REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05-05-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
Election Security Development in International Law

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Gaston, Todd J. (Major)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States must prioritize the threat that election meddling operations pose to governmental legitimacy, understand the ambiguity in international law that allows hostile forces to use the law as a shield and the corresponding risk it creates for decision makers, and take a leadershiip role in developing clear standards for cyber conduct to diminish the threat. Starting in the early 2000s, foreign actors began using cyber election influence operations to sway target state populations towards foreign strategic objectives. These operations evolved to include interference operations that target election infrastructure through data manipulation and loss of functionality attacks. The United States and others acknowledge the threat these operations pose but have done comparatively little to create a clear framework for responsive actions. The United States can lead the international community towards certainty to mitigate unnecessary conflict due to election meddling by establishing a tough policy and utilizing the United Nations structures to develop law in the area.

15. SUBJECT TERMS
election security; cyber norms; influence operations; interference operations; United Nations group of governmental experts

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	36	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: ELECTION SECURITY DEVELOPMENT IN INTERNATIONAL LAW

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

MAJOR TODD GASTON

AY 2019-20

Mentor and Oral Defense Committee Member: Jill Goldenziel, Ph.D.
Approved: //Signed//
Date: 21 April 2020

Oral Defense Committee Member: Matthew J. Flynn, Ph.D.
Approved: //Signed//
Date: 21 April 2020

Executive Summary

Title: Election Security Development in International Law

Author: Major Todd Gaston, United States Marine Corps

Thesis: The United States must prioritize the threat that election meddling operations pose to governmental legitimacy, understand the ambiguity in international law that allows hostile forces to use the law as a shield and the corresponding risk it creates for decision makers, and take a leadership role in developing clear standards for cyber conduct to diminish the threat.

Discussion: Starting in the early 2000s, foreign actors began using cyber election influence operations to sway target state populations towards foreign strategic objectives. These operations evolved to include interference operations that target election infrastructure through data manipulation and loss of functionality attacks. Additional tactics also include seizing foreign state media accounts and posting false statements with diplomatic consequences. The United States and others acknowledge the threat these operations pose but have done comparatively little to create a clear framework for responsive actions. The *Tallinn Manual 2.0* sought to identify how international law applies to the cyber domain but its evaluation tools are riddled with uncertainty due to an absence of state practice. That uncertainty creates risk that both friendly and hostile actors miscalculate each other's intentions leading to conflict. The United States can lead the international community towards certainty to mitigate unnecessary conflict due to election meddling in several ways. The United States should publicly establish a tough policy with identified responsive actions to these operations. The country can then utilize United Nations structures including the Group of Governmental Experts and the Internet Governance Forum to develop longer-term solutions for norms, customary international law, and treaty-based obligations.

Conclusion: The global community is prepared to take the next step towards certainty in combating election influence and interference operations. The United States should utilize frameworks articulated in the *Tallinn Manual 2.0*, expound on ambiguous areas to combat current threats, and leverage the United Nations to develop long-term solutions.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

I. Introduction

The 2024 U.S. presidential election cycle is filled with polarizing stories and partisan attacks. The U.S. electorate continues to gather and discuss information from online news outlets and social media platforms. Foreign actors are promulgating misinformation stories to sway the American voter to elect a candidate favorable to their interests. Analytic research shows that only a sliver of the U.S. population is willing to cast their vote for an opposing political party and the foreign actors are specifically targeting that audience. The actors also conduct cyber operations to gain sensitive information from political candidates to help sow discord in the system and undermine the opposition. Some misinformation from the foreign actors is cloaked in the guise of official U.S. government statements to further influence the population. Hostile cyber tools reside in election infrastructure that are prepared to shut down voting systems and skew the vote utilizing fake voter registration rolls if needed. The hypothetical foreign actors' candidate wins the election by a slim margin and the American people are left outraged by the specter of impropriety surrounding the process.

The problem of foreign cyber influence and interference operations targeting key election processes in democratic nations around the world is a challenge that countries now face. Misuse of information and communications technology (ICT) by great power competitors, regional drivers of instability, and violent extremist organizations is a critical global security problem.[1] Hostile actors that utilize electronic espionage coupled with data manipulation to project power threaten the United States and the global community.[2] While not a traditional armed attack of one nation against another, these operations form part of a cyber threat that, "could precipitate massive economic and societal damage."[3] Therefore, the United States must prioritize the threat that election meddling operations pose to governmental legitimacy, understand the ambiguity in

international law that allows hostile forces to use the law as a shield and the corresponding risk it creates for decision makers, and take a leadership role in developing clear standards for cyber conduct to diminish the threat.

