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

Kiana Harkema

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.

Introduction

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[1] 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.

The road to cyber global governance in safeguarding elections is paved by international organizations that are seeking to establish norms that are proposals for how international law should play a role in establishing conduct in cyberspace, as well as other guidelines for behavior. The international organizations of interest in this research are the United Nations Group of Governmental Experts (UN GGE), the United Nations Open-Ended Working Group (UN OEWG), the Paris Call for Trust and Security and Cyberspace, and the Global Commission on Stability in Cyberspace. My research seeks to understand how effective the United States has been in getting its own domestic cyber norms, in the context of election security, legitimized in these international bodies. 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, the norms valued by the United States are not equally effective in gaining international legitimacy.

I rely on the textual analysis of key cybersecurity standardization documents, Congressional hearings, and other relevant statements to understand norms the United States values in its election-oriented cybersecurity practices. 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 misinformation and 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. However, at the same time, the United States has faced obstacles in legitimizing other domestic norms that have arisen out of these practices. 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.

[1] Disinformation is defined as false information that is intentionally spread to cause some form of harm, while misinformation is not necessarily spread with the same intent (e.g., social media users unknowingly sharing fallacious news articles).

Cybersecurity Practices as Insight into American Cyber Norms

In determining the cyber norms valued by a nation, I argue cybersecurity practices can provide valuable insight. Furthermore, the elucidated norms can be used to understand international norm-setting behavior through the lens of a studied nation. Specifically, I use this method in the context of identifying American cyber norms and analyzing the extent to which these norms are present in those established by the UN GGE, the UN OEWG, the Paris Call, and the Global Commission. The result is a more nuanced understanding of the path a nation has taken to establish a method of cyber global governance.

The successful identification of norms within cybersecurity practices relies upon the theory of organizational isomorphism, Keywords-in-Context (KWIC) analysis, and the examination of cybersecurity standardization documents. The usage of these tools, in tandem, have been historically underutilized.

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. However, Jeyaraj and Zadeh stopped short of analyzing these key terms in their specific context, thus necessitating my usage of the KWIC analysis. Per the KWIC theoretical framework, sentiment, and in this case norms, 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.). Thus, I extract the keywords noted by Jeyaraj and Zadeh, identify the most commonly invoked ones within American cybersecurity documents, and analyze the context in which they are used to elucidate important cyber norms that could later be used in my research to understand how effective the United States has been in gaining international legitimacy for these norms.

The documents used in the KWIC analysis ware provided by the Election Assistance Commission (EAC), the 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 order to protect against cyberattacks and yield the following results following a keyword analysis, as depicted below in Table 1 (Becker et al. 2018; Casey et al. 2019; Checklist for Securing Voter Registration Data 2017; Testing and Certification Program Manual Version 2.0 2015; Voting Systems Performance and Test Standards: Volume 1 & 2 2002; Cortes, Howard, and Norden 2018):

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. [2]

Upon analyzing these keywords using the KWIC framework, the following three unique facets of American society that have engendered norms surrounding electoral protection are identified: (1) election infrastructure is designated as critical infrastructure; (2) the use of electronic voting machines; and (3) private-public partnerships necessitated by misinformation and disinformation campaigns meant to undermine elections.

Keywords such as the *National Institute of Standards and Technology* (NIST) and other technical terms used to characterize a NIST-approved procedure in responding to a cyberattack upon election infrastructure make clear that *election infrastructure is critical infrastructure*. The Department of Homeland Security 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" (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 2018). 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 is telling that within documents focused specifically on securing election infrastructure, traditional methods of securing critical infrastructure are frequently relied upon, including reliance on a voluntary system of adherence to security standards. Thus, the following American norms are revealed: (1) The value American cybersecurity practices hold for voluntary standardization as a means of security assessment and (2) the extent to which the United States treats election infrastructure as critical infrastructure.

Prominent keywords additionally characterize technical methods of ensuring the integrity of electronic voting machines, which are unique features of the American voting system. KWIC analysis reveals that American cybersecurity practices choose to address the security of electronic voting machines by focusing on the

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

implementation of effective audit and federal accreditation measures, as demonstrated in Table 2. As a result, the following norms became identifiable: (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.

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

The role of misinformation and disinformation management in safeguarding elections is an emerging issue stemming due 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 as demonstrated by the public-partnership efforts that went toward the creation of documents studied in the KWIC analysis.

