact point to facilitate pertinent communications and dialogue on ICT-related incidents and coordinate responses. France is one of the lead countries to operationalize this measure, including through communication checks and exercises. Exchanges of information and communication between States can stop an unintentional conflict by defusing potential tensions and stopping or slowing down the spiral of escalation.

Regional organizations such as the OSCE are ideal platforms for building confidence in cyberspace, as they have often been conceived for conflict prevention and offer practical expertise with CBMs. So far, some successful “comcheck” exercises have been launched by the OSCE secretariat, which underline the utility of such measures in order to reinforce stability in cyberspace through a continuous dialogue between States.

Preventing the ultimate realization of the cyber risk: the Nuclear Threat Initiative gathers technicians from the nuclear industry so they can equip themselves
Nuclear systems, be they civilian or military, contain digital components.

The risk of them being compromised is thus present. A successful cyberattack on nuclear weapons or related systems could have catastrophic consequences. Among scenarios studied by the Nuclear Threat Initiative are those in which a cyberattack could lead to a nuclear launch as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and undermine confidence in the nuclear deterrent, affecting strategic stability.

The Nuclear Threat Initiative NGO aims at improving and reinforcing cybersecurity practices at nuclear facilities, by bringing together the global technical cyber-nuclear

community in the Cyber Nuclear Forum to facilitate information exchange and foster a network of relationships upon which nuclear operators can draw for advice and assistance.

It also supports studies aiming at providing recommendations for cybersecurity practices at nuclear facilities. For instance, through a comparison of regulatory requirements necessary to protect nuclear facilities against cyber attacks in five nuclear-armed countries. But also through forward-looking approaches for protecting nuclear facilities from cyber attacks that could lead to the theft of weapons-usable nuclear materials or an act of radiological sabotage.

Appendix H

The Global Commission Norms

1. **Protect the Public Core of the Internet:** State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace

2. **Protect Electoral Infrastructure:** State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. **Avoid Tampering:** State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. **No Commandeering of ICT Devices into Botnets:** State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. **Norms to a Create Vulnerabilities Equities Process:** States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

6. **Reduce and Mitigate Significant Vulnerabilities:** Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7. **Basic Cyber Hygiene as Foundational Defense:** States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. **No Offensive Cyber Operations by Non-State Actors:** Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

Appendix I

UN OEWG Rules, Norms and Principles for Responsible State Behaviour

Voluntary, non-binding norms reflect the expectations of the international community and set standards regarding the acceptable and unacceptable behaviour of States in their use of ICTs. They play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. Norms do not replace or alter States' obligations under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs. In 2015, the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which sets out 11 voluntary, non-binding norms of responsible State behaviour. Alongside international law, voluntary non-binding norms complement confidence-building and capacity-building measures and related efforts to promote an open, secure, stable, accessible and peaceful ICT environment.

38. In their discussions at the OEWG, States reiterated that voluntary, non-binding norms of responsible State behaviour are consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights. States affirmed that norms play an important role in preventing conflict. States highlighted that norms should not place undue restrictions on international cooperation and technology transfer, nor hinder innovation for peaceful purposes and the economic development of States. States also stressed the interlinkages between norms, confidence-building and capacity-building, and urged that gender perspectives be mainstreamed into norm implementation. States noted that given the unique attributes of ICTs, additional norms could be developed over time.

39. States reaffirmed the 11 voluntary, non-binding norms of responsible State behaviour of the 2015 GGE report,6 recalling that consensus resolution 70/237 calls upon States to be guided in their use of ICTs by the 2015 GGE report, which includes those norms. States at the same time recalled that in General Assembly resolution 73/27, States welcomed a set of 13 rules, norms and principles of responsible behaviour of States, which encompass therein the 11 norms of the 2015 GGE report.

40. Attention was drawn to the international code of conduct for information security tabled in 2015.7 States also recalled General Assembly resolutions 2131 (XX), 1965 entitled "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty" and 58/199 entitled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures".