II. Threat Vectors for Cyber Election Influence and Interference Operations

Military commanders and government decision makers can seek numerous effects through cyber operations. They range from merely conducting defensive network operations, to cyber intelligence, surveillance, and reconnaissance, all the way to operations having destructive physical effects in the real world. Among these operations is the increasingly concerning use of election influence and interference operations intended to mislead populations and detract from their overall faith in the electoral process. These operations threaten all populations charged with electing their leaders excepting those authoritarian regimes less at risk of an incompetent public unwittingly suborned to a foreign power. The methods foreign actors are using to fulfill their objectives are constantly evolving and can seek not only to spread targeted misinformation, but also manipulate election infrastructure. Recent escalation should inform both military commanders and policy makers of the need to prioritize this threat. Before assessing recent operations, readers should understand that states can be unlikely to publicly disclose that they are the victim of cyberattacks, including influence and interference operations, for a variety of political, strategic, and operational reasons.[4] Additionally, classification challenges frequently limit discussion and public attribution. As such, evaluating the extent of attacks and responsive action provides an imprecise assessment of capabilities and growing norms of behavior.

First, consider Russian cyber election operations against Ukraine. Russian operatives reportedly intervened in Ukraine's elections starting in 2004.[5] Their tactics included the use of social media and misinformation campaigns indicating that "Ukrainian children are forced to

play with stuffed Adolf Hitler dolls and that Ukraine's national church 'is becoming the Christian version of ISIS.'"[6] Their tactics grew over time to include both influence operations and election infrastructure interference in the 2014 Ukrainian presidential election. Russian operations rendered Ukrainian voting systems inoperable and disclosed evidence of its success to the Ukrainian people.[7] This disclosure was likely aimed to impact voter turnout and demonstrate Ukrainian ineffectiveness. After officials fixed the infrastructure, the attack continued with a virus that would manipulate the vote totals showing Dmytro Yarosh as the winner with 39 percent of the vote and his opponent only receiving 29 percent.[8] Although Ukrainian government cyber actors found and removed the virus less than an hour before broadcasting the correct election results—in which Yarosh received less than one percent of the vote—a Russian-owned news channel broadcast the manipulated data as the actual outcome.[9] This cyberattack demonstrated the possibility of mutually supporting influence operations along with a targeted interference attack and data manipulation. Democratic governments must take steps to counter such threats.

Russia continued these tactics against the United States. In 2016, Russian trolls and automated bots maneuvered voters towards one particular candidate; they focused on, "attacking the American social fabric where it is most vulnerable, along lines of race, gender, class and creed."[10] These efforts were multiplied by the breach of the Democratic National Committee's (DNC) computer system and public posting of emails with the aim to further influence the electorate.[11] To complete the operation, the actors targeted twenty-one states' election infrastructure with some success.[12] A subsequent Director of National Intelligence report found with high confidence that the Russian president ordered this influence campaign in order to

"undermine public faith in the US democratic process, denigrate Secretary Hillary Clinton, and harm her electability and potential presidency."[13]

The Russian cyber campaign persisted through the 2018 U.S. midterm elections. Though Russian and other foreign actors were unable to penetrate election infrastructure due to U.S. Cyber Command actions, Russian actors continued their influence campaign to mold the U.S. government consistent with their strategic aims.[14] These efforts led President Donald Trump to declare a national emergency to deal with the "extraordinary threat to the national security and foreign policy of the United States" by foreign actors seeking to "undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation."[15] A DNC lawsuit against Russia (and others) also identified that those believed to be Russian operatives conducted a spear-fishing campaign targeting numerous party emails.[16]

In addition to these efforts, Russian actors also engaged in a multi-stage cyber campaign against the United States from reconnaissance through installation and exploitation of other critical infrastructure assets in the energy, manufacturing, and nuclear fields.[17] Russian tactics included utilizing staging targets on the periphery to ultimately gain access and impact intended targets.[18] These tactics will combine with their counter-election campaigns to create a broad offensive against U.S. democracy that commanders and policymakers must consider in determining how to protect U.S. interests.

In addition to Russia, other actors have now targeted the 2020 U.S. presidential election.[19] Iranian groups utilized similar tactics in seeking to infiltrate campaign email accounts of prominent personnel, U.S. officials, and journalists.[20] The Iranian cyber operation lasted approximately one month wherein the group made over 2,000 attempts to gain access to

Microsoft email accounts.[21] This may have been one operation in a line of escalatory actions between the two countries.[22] Whether influence operations targeted at the U.S. political system are escalatory is debatable but the tactic shows the ease with which foreign powers can impact the United States.

Germany suffered a similar campaign in its 2015 election at the hands of Russian-connected actors. First, the group brought down the German parliament's website; then they gained access to the parliament's servers for several months enabling data collection and manipulation.[23] Chancellor Angela Merkel's political party, the Christian Democratic Union, also suffered multiple intrusion attempts but the party declined to indicate the severity of any potential breach.[24] However, the German government remains wary and poised to act if the Russians use captured documents in a possible future misinformation campaign.

Not all recent influence campaigns come from eastern nations against those in the west. China's civil-military cyber force recently began influence operations against Taiwan by disseminating misinformation; the goal of these operations was to undermine Taiwanese President Tsai Ing-wen.[25] Whether or not these operations actually swayed the election is difficult to determine, but Tsai Ing-wen's Democratic Progressive Party suffered a "huge defeat" in the local elections causing her to resign as leader of her party.[26] China not only engages in misinformation campaigns, but interferes in election infrastructure as well. China, along with Russia and other actors, carried out multiple attacks against the Indonesian voting agency in 2019 to manipulate presidential and legislative elections and create "ghost voters."[27] Thus, China has shown the capability and willingness to undertake operations similar to Russian cyber election campaigns.