Although I find that domestic cybersecurity practices do provide valuable insight into American domestic norms, its usefulness in this research is dependent upon its value in an international context. Specifically, the purpose of this research is to understand if, and how, domestic norms are observable in international cyber norms. In doing so, it shows that cybersecurity practices can be used as a means in understanding nations' international behavior as they seek to establish an order of cyber global governance. Furthermore, this research seeks to demonstrate that although the future of cyber global governance is uncertain, we are not helpless in understanding where that path might lead. The United States, when used as a case study, proves as much.

American Cybersecurity Norms in International Practice: The Triumphs and Tribulations

The previously elucidated American domestic norms are analyzed in the context of international norm-setting bodies 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. In conducting this analysis, it demonstrates the usefulness that norms, derived from the analysis of domestic cybersecurity practices, have in understanding how cyber global governance manifests.

Norms of Critical Infrastructure Protection Prevail in the UN GGE

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. The 2015 UN GGE Report was foundational in that all successive bodies of international norms drew inspiration from it and is the first time critical infrastructure protection and international law are acknowledged as being vital components of international norms (Maurer et al. 2020). 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.

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 [information and communication technologies] ICT activity that 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 remarkable resemblance to those present American cybersecurity practices, including those that involve information sharing and cooperation, targeted training of critical infrastructure operators, and the establishment of proper channels to report cyber incidents (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 2018; Grisby 2015; Marks 2015).

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.[3] "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] The 2021 UN GGE report has yet to be published as of the writing of this work. 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.

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

The 2015 UN GGE report not only reinforced the United States commitment to, and successful implementation of critical infrastructure protection norms, 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).

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.

The United States has 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. 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 provide 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. Furthermore, electronic voting machines are subjected to a decentralized accreditation system, in which each state is free to utilize security standards produced by the EAC in the way they best see fit, thus upholding a value for flexibility in standardization.

By upholding international law as the preferred method for governing norms rather than a formal treaty, the United States is able to exercise more freedom in how it conducts itself within cyberspace with the same flexibility it is accustomed to domestically. For example, 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 (Fidler 2016; Segal 2016; United States Department of the Treasury 2019).[4]

Via the 2015 UN GGE report, the United States was successful in gaining international legitimacy for its norms surrounding critical infrastructure, however, other norms valued by the United States did not receive the same level of legitimacy.

The UN OEWG: An Uphill Battle for American Norms of Cyberwarfare

The norms that have caused tensions, and ultimately led to the stalling of the UN GGE in 2017 and creation of the Russian-led UN OEWG, center upon differing interpretations and applicability of the international law of State responsibility and international humanitarian law in cyberspace. The tension is only further exacerbated by 2016 Russian interference and influence in the 2016 United States Presidential Election.

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 its 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.).

American UN GGE-tendered expert 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

[4] 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 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).

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)

Russia makes clear its objection to cyberattacks being contextualized in such a way: as a tool in warfare. In Russian's commentary, it justifies its 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).[5]

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 laws that govern activities of war. The United States' domestic cybersecurity activities indicate as much with the significant emphasis it places on critical infrastructure protection. Critical infrastructure protection programs, and its cybersecurity practices, are a prevalent component of American society and demonstrate how the United States perceives cyberattacks upon critical infrastructure: an action that can be treated as an act of war.

In war, humanitarian concerns take on a new focus and the United States has made clear its normative value that humanitarian law, as such, has a role to play in governing an increasingly militarized cyberspace. As expected, Russian continues to disagree with this characterization, especially when considering what the United States perceives to be the cornerstone of humanitarian law in cyberspace: the significance of Internet freedom.

There is an inexorable, American association between international humanitarian laws and norms and freedom of speech online. For example, 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).[6] The same reverence for Internet freedom was evident on a domestic level.

Internet freedom has been at the center of the American debate regarding one of the most discussed threats to the democratic process: misinformation and disinformation. Vying opinions regarding how to best regulate misinformation spread on large social

[5] 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, another point of contention between the United States and Russia

[6] 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."

media platforms has become significant in the election security. Regardless of a private or public sector association, or affiliation with the Democratic or Republican Party, there remains a key conviction that freedom of speech must be protected while addressing issues caused by disinformation (Big Tech Company's Liability Shield 2020; Hearing Disinformation Online and a Country in Crisis 2020; Business et al. 2018). Unfortunately, this shared ideal across various sectors is the not enough to overcome yet another impediment to the legitimacy of American domestic norms: the fractured multi-stakeholder framework.