41. States stressed the need to promote awareness of the existing norms and support their operationalization. While these norms articulate what actions States should or should not take, States underscored the need for guidance on how to operationalize them. In this regard, States called for the sharing and dissemination of good practices and lessons on norm implementation. Different cooperative approaches were also proposed, such as developing a roadmap to assist States in their implementation efforts and surveys for the sharing of good practices.

42. States also made proposals for the enhancement as well as further elaboration of norms. Such proposals included, inter alia, that States affirm their commitment to a culture of restraint and to international peace and security in their use of ICTs; that States reaffirm their primary responsibility for maintaining a secure, safe and trustable ICT environment; that the general availability or integrity of the public core of the Internet should be protected; and that States should not conduct ICT operations intended to disrupt the infrastructure essential to political processes or to harm medical facilities. States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products, and the responsibility to notify users when significant vulnerabilities are identified. States also highlighted that the protection of transborder critical information infrastructure, as a distinct category of critical infrastructure, is the shared responsibility of all States.

43. [placeholder: additional proposals by Member States under agenda item “Rules, norms and principles” could be introduced here]

44. The role of regional organizations was recognized in norms implementation. The need to encourage further partnerships and joint efforts with other stakeholders such as the private sector on the implementation of norms was also recognized. Such partnerships could, for example, be built to ensure sustainable capacity-building efforts to address differences in implementation capacities. States could be called on to take the necessary outreach, cooperation and, where necessary, regulatory steps to ensure that various stakeholders, including the public and private sectors and civil society, uphold their responsibilities.

Appendix J

name	category	nationality	nature	website	twitter	date_signed
Access Now	civil-society	USA	ONG			
Alliance for Peacebuilding	civil-society	USA	ONG			
American Institute of Contemporary German Studies	civil-society	USA	Fondation			
Atlantic Council	civil-society	USA	Think tank			
Carnegie Endowment for International Peace	civil-society	USA	Think tank			
Center for Democracy and Technology	civil-society	USA	Think tank			
Center for European Policy Analysis	civil-society	USA		https://cepa	CEPA	12/18/20
Center for Information Technology Research in the Interest of Society (CITRIS)	civil-society	USA	Centre de recherche			
Center for International Law and Governance, Fletcher School of Law and Diplomacy at Tufts University	civil-society	USA	UniversitÝ©			
Center For Long Term Cybersecurity (CLTC) (University of California, Berkeley)	civil-society	USA	Centre de recherche			
CodeVA	civil-society	USA	Organisation Ý† but non lucratif			
Cordell Institute for Policy in Medicine and Law	civil-society	USA	UniversitÝ©			
Design 4 Democracy Coalition (D4D)	civil-society	USA	Organisation Ý† but non lucratif			11/12/19
EastWest Institute	civil-society	USA	ONG			
German Marshall Fund of the United States	civil-society	USA	Think tank			
iRespond Global	civil-society	USA	ONG			
Indiana University	civil-society	USA	UniversitÝ©			
International Civil Society Action Network	civil-society	USA	ONG			
International Foundation for Electoral Systems (IFES)	civil-society	USA	Organisation Ý† but non lucratif			
International Republican Institute	civil-society	USA	Organisation Ý† but non lucratif			
Internet Governance Lab at American University	civil-society	USA	UniversitÝ©			
LEADx Change	civil-society	USA	Organisation Ý† but non lucratif			
Middlebury Institute of International Studies at Monterey	civil-society	USA	UniversitÝ©			
National Democratic Institute	civil-society	USA	Think tank			
Nuclear Threat Initiative	civil-society	USA	ONG			
Partnership For Global Security	civil-society	USA	Centre de recherche			
Pegasus Research Foundation	civil-society	USA		https://www.ncip.tech/		11/15/19
Public Knowledge	civil-society	USA	Fondation			
Quad9	civil-society	USA	Organisation Ý† but non lucratif			
Tech Impact	civil-society	USA	Organisation Ý† but non lucratif			
Temple University	civil-society	USA	UniversitÝ©			
The Future Society	civil-society	USA	Think tank			
The Internet Society (ISOC)	civil-society	USA	Association			
The Media Institute	civil-society	USA	Organisation Ý† but non lucratif			
The World Wide Web Foundation	civil-society	USA	Fondation			
University of Pittsburgh Institute for Cyber Law, Policy and Security (Pitt Cyber)	civil-society	USA	UniversitÝ©			
Yale Privacy Lab	civil-society	USA	UniversitÝ©			