In May of 2017, the United Arab Emirates (UAE) took the next step. They commandeered Qatari state social media and news agencies for two days.[28] During that time, the UAE actors posted, "fiery but false quotes linked to Qatar's emir," causing the UAE, Saudi Arabi, Egypt, and Bahrain to cut diplomatic ties. [29] This tactic appears similar to other influence operations aimed at public persuasion, but the escalation to creating false posts by government actors on government media platforms can cause hastier changes in foreign relations.

The United States is beginning to understand the challenges posed by cyber operations targeting a nation's election process. The former Director of National Intelligence, Daniel Coats, in the 2019 Statement for the Record to the Senate Select Committee on Intelligence highlighted that U.S. "strategic competitors will increasingly use cyber capabilities – including cyber espionage, attack, and influence – to seek political, economic, and military advantage over the United States and its allies and partners."[30] He noted that while Russia and China pose significant espionage threats, the U.S. is also likely to face this asymmetric threat from potential adversaries, including violent extremist organizations, in the future.[31] These bad actors are learning how to manipulate the American population through "social media to alter how we think, behave and decide."[32] Attacks are also aimed "to directly manipulate or disrupt election systems – such as by tampering with voter registration or disrupt[ing] the vote tallying process – either to alter data or to call into question our voting process."[33] Of note, the updated Worldwide Threat Assessment changed in 2019 to now categorize "Online Influence Operations and Election Interference" as its own threat category similar "Weapons of Mass Destruction Proliferation." This realignment shows a growing strategic concern of such operations in the information environment as adversaries, "try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere."[34]

Despite these realizations, the United States has taken relatively few actions to prioritize this threat, lead the world towards a unified approach to combat election meddling.

III. Ambiguous Legal Repercussions

One line of effort to mitigate the serious threat posed by election meddling is through lawfare. The term "lawfare" gained notoriety and acceptance in the mid-2000s and stands for a strategy that includes the use (or misuse) of law to reach operational or strategic objectives.[35] The key feature is to use aspects of the legal system and tools like contracts achieve a certain effect.[36] The current international legal regime applied to cyber operations is underdeveloped and allows hostile actors to shield their election meddling campaigns as potentially lawful or otherwise minor illegal encroachments. Uncertainty in how a state can and should respond to hostile cyber operations amplifies the danger of escalation towards war and thus contributes to regional and global instability. Accordingly, the United States should employ a legal line of effort to clearly define what constitutes an internationally unlawful cyber act and the nature of appropriate state responses. Imposing these clear international laws and will produce the desired effect of lessening the frequency and severity of election meddling operations by creating a clear deterrent regime that increases the cost of such operations and prevents hostile actors from using legal ambiguity as a shield. An assessment of the current international legal rules applicable to cyber operations will demonstrate the areas of ambiguity used as a shield as well as the avenues for the United States to achieve the desired effect.

Public international law stems from states committing themselves to treaties or through customary international law (CIL). Cyber operations have yet to be the subject of or explicitly incorporated into an internationally agreed-upon treaty similar to the Geneva Conventions of 1949. Thus, the basis for legal restraints must come from previously established treaty law or

CIL.[37] Customary international law is established by general practice by states AND is acknowledged as a legal obligation.[38] States have made few indications of whether and how they will apply the law to the cyber domain. However, many in the legal community have come to rely on the *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations* as a guidepost.[39]

The development of the *Tallinn Manual 2.0* stemmed from state concerns regarding emerging operations in the novel domain. Estonia initially recognized the need for a coordinated cyber effort and proposed that the North Atlantic Treaty Organization (NATO) adopt a cooperative cyber defense center of excellence (CCDCOE) in 2004.[40] Ultimately, NATO adopted and accredited the institution that subsequently called for an "'International Group of Experts' [IGE] to produce a manual on the law governing cyber warfare," in Tallinn, Estonia in 2009.[41] Shortly thereafter, the United States recognized that existing CIL applies in cyberspace but acknowledged that, "unique attributes of networked technology require additional work to clarify how these norms might apply. . . ."[42] The U.S. policy did identify principles and emerging norms to guide future development.[43] This U.S. acknowledgment identified the broad boundaries of an otherwise undefined domain.

After a rigorous analytic process, the IGE published the *Tallinn Manual On the International Law Applicable to Cyber Warfare* in 2014 that applied the laws that states use as a basis to go to war and the rules applicable within war to the cyber domain. The IGE recognized that cyber operations below the level they perceived as an armed attack, such as cyber espionage, intellectual property theft, and other criminal activities, "pose real and serious threats to all States" but were beyond the first manual's scope.[44] As a result of the first manual's acclaim and the increasing frequency of cyber threats along the range of military operations, the NATO CCD

COE convened a new IGE in 2013 to expand the manual to include cyber operations short of war.[45] In addition to the large panel of the IGE, over 50 states also provided insight in a non-attribution environment. This inclusive effort ideally endowed the final product with an increased likelihood that the international community would approve of its application of existing laws.