The Paris Call and the Global Commission: The Results of the 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 being evident on an international level. The debate over how to protect against misinformation, as discussed in the previous section, is one such embodiment of this struggle.

Social media companies wish to moderate their content in a way that avoids harm to the public and is free from government intervention. Conservatives fear social media companies are using their content moderation abilities to purposefully prevent certain political ideologies from proliferating. Liberals believe that social media companies are not doing enough to curb misinformation efforts.

Across Congressional hearings, technology companies also methodically avoided committing themselves to partnerships with governments. Rather, they elected to establish organizations, solely comprised of private sector entity, meant to protect electoral integrity, such as the Twitter-led Global Internet Forum to Counter Terrorism (GIFCT) (Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Panel I 2017). At the same time, the government has attempted to force private sector entities to be more forthcoming with information pertinent to electoral protection, to no avail.

As a result, the same fractured multi-stakeholder framework has become evident internationally. The private sector and civil society have chosen to 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.

By analyzing private sector and civil society involvement in the Global Commission and the Paris Call, the following domestic norms become observable in an international setting: (1) a stated desire for collaboration with the United States government, with no significant private or public 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.

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. 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 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).

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 (Maurer et al. 2020). The Global Commission departs from traditional public sector norms by endorsing the important role non-state actors have in securing cyberspace and the need for more technical specifications being incorporated in cyber norms that can be aided by private sector entities.

The technical norms developed by the Global Commission are inspired by the recognition that the Internet contains the public core of society since it supports the 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. Consequently, technology companies and other private sector actors are vital components of that public core.

Cybersecurity practices within the United States reveal a particular interest in best reporting practices that are tied to transparent auditing procedures that stem from the use of electronic voting machines. For example, the principle of software independence[7] 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 (Human Factors and Privacy Subcommittee and Security and Transparency Subcommittee n.d.). Furthermore, the Global Commission recognizes the United States' leadership in endorsing this practice through its Vulnerability Equities Processes (VEP), a framework used in determining whether the United States government should 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 of the Global Commission, 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 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). In this way, the Paris Call and Global Commission further support the idea that protecting elections holds a highly influential role in forming cyber global norms. Additionally, these bodies also reflect domestic norms in an international context, including how the domestic multi-stakeholder framework has transcended beyond the United States' borders and the need for enforcing more technical norms.

Conclusion

Cybersecurity practices act as key insight into what nations value and how those values may manifest in an international setting. Through such analysis, it is revealed the United States has a deep concern over the protection of critical infrastructure, especially

[7] Software independence, in the context of the usage of electronic voting machines, is the proposal that purely technological problem, originating with voting software, should not be capable of going undetected in the election as a whole.

regarding how an attack upon critical infrastructure can spur cyberspace into a warzone and thus necessitate the applicability of international law in addressing cyber incidents. Such ideals are successfully reflected in the UN GGE. However, not all observable domestic norms are able to attain the same success.

The tension between Russia and the United States demonstrates how specific areas of international law, such as those related to countermeasures and humanitarian concerns, are so valued by the United States that it led to the stalling of the 2017 UN GGE as well the creation of the UN OEWG, as led by Russia. Furthermore, the United States faces its own internal struggles in which the private sector has taken it upon itself to pursue its own norms and thus leading to a new context in which domestic norms, such as those stemming from the usage of electronic voting machines, can be observed: the Paris Call and the Global Commission.

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 a 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 protect 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).

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).

Becker, David, Jacob Kipp, Jack R. Williams, and Jenny Lovell. 2018. "Voter Registration Database Security."

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

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).

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

"Checklist for Securing Voter Registration Data." 2017.

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

Cortes, Edgardo, Liz Howard, and Lawrence Norden. 2018. "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack."

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).

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.

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).

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.

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).

"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).

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).

Human Factors and Privacy Subcommittee and Security and Transparency Subcommittee. "Software Independence and Accesibility."

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.

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 Telecommunications." *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).

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.

"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).

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).

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).

Testing and Certification Program Manual Version 2.0. 2015. United States Election Assistance Commission.

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

"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 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).

Voting Systems Performance and Test Standards: Volume 1 & 2. 2002. Federal Election Commission.