Civil Society Signatories "The Paris Call of the 12 November 2019 — Paris Call." 2019. https://pariscall.international/en/call (November 30, 2020).

name	category	nationality	nature	website	twitter	date_signed
ActiveGraf	private-sector	USA	Entreprise			
AES Corporation	private-sector	USA	Entreprise			
Albright Stonebridge Group	private-sector	USA	Entreprise			
American Chamber of Commerce in Germany	private-sector	USA	Chambre de commerce			
American Chamber of Commerce in Kenya	private-sector	USA	Chambre de commerce			
American-Hellenic Chamber of Commerce	private-sector	USA	Chambre de commerce			
AnchorFree	private-sector	USA	Entreprise			
Anomali	private-sector	USA	Entreprise			
Archive360	private-sector	USA	Entreprise			
BSA | The Software Alliance	private-sector	USA	Association professionnelle			
CA Technologies	private-sector	USA	Entreprise			
Carbon Black	private-sector	USA	Entreprise			
Charity Navigator	private-sector	USA	Entreprise			
Cisco	private-sector	USA	Entreprise			
Cloudflare	private-sector	USA	Entreprise			
Cognizant	private-sector	USA	Entreprise			
Contrast Security	private-sector	USA	Entreprise			
CREOpoint	private-sector	USA				
Cyber Adapt	private-sector	USA	Entreprise			
Cyber Law International	private-sector	USA	Entreprise			
CyberRx Inc	private-sector	USA	Entreprise			
Cybereason	private-sector	USA	Entreprise			
Datastax	private-sector	USA	Entreprise			
Dell	private-sector	USA	Entreprise			
Dell Technologies	private-sector	USA	Entreprise			
Docusign	private-sector	USA	Entreprise			
DXC Technology Company	private-sector	USA		https://ww	www.dxc	1/18/21
Exeltek Consulting Group	private-sector	USA	Entreprise			
Facebook	private-sector	USA	Entreprise			
Fastly	private-sector	USA	Entreprise			
FireEye	private-sector	USA	Entreprise			
Foley Hoag, LLP	private-sector	USA	Entreprise			
Fortinet	private-sector	USA	Entreprise			
Fractal Industries	private-sector	USA	Entreprise			
Gauba Recording Studio	private-sector	USA	Entreprise			
Gigamon	private-sector	USA	Entreprise			
GitHub	private-sector	USA	Entreprise			
Gitlab	private-sector	USA	Entreprise			
Global Cyber Alliance	private-sector	USA	Entreprise			
Google	private-sector	USA	Entreprise			
HackerOne	private-sector	USA		https://hack	Hacker0x01	1/11/21
HP Inc	private-sector	USA	Entreprise			
HPE	private-sector	USA	Entreprise			
IBM	private-sector	USA	Entreprise			
Imperva	private-sector	USA	Entreprise			
Implant Compare	private-sector	USA	Entreprise			
Infinitum Humanitarian Systems	private-sector	USA	Entreprise			
Information Technology Industry Council (ITI)	private-sector	USA	Association professionnelle			
Intel Corporation	private-sector	USA	Entreprise			
Intensity Analytics Corporation	private-sector	USA	Entreprise			
Internet Association	private-sector	USA	Association professionnelle			
Internetwork Service LLC	private-sector	USA	Entreprise			
Intuit	private-sector	USA	Entreprise			
Juniper Networks	private-sector	USA	Entreprise			
Koolspan	private-sector	USA	Entreprise			
Linkedin	private-sector	USA	Entreprise			
Marsh & McLennan Companies	private-sector	USA	Entreprise			
Mastercard	private-sector	USA	Entreprise			
Match Group	private-sector	USA	Association professionnelle			
McCoy Information Sytems, Inc	private-sector	USA	Entreprise			
McKinsey & Company	private-sector	USA	Entreprise			
McAfee	private-sector	USA	Entreprise			
Microsoft	private-sector	USA	Entreprise			
Mindtree	private-sector	USA	Entreprise			
MSD	private-sector	USA		https://ww	NA	12/8/20
NewsGuard	private-sector	USA	Entreprise			
Nielsen	private-sector	USA	Entreprise			
OneSpan	private-sector	USA	Entreprise			
OPSWAT	private-sector	USA	Entreprise			
Oracle	private-sector	USA	Entreprise			
Packet Clearing House	private-sector	USA	Entreprise			
Palo Alto Networks	private-sector	USA	Entreprise			
Pax8	private-sector	USA	Entreprise			
Professional Options	private-sector	USA	Entreprise			
Risley Advisors	private-sector	USA	Entreprise			
Rockwell Automation	private-sector	USA	Entreprise			
RSA	private-sector	USA	Entreprise			
Salesforce	private-sector	USA	Entreprise			
SAP	private-sector	USA	Entreprise			
Schneider Electric	private-sector	USA	Entreprise			
StackPath	private-sector	USA	Entreprise			
Stripe	private-sector	USA	Entreprise			
Strong Connexions	private-sector	USA	Entreprise			
Symantec Corporation	private-sector	USA	Entreprise			
TAD GROUP	private-sector	USA	Entreprise			
TechNet	private-sector	USA	Association professionnelle			
Tenable	private-sector	USA	Entreprise			