First published in 2017, the IGE put forth *Tallinn Manual 2.0*, a 500-page comprehensive volume aimed to capture the law as it existed at the time without regard to politics or policy.[46] The text captured disagreements among the experts, which highlighted the challenges in actual application of the rules as many of the disagreements centered around application scenarios. Meanwhile, a United Nations Group of Governmental Experts (GGE) published consensus reports in 2013 and 2015 that recognized that "existing obligations under international law are applicable" to information and communications technology (ICT).[47] This recognition is a useful first step but it did little to actually narrow down how states should apply preexisting rules or if there even is a preference towards the *Tallinn Manual*. The *Tallinn Manual* provides a workable framework as a backdrop for future development and a restatement of broadly applicable law, but it does not reduce the ambiguity that hostile actors use as a shield or offer leaders flexible, deterrent options.

A. Cyber Armed Attacks or Use of Force

A starting point for the vague application of international law to the cyber realm should begin with recognized self-defense requirements. The U.N. Charter requires that states refrain, "from the threat or use of force against the territorial integrity or political independence of any state."[48] However a state may resort to self-defense measures when subject to an armed attack.[49] The *Tallinn Manual* extends these requirements, and the corresponding scale and effects test for

determining an armed attack, to cyber operations.[50] The commentary to the *Tallinn Manual* rule makes clear that physical damage and destruction from a cyber incident is easily understood in this paradigm (e.g. the 2010 Stuxnet attack against Iranian nuclear facilities).[51]

However, neither the IGE nor subsequent analysis found consensus on what scale and effects requirements for cyber operations causing "nondestructive or injurious consequences" justify a self-defense response.[52] The renowned general editor of both *Tallinn Manuals*, Michael N. Schmitt, is of the opinion that the 2016 Russian election meddling does not reach the scale and effects of an armed attack.[53] This opinion is only as good as the certainty, or lack thereof, that it provides to strategic decisionmakers. At the time of the event, President Obama is reported to have warned Russia of a potential U.S. response to their 2016 cyber election operations based in the law of armed conflict and other international norms; the reference to a law of armed conflict response indicates that at least one decision-maker may have viewed these cyber operations as meeting the armed attack threshold.[54] Leaders around the world could also view President Obama's subsequent statements regarding future actions as either adopting an expansive view of the *Tallinn Manual* rules or merely a new norm irrespective of the proposed rules.[55] Scholars Dan Efrony and Yuval Shany also point out that the United Kingdom Prime Minister Theresa May's comments indicating that "[t]he UK will do what is necessary to protect ourselves, and work with our allies to do likewise," may indicate a growing view that these cyber election operations are an international law violation.[56] The "protect ourselves" language could imply that a self-defense response utilizing cross-domain kinetic operations is appropriate or merely indicate a lesser legal violation. In either event, these statements demonstrate the uncertainty the United States, partners, and foreign actors face in responding to these operations.

The *Tallinn Manual* IGE also grappled with the question of whether the potentially lower "use of force" standard in the U.N. Charter encompasses force that would otherwise not reach the high bar of an armed attack. The U.S. position remains that any use of force constitutes an armed attack and justifies self-defense.[57] The IGE adopted the position of other states that there is a difference between the two standards and determinative to the analysis is a use of force's lesser degree of impact given the scale and effects.[58] It is unclear how many states currently believe there is actual daylight between the two criteria and, if so, how states view this in the cyber realm. The fallback position appears to be to identify similarities to potential kinetic operations that may meet that narrow space.[59] Accordingly, states believing there is a difference between the two standards will not use self-defense towards all cyber uses of force, but they may be able to articulate justification for stricter countermeasures to combat such actions.

Experts recognized during the 1945 drafting of the U.N. Charter, that mere economic coercion or political pressure was deemed insufficient to qualify as a use of force.[60] The IGE, seemingly using this as justification, put in the Rule 69 commentary that, "non-destructive cyber psychological operations intended solely to undermine confidence in a government" did not meet the use of force standard.[61] While this rule is historically appropriate, the complexity of cyber-enabled influence and interference campaigns are more egregious and not rightly characterized as political pressure. Furthermore, undermining confidence in the government can include a host of less significant operations than challenging election processes at the core of a nation's political independence. Another challenge could also develop as states start to seek a persistent presence in the cyber domain. A state may not be able to discern operations seeking to undermine a government over time from those that target an election. That challenge will lend even more uncertainty, increase the touchpoints with hostile actors, and bend the international

community towards instability as states seek to defend their political independence. Alternatively, cyber election meddling could suffice an international law violation under the *Tallinn Manual* in two other ways: a violation of sovereignty or a breach of the duty to not interfere in the activities of the State. These violations are less egregious international law breaches and thus do not constitute armed attacks or justify self-defense.

B. The Sovereignty Debate

Sovereignty as a principle is the concept that states have the supreme authority over what happens within their own borders.[62] This principle is the foundation for and begets numerous international laws. Yet, there is debate as to whether sovereignty serves as an independent rule capable of violation in the cyber realm. Those that believe a threat actor can violate the cyber rule of sovereignty have varied opinions on the type of intrusions that constitute a violation. Others view sovereignty as merely a principle whose breach is not an international law violation. The uncertainty regarding a cyber sovereignty rule makes it more likely that hostile actors will continue to probe the seams discussed below and persistently confront leaders across the domain.

The *Tallinn Manual* defined the cyber sovereignty rule as a state's right to control cyber activities and infrastructure within its territory, and that its violation constitutes a breach of international law.[63] Schmitt also independently found a basis for this determination in a 2015 U.N. GGE report along with an in-depth review of public international jurisprudence.[64] The *Tallinn Manual* identified two independent tests that create a sovereignty violation. Though two checks on conduct may appear to encompass more behavior as a violation, they could actually produce more gaps for exploitation.

The first test is based on the level of infringement upon a state's territorial integrity.[65] The three factors the IGE used for assessment are 1) physical damage, 2) loss of functionality of

cyber infrastructure, and 3) infringement upon territorial integrity less than loss of functionality—actions like altering or deleting data and installing backdoors; a violation does not require all three factors. [66] Though the IGE reached consensus in some areas – notably physical damage – the experts could not specify the extent of behavior necessary for a violation relating to functionality due to a lack of state practice indicating a legal obligation.[67] The IGE agreed that a functionality violation could stem from actions forcing a country to replace infrastructure or reinstall software or data. Though Russia targeted and gained entry to election infrastructure in the 2016 U.S. presidential election, the system remained functional. The 2014 Ukrainian data manipulation set to skew results could be considered a temporary loss of functionality given the purpose of the infrastructure, or as an impact less than loss of functionality. Similarly, the UAE control over Qatari state media systems could also fit as a significant but temporary loss of functionality. Schmitt found that the mere entry or presence of Russian cyber actors in U.S. election infrastructure and its corresponding influence campaign was insufficient to justify a violation in the less than loss of functionality criterion.[68] Despite this determination, Schmitt did recognize that "it is impossible to draw definitive red lines regarding cyber election meddling" under this rule.[69] The ambiguity problem remains that a state could view such actions as a violation that justifies an unexpected, escalatory responsive countermeasure.

The second method of a sovereignty violation is the usurpation of an inherently government function. The group could not define what an inherently government function included but recognized that usurpation of that activity is a violation since the government should enjoy the exclusive right to conduct those activities.[70] Examples include "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, [and] the effective conduct of diplomacy. . . ."[71] As Schmitt identified,

cyber interference operations to manipulate election data or even limited distributed denial of service attacks against election infrastructure are sovereignty violations.[72] However, he noted that the regularity of election propaganda campaigns by foreign actors does not suffice for such a violation.[73] In this view, only the 2014 Ukrainian attempted data manipulation and possibly the Qatari media campaign qualify as a sovereignty violation.

While Schmitt's assessment stemmed from the application of historical propaganda campaigns, the nature of targeted information consumption and the rapid spread of propaganda increases its threat the cyber environment. The cornerstone of free and fair elections is that the electorate is able to make educated choices regarding their representation. The population must evaluate sources and be prepared to assess whether domestic actors are skewing the truth for their own ends. However, when foreign actors masquerade as individuals from the state to implant false stories for foreign benefit, it is unreasonable to expect the electorate to be sufficiently savvy to evaluate that media. Mr. Schmitt did recognize a possible sovereignty violation argument in the case of the Russian 2016 influence campaign since the Russian propaganda coincided with targeted data exfiltration and "weaponized" release.[74] Yet this nuanced approach will exacerbate the scale, effects, and harm of future influence campaigns as it affords hostile actors various avenues to shield their behavior.

A corollary example identified by the IGE included a violation for usurping communications among state leadership but not merely posting information on a website.[75] Schmitt identified this as being a significant gray area between the things that we know are inherently governmental activities, like law enforcement and security, and those that are clearly not – commercial activities.[76] Under this construct, the UAE fake communications by the Qatari Emir may count as a sovereignty violation though the use of fake stories falsely issued under the

name of the Qatari news agency may not. The electorate's ability to assess information is even more challenged when they are asked to evaluate whether state communications truly emanate from the state. Although impersonating government officials and usurping communications may constitute domestic law violations in some states, such an avenue for redress has proven inconsequential and ineffective. Vague international standards will not stem hostile actor operations.

Conversely, Colonel Gary Corn, writing as the Staff Judge Advocate for U.S. Cyber Command, maintains the alternative viewpoint. His view is that sovereignty is merely a principle for the cyber domain and that violating the proposed *Tallinn Manual* sovereignty tests does not create an international law violation.[77] This position stems from "insufficient evidence" that sovereignty as a rule is CIL, and that the threshold of harm from traditional violations of territorial integrity are much more significant compared against the limited impact of cyber operations.[78] Colonel Corn notes that the varied international law regimes applied to the air, space, and sea domains "underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace."[79] As merely a sovereignty principle, it "does not obligate other states to refrain from all activities that might infringe upon or operate to the prejudice of the territorial state's internal sovereignty."[80] In this view, espionage and influence operations purely subject the foreign actor to domestic prosecution or diplomatic pressure.[81] The United States and the DNC took such domestic legal actions against Russian intelligence officers and companies for their 2016 and 2018 influence operations. [82] Such action offers little in the effort to clarify what is prohibited by international law and possibly less as a deterrent effect given that the Russian actors will suffer few consequences. Consequently, the beginning of an

effective deterrent strategy may include endorsing clear standards for sovereignty as a rule or elevating such conduct to the level of a use of force.