The Boston Consulting Group	private-sector	USA	Entreprise			
The Coalition of Services Industries	private-sector	USA	Association professionnelle			
The Linux Foundation	private-sector	USA	Association professionnelle			
Threat Modeler	private-sector	USA	Entreprise			
UiPath	private-sector	USA	Entreprise			
Unisys	private-sector	USA	Entreprise			
Ursa Major Technologies, Inc.	private-sector	USA	Entreprise			
US Licensing Group	private-sector	USA	Entreprise			
US Medical IT	private-sector	USA	Entreprise			
Visa	private-sector	USA	Entreprise			
VMWare	private-sector	USA	Entreprise			
WestExec Advisors	private-sector	USA	Entreprise			
Workday	private-sector	USA		https://www	@Workday	11/18/19
Zimmer Biomet	private-sector	USA				
Zoho	private-sector	USA	Entreprise			

Private Sector Signatories "The Paris Call of the 12 November 2019 — Paris Call." 2019. https://pariscall.international/en/call (November 30, 2020).

name	category	nationality	nature	website	twitter	date_signed
City of Huntington, West Virginia	public-authority	USA	Collectivitv© locale			
City of Louisville, Kentucky	public-authority	USA	Collectivitv© locale			
Commonwealth of Virginia	public-authority	USA	Etat fv©dv©rv©			
Redmond	public-authority	USA	Collectivitv© locale			
San Josv©	public-authority	USA	Collectivitv© locale			
State of Colorado	public-authority	USA	Etat fv©dv©rv©			
Washington State	public-authority	USA	Etat fv©dv©rv©			

Public Authority Signatories "The Paris Call of the 12 November 2019 — Paris Call." 2019. https://pariscall.international/en/call (November 30, 2020).

Appendix K

A significant portion of the most frequent keywords across American standards documents characterize general aspects of cybersecurity. For example, the literal words "cyber" and "security". For logical reasons, it is necessary to examine how Americans standards actually use these two terms in context in order to distinguish it from other countries and their usages. Furthermore, understanding the context in which cybersecurity is understood illustrates how the nation interprets the field and how that interpretation may translate to activities within the international organizations of focus. As the EAC was the clearinghouse for this information, I begin by analyzing what the EAC understands as "security". The Congressional Research Service (CRS) presents a 2019 overview of EAC's functions and situates the EAC's role in the larger idea of "security". First, it points out one of the distinguishing characteristics of United States cybersecurity practices when it comes to electoral protection: the designation of election infrastructure as "critical infrastructure" by the Department of Homeland Security (DHS) in 2017. The designation of election of infrastructure as such justified the United States Congress' decision to appropriate $380 million toward the enhancement of election security and election technology in March 2018 (Volz 2018). As this CRS document notes, the EAC was responsible for overseeing this enhancement to security. What the EAC did with this responsibility allows us to understand what "security" entails, as it relates to cybersecurity practices. Following the DHS's decision, the EAC orchestrated the establishment of threat sharing networks specifically concerned with protecting election infrastructure as critical infrastructure (Election Infrastructure Security | CISA n.d.; Shanton 2020). This decision also brought the Cybersecurity and Infrastructure Security Agency (CISA) to the forefront of the effort to protect election infrastructure from cyberattacks. CISA was established in 2018 to lead the US in protecting critical infrastructure from all threats, from cyberattacks to natural disasters. When election infrastructure was designated as critical infrastructure, its protection fell to CISA. With CISA and the EAC now focused on protecting election infrastructure from a standpoint of its status as critical infrastructure critical infrastructure, it is possible to evaluate the normative value that comes with that relationship.

Appendix L

Further Explanation on the "Protect" Functionality in the American Cybersecurity Sector

Authentication and access control measures are common recommendations across the studied documents and within the industry. They emphasize the different roles across elections and makes clear that each should only have access to data that is necessary to fulfill their duties. This is known as the "least privilege" principle and is prevalent across election infrastructure security (Anderson and Mutch 2011; Casey et al. 2019). The data being handled by election officials, and of particular concern in these documents, is information such as social security numbers, address, and date of birth which are commonly stored in voter registration databases. Although some aspects of voter registration databases are available to the public, other information is restricted to poll workers and are only used for verification purposes. In addition to restrictions on access, control is another issue of focus. Poll workers may have access to additional information beyond that for public consumption while information technology professionals have control over the databases for modification purposes. These documents vouch for the "least privilege" principle to clearly distinguish roles by the access and control granted to them. An individual may be a poll worker and database manager, however, there is a preference to have this individual only have certain privileges depending on the role they are assuming at a given time. Control as concise as this is reserved for the protection of "sensitive information and assets". So, while authorization and access control measures present in these documents make the "least privilege" principle noticeable, it also elucidates what exactly is being interpreted as "sensitive": in this case, it is voter registration information.

In pursuit of protection, organizations also seek to disable harmful capabilities embedded in election infrastructure. For example, analysis of these documents revealed that disabling WiFi capabilities are of particular concern. Internet-connected assets within election infrastructure has long been a concern and will be further discussed in regard to electronic voting machine security and in the context of software independence. These are not the only assets organizations seek to disable, however. Peer-to-peer (P2P) capabilities[35], USB device access, inactive accounts, caching capabilities, and outdated security protocols are also recommended to be disabled. Above all, it appears organizations seek to limit unnecessary points of access to election infrastructure.

Firewall configuration is a cornerstone of election infrastructure security control measures as identified by the examined documents. They are responsible for filtering, identifying, and overall managing the flow of network of traffic between the internal election infrastructure network and external destinations. In addition to vouching for such measures, the discussion of firewalls also reveals a preference for network segmentation to clearly distinguish which parts of the network are to be used solely for

[35] P2P is a form of network architecture that allows two clients to communicate with one another directly over a private or public network. The usage of P2P is concerning because all clients on the network are not known or available at the time of communication.

specific functions of election infrastructure. With network segmentation, the network is divided into sections that certain individuals will have access to dependent upon their role in the organization. This kind of architecture lends itself to the "Zero Trust" model - no individual is trusted completely, including individuals with access to the network at large. This kind of model can imply two normative values: 1) Concern for insider attacks[36] and 2) Concerns about the risk of employees inadvertently leaking sensitive information. To identify which is generally more of concern, I analyzed these documents and Congressional hearings for rhetoric that reflected fear of insider attacks.