Colonel Corn's view is shaped by challenges he notes in current operations. While cyber operations should consider the principle of sovereignty in their planning and execution, he finds that the above sovereignty rule is overly restrictive in combatting transnational violent extremist organizations (VEO).[83] Such a rule would require U.N. Security Council authorization or host nation acceptance to target a VEO's cyber infrastructure abroad.[84] While generally the same requirement for lawful kinetic operations, the level of impact to the host nation from these cyber operations is de minims. Additionally, the countermeasures (a limited response to a sovereignty violation) structure under the *Tallinn Manual* is only available against a state; the state duty of due diligence against VEO cyber operations appears too difficult to actually attribute a breach of that duty.[85] As such, states operating against a VEO would be left with comparably few arduous options if cyber sovereignty is a rule.

These difficulties underscore the dilemma states face in developing clear standards. Ambiguous laws allow states freedom of movement in the cyber domain and greater flexibility in taking responsive cyber actions against adversaries, including VEOs. Though cyber operations against VEOs may have relatively limited impact compared to physical sovereignty breaches, election meddling operations pose a significant threat such that legal ambiguity will foster unexpected escalation and likely cross-domain operations. Clear sovereignty as a rule standards will help safeguard electoral processes by permitting responsive action to election meddling while also incorporating such violations into the broader deterrence and response international framework. In the absence of a sovereignty rule, cyber operations less than a use of force are only prohibited by the law of nonintervention.

C. Nonintervention

The law prohibiting intervention in another state's affairs is widely recognized by states and stems from the sovereignty principle. This law may capture some activities discussed above given a breach requires both that the act in question relates to the internal or external affairs of the state, and that the act is coercive.[86] The determination of qualifying affairs includes the "choice of a political, economic, social, and cultural systems, and the formulation of foreign policy.[87] The United Nations and others identified that this also includes a state's ability to conduct elections."[88] Thus, scholars recognize that cyber operations impacting the process or the outcome of elections violate this first prong.[89]

The coercion element thus becomes dispositive. Coercion, both direct and indirect, is more readily apparent when a state uses classic military force to achieve its ends.[90] The *Tallinn Manual* attempted to expand upon this understanding and included acts "designed to deprive another State of its freedom of choice," and emphasized that the state's actions would be "involuntary."[91] Schmitt found that the Russian 2016 cyber influence campaign did not rise to the level of coercion as it was simply false or slanted reporting.[92] However, he, the IGE, and others acknowledge the relative novelty in determining how to apply the element to cyberspace.[93] Thus, U.S. policy makers could claim that the "covert" 2016 Russian campaign utilizing "troll operation[s]" to the benefit of one particular candidate could be coercive.[94] Russian actions against Ukraine likely suffice as a breach under this broader interpretation, and possibly the Chinese campaign against Taiwan as well. Even under a narrower interpretation, the UAE cyber operations against Qatar would likely be sufficient coercion had they been in the context of an electoral campaign. With the coercion element met, states could respond to violations with appropriate countermeasures without being deemed the aggressor.

A broad interpretation of the coercion element is appropriate in the election context given that an essential element of the electoral process is an informed electorate. The absence of a clear position or even some impression of a likely U.S. response will continue to enable hostile actors to threaten U.S. and allied political independence. The Russian election interference and influence campaigns over the last two decades against Ukraine and their continued effort to undermine U.S. democracy demonstrate the ineffectiveness of silence. The Russian attacks against the 2016 U.S. presidential election morphed into an influence campaign targeting the 2018 congressional elections, and now resume in the 2020 presidential election targeting both the president and his leading challenger.[95] Threats met only with defensive actions to prevent significant impact is unlikely to change this cycle in the future. Commanders and policy makers must take a firm stance against electoral influence and interference operations. Doing so requires them to advocate for clarity in the application of these international law rules and then to vigorously enforce those rules. Given the low cost to foreign actors in conducting these campaigns, demanding responses that could include military components are appropriate.

However, an examination of major attacks across the spectrum in 2018 demonstrated a "cautious approach" to application of the *Tallinn Manual* rules, especially in the realm of use of force determinations.[96] This cautiousness is partly a result of the difficulty in establishing attribution sufficient to justify responsive actions to the international community.[97] Imposition of countermeasures against infringing nations to bring them back into compliance as well as acts of retorsion (lawfully acceptable but diplomatically painful acts such as closing embassies or limiting foreign access to markets) provide no insight on whether states are adopting aspects of the *Tallinn Manual* given the limited official communications surrounding such actions. States appear to be pursuing at least one of a three options: 1) optionally applying the *Tallinn Manual*

rules, 2) utilizing both acknowledged and unacknowledged pathways, or 3) distinguishing between what will generate a response and what will not.[98] Even if states advanced the *Tallinn Manual* commentary and interpretations, uncertainty will remain. States should not wait until after growing cyber operations lead to a kinetic war to take a position. They should advocate for strict accountability measures to ease attribution problems and permit self-defense responses to counter the attacks against a state's cyber infrastructure, sovereignty, and political independence.