There was little indication of fear over insider threats in the form of electronic data exfiltration that is being used to aid in foreign interference or influence. All Congressional hearings on matters of election security held since 2015 have yet to mention concern over insider threats that would compromise election cybersecurity. Rather, there has been a focus on malicious insider activity that compromises physical rather than cyber security. There have been accusations of election workers stealing ballots in the 2020 US Presidential Election and other physical forms of malicious insider activity, however, there has been little evidence to support this claim (Brown 2020; Fichera 2020; Georgia election 2021; Swenson 2020). Despite there being minimal discussion concerning insider threats insofar as abating successful cyberattacks, a boilerplate discussion on the danger of insider threats is present within prominent reports on best security practices (Johnston 2011; Wilson, Garcia, and Langlois 2019).

Appendix M

Transaction logs record activity within the database, such as viewing, adding, or deleting information. These logs are key to understanding what aided in successful attacks upon election infrastructure. In affirming the security of his state's elections before the 116th Congress, Massachusetts Secretary of State Bill Galvin testified that its underlying network infrastructure is effectively monitored due to the implementation of Albert sensors and the logging of all user activity within transaction logs (Securing U.S. Election Infrastructure and Protecting Political Discourse 2019). In addition to monitoring and logging capabilities, regular audits are important in detecting irregularities and are most frequently invoked as important solutions in the context of electronic voting machine security.

Appendix N

Similar to what was observed from non-voting security normative concerns, unauthorized access was a vital piece in cybersecurity practices. Sounds practices are responsible for ensuring the "integrity, availability, confidentiality, and accountability" of the system as a whole and it begins with mitigating unauthorized access. It is noticeable that the federal guidelines by which voting machines are certified noticeably highlights retention of the election results' integrity as one of the highest priorities. As a result, federal guidelines strictly lay out expectations as to how best ensure the integrity and accuracy of voting results in a procedural manner. Beginning with accuracy and integrity of initial voting

[36] Insider attacks occur when individuals with access to network, hired on an assumption of trust, intentionally leak sensitive information for financial gain or other motive related to self-interest.

reporting, federal guidelines allow for "zero margin of error" in voting system software, firmware, and hardwired logic. Simply put, this means that the software responsible for recording the voters' selections must always be properly recorded. The federal guidelines, however, recognize physical factors can damage voting systems and are largely outside the control of voting systems' manufacturers. Regardless, such errors in software are not tolerated and, in the event of glitches within the system, they must be detectable.

After initial voting, auditing is still a significant factor in federal certification standards. Volume I of the VVSG notes that "Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors" (Volume I: Voting System Performance Guidelines 2015). To ensure proper auditing procedures are in place, federal certification standards list operational requirements that are all concerned with accurate logging and error reporting. This focus on integrity and accuracy, throughout every step in the election process, is prevalent in Volume I of the VVSG. Volume II: National Certification Testing Guidelines Summary emphasizes the importance of these same points; however, it is intended for a more technical audience (i.e. voting system manufacturers) (Volume II: National Certification Testing Guidelines Summary 2015).

Appendix O

Private Sector Actions in Addressing Misinformation

Google, Twitter, and Facebook have all taken steps to protect against State-sponsored disinformation campaigns. In 2018, these three companies created specialized teams tasked with identifying State-sponsored users and groups utilizing their respective platforms to spread disinformation regarding elections. As a result of this efforts, Facebook removed 70 Facebook accounts, 65 Instagram accounts, and 138 pages tied to Russia's Internet Research Agency (IRA) (Dutta et al. 2020). Actors from Iran, Pakistan, and India have also been removed from these platforms. Additionally, Google, Twitter, and Facebook have introduced policies that strengthen the requirements for paid political advertisements that utilize their platforms: paid political advertisements are required to have a "Paid for by" disclaimer with some countries, such as the United States, adopting the requirement that such advertisements can only be run by verified American citizens. Steadily, States have also been introducing legislation that requires private entities to take greater ownership over removing and labeling content that can be misleading and undermine the democratic process. Leading up to the 2020 United States Presidential Election, Facebook and Twitter began labeling content for all users to see if such content could be interpretated as being misinformation. On Twitter, this policy began being applied to prominent political figures' content, including US President Donald Trump's Twitter account (Business et al. 2018; Facebook, Twitter CEOs to be pressed on election handling 2020; McFaul 2019).

Appendix P

The Creation of the American Critical Infrastructure Protection Program

Critical infrastructure became an important issue long before the foundational 2015 UN GGE Report. The Homeland Security Presidential Directive 7 was published in 2003 and directed federal agencies to identify and prioritize critical infrastructure protection. To complement this directive, Executive Order 1363: Improving Critical Infrastructure Cybersecurity directed NIST to develop the Cybersecurity Framework in pursuit of a better critical infrastructure cybersecurity posture (Homeland Security Presidential Directive 7 | CISA 2003; Huergo 2014) . This executive order is another instance in which domestic cybersecurity policy predicted a United States effort to advocate for certain international norms. However, the identification and prioritization of critical infrastructure is only the beginning of the story, as discussions on international protection from cyberattacks upon elections added further complexity to the norms valued by the United States.

Appendix Q

A Response to a Cyber Attack on Critical Infrastructure

In January 2021, a hack of the network monitoring tool SolarWinds allowed Russian actors to successfully infiltrate the networks of nine United States government agencies and approximately 100 private companies. Since "government facilities" is defined as one of the United States sectors of critical infrastructure, this act was an attack upon critical infrastructure and with that brings the connotation that this was an attack upon infrastructure whose incapacitation can have a "debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (https://www.cisa.gov 2020). The United States has responded accordingly with economic sanctions and other undisclosed retaliatory measures against Russian and, in the process, invoked the same norms that have created a divide between itself and Russia. United States National security adviser Jake Sullivan stated the response to the Russian hack "will include a mix of tools seen and unseen, and it will not simply be sanctions [...] We will ensure that Russia understands where the United States draws the line on this kind of activity" (Nakashima 2021).

Sullivan's statement implies that the United States is prepared to go beyond the level of sanctions in punishing Russian actions. Under the UN Charter, the retaliatory action Sullivan alludes to are only appropriate in the circumstances described within the UN Charter under Article 51, which defends the right of a State to respond to an armed attack before the Security Council is able to take steps toward maintain peace (UN Charter (full text) 2016). The circumstances described in Article 51 would also correlate to a state of *jus ad bellum* in which the United States is within its right to respond to the SolarWind hack with acts of self-defense. However, all of this is contingent upon the United States norm that cyberattacks are severe enough to constitute an "armed attack".

Appendix R

Human Rights Council Resolution Committed to Preserving Internet Freedom

The Human Rights Council resolutions affirm the human rights that individuals have offline, including the right to freedom of speech, must be protected online as well, regardless of the mediums through which individuals choose to communicate (Human Rights Council Resolution 20/8 2012). The General Assembly resolutions uphold the same ideas as those present in the Human Rights Council resolutions, however, it focuses on reaffirming an individual's to privacy as a vital component in preserving freedom of expression on the Internet (United Nations General Assembly Resolution 68/167 The Right to Privacy in the Digital Age 2014). The United States is using these foundations of international law to establish its applicability in cyberspace, as well the importance of its inclusion in the cyber norms to be developed. As a result, the United States is advocating for the norm in which international humanitarian law, grounded in these resolutions, should be of the utmost concern in cyberspace. This ideal stands once again in contrast to those ideas proposed by Russia through its participation with the UN OWEG and includes significant implications for electoral protection as it relates to misinformation and disinformation management.

Appendix S

Why has the United States, as a nation, not signed the Paris Call?

The United States government has not issued a statement as to why they have not signed the Paris Call. However, analysis conducted on behalf of third parties indicates that the decision is justified by another previously discussed norm regarding the importance of flexibility in cyberspace to the United States, especially when responding to cyberattacks. An analysis conducted by the *New York Times* revealed that, based upon previous patterns of the United States' behavior, the government may be "leery of any kind of agreement that might make illegal the types of activity — like espionage, data manipulation or attacks on infrastructure — that the United States may want to use in a future conflict". An unnamed United States diplomat, however, did mention the possibility of the federal government signing the Paris Call in the future (Sanger 2018). For the time being, collaboration between the United States government and non-state actors is an idea that remains evident in rhetoric alone.