IV. Developing Timely, Lasting Certainty

Despite the multitude of other cyber lines of operation, the focus on election influence and interference highlights the uncertainty that both operational and strategic decisionmakers face when confronted by hostile actions. Uncertainty increases the potential that leaders will use cyber and the other elements of national power in response to such actions in unpredictable ways. As the United Kingdom Attorney General noted in 2018, "[t]he very pervasiveness of cyber makes silence from states on the boundaries of acceptable behavior in cyberspace unsustainable."[99] He noted that such silence would lead "cyberspace to continue to become a more dangerous place."[100] Accordingly, the United States must take a leadership role in advancing clear international laws to avoid unnecessary and unexpected provocation before it leads to conflict.

First, the United States must publicly identify an unequivocal position against election influence and interference operations and specify them as a violation of international law. As noted above, history supports considering these operations as a violation of the law of nonintervention. Expanding the range of permissible responses, to include cross-domain deterrent operations and possibly to elevate counter-election campaigns to a use of force status, would be prudent. The United States must also identify the types of appropriate kinetic and non-

kinetic responsive actions it views as a proportional response to adequately deter hostile actors. In either scenario, foreign hostile actors will understand the elevated consequences of continuing such operations and thereby reduce their occurrence.

Second, the United States must gain international legitimacy for the above interpretation. Utilizing an expansive view of the *Tallinn Manual* rules is a start. Given the number of state observers to the *Tallinn Manual* process, the highly respected experts responsible for its development, and its stated position as the law in existence, an expansive view can provide the United States firm public footing. Further, leaders can justify an expansive view of the rules to help produce clarity and advance the state of the law in the relatively novel domain. Such action by states is not new. China, Russia, and other central Asian nations submitted an initial and then a revised code of conduct for cyber operations in 2015.[101] The Chairman of the 2017 ASEAN Conference on Cybersecurity also noted that his organization is attempting to move towards "basic, operational and voluntary norms of behavior" to enhance trust, build confidence, and bring about economic prosperity.[102] The Chairman linked that effort to the U.N. report calling for the application of the current international law regime to cyber operations.[103] Additionally, the 2018 Paris Call for Trust and Security in Cyberspace is a French-led effort supported by 76 states to "face new threats endangering citizens and infrastructure," focused around nine principles of cyberspace.[104] The Paris Call's third principle is to "[d]efend electoral processes," which includes "prevent[ing] malign interference by foreign actors . . .through malicious cyber activities."[105]

These norm-building actions demonstrate the global willingness to provide certainty and provide moral legitimacy to defend elections. While norm development is essential to progress, it does not support timely change in light of current cyber threats. The United States should

make this development a priority consistent with the U.S. National Cyber Strategy of 2018 that details the necessity of "[s]ecuring our democratic processes" and the imperative to "coordinate the development of cybersecurity standards and guidance."[106] Other nations are coalescing around the need for such development as well. As of this drafting, 80 countries have published cybersecurity strategies or cyber-related goals similar to the U.S. strategy, many of which focus on improving security, resilience and advancing economic prosperity.[107] Articulating and defending a position will help counter current threats and serve as a marker for a broader cyber CIL discussion.

Finally, the United States must lead the United Nations in developing a cyber-focused treaty to lend additional certainty. The U.N. General Assembly adopted resolution 73/179 in December of 2018, "[e]xpressing the concern about the spread of disinformation and propaganda, including on the internet" and its ability to mislead, violate rights, and incite violence and hatred.[108] Coupled with a new U.S. position regarding election meddling, the international community may finally emerge from its silence regarding these operations and coalesce around an agreement. The United States should emphasize that this is the logical next step from the Russian and Chinese 2015 revised code of conduct circulated through the United Nations that recognized the necessity to mitigate risk by creating legal certainty and called upon member nations to not use ICT to undermine political and social stability.[109] As treaty development typically occurs over a long timeframe, the United States should also take a leadership role in the frequent United Nations' GGE given their position in addressing international cyber challenges. The GGE, which reached broad consensus on a variety of cyber issues including a ban on using proxies for unlawful acts, met five times from 2004 through 2017 and was composed of between 15 and 25 members.[110] Though the GGE found that United

Nations should take the lead in future cyber rule development, the United States should drive the process as a prominent stakeholder.[111]

The United Nations recently split the cyber burden into two groups. The first, an Open-Ended Working Group (OEWG), is open to all states and will discuss cyber security amongst members as well as industry leaders, civic organizations and academia (with a report due in 2020).[112] The second group is another GGE of 25 members and seeks to include discussions with international organizations such as the African Union, European Union, the Regional Forum of the Association of Southeast Asian Nations and others (with a report due in 2021). This GGE will include many western states as well as China, Japan, Russia, and Indonesia.[113] The United States will need to articulate its election meddling position in these groups to gain support and additional legitimacy while also advancing cyber rules applicable to other contexts. As all of these actions will take place over the long-term, the United States must also use other venues to advance its position.

The U.N. Internet Governance Forum (IGF) is the best consistent option to advance U.S. interests. The IGF started in 2006 with the goals to discuss public policy related to internet governance, facilitate communication among states and nonstate stakeholders, identify emerging issues, and consider overall internet infrastructure concerns.[114] The IGF is an annual meeting of diverse stakeholders. The latest cycle had 2,403 individuals in attendance with 21 percent as government representatives, 22 percent from the private sector, 34 percent from civil society, and 14 percent from the technical and academic communities.[115] The United States can use the IGF to build consensus and move priorities onto the international agenda, which is consistent with the IGF's mission.[116] The IGF is already working along this line of effort by recognizing in

November of 2019 the "indispensable" nature of trust building and cooperation to solve the "the low-intensity cyber-conflict between major States." [117]

The United States can also use the IGF coupled with the GGE and OEWG as a clearinghouse for similar efforts around the globe. The UN Secretary-General already tacitly acknowledged the challenge of numerous parallel efforts when he announced the appointment of a "Technology Envoy" with the mission to advance an international cyber framework.[118] The United States should coopt that position and ensure that nongovernmental organizations utilize these processes in the future. The International Committee of the Red Cross (ICRC) already put forth a December 2019 statement calling for the "development of law or norms . . . [built] on existing rules."[119] Further, organizations like the Global Commission on the Stability of Cyberspace are also seeking to "develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace."[120] Similarly, Microsoft has been emphasizing the need for a "Digital Geneva Convention" to protect the public since 2017.[121] While the numerous ideas can spark ingenuity, the plethora of opinions and fora will grind U.S. efforts to a halt. The United States must acknowledge the value these organizations offer and also ensure that the organizations understand that the IGF is their appropriate forum for cyber advancement. Thus, IGFs are an excellent opportunity for the United States to bring both senior political, military, and business representatives together to further cyber certainty goals. The IGF provides a mid-term avenue for cyber progression to complement the U.S. short-term policy announcement, and the relatively longer-term CIL and treaty development goals at the United Nations.

V. The Case for Patience

The United States retains alternatives to the challenging work of developing a comprehensive international legal regime. First, any effort at treaty or CIL development will require significant time and political capital for relatively minimal effect. Ever since Russia began its effort at normalization in 1999 and Estonia called for development in 2004, minimal progress has actually taken place. There are no more standards of conduct today than there were at the advent of the domain. The international community has expressed ambiguous standards that do not amount to any chargeable violation of international law. It will be even more difficult to gain international acceptance for rigorous, defined standards when two of the five members of the U.N. Security Council actively employ highly successful election meddling operations.

Second, even if the United States developed a workable international law paradigm, it may not successfully increase costs on threat actors. The typical avenue of redress for a violation of international law short of an armed attack is to protest at the United Nations (of dubious utility) or to utilize the International Court of Justice (ICJ) in The Hague, Netherlands. Though the ICJ option may be appealing for some states, the United States has so far been unwilling to cede jurisdictional authority for international law disputes to the ICJ. Thus, any low-level violation has functionally no useful method of recourse under international law.

Third, elections differ by state as sovereign expressions of control and most states will want their processes divorced from international law reins. Many states will see any international regulation of elections as a challenge to their sovereignty. Russia, Iran, the Democratic Republic of Congo, and others have historically sought to use their power to prevent free and fair elections. Additionally, some governments may even support the influence of foreign powers to achieve their desired ends. In western states, the priority of free speech is so

great that those states may not be able to effectively differentiate between foreign influence operations and legitimate speech. Further, states that seek redress can develop domestic laws to criminalize election meddling as they see fit, seek extradition of bad actors, seize the actors' assets pending trial, and levy sanctions against the offending state.

Finally, any additional development of international law for the cyber domain will undercut the effectiveness of U.S. Cyber Command (CYBERCOM). They have proven successful at stopping threat actors from impacting the U.S. 2018 elections. In the future, CYBERCOM will continue to meet threats forward in the cyber domain and can adequately safeguard U.S. elections. As Colonel Corn indicated, CYBERCOM utilizes these gray areas to conduct a range of military operations against VEOs and others, from intelligence gathering to financial and computer network disruption. Imposition of defined boundaries will likely slow future operations by requiring consent from the state physically controlling servers or a strategic calculation that a foreign state is unwilling or unable to combat the threat. Imposition of those requirements will limit CYBERCOM's ability to act rapidly, defend forward, and defeat threats before they manifest in the United States.

V. Conclusion

Cyber election influence and interference campaigns pose a significant threat to sovereignty and political independence. Though the United States, other countries, and nongovernmental organizations all realize the seriousness of the threat, none have successfully used the international legal regime to diminish the likelihood of continued election meddling.

The sovereign powers of one state are insufficient to impose the necessary costs on foreign hostile actors. A state can develop its own laws criminalizing foreign election meddling and even create stiff penalties. However, the majority of hostile actors are outside of friendly

state jurisdiction. For the United States, use of the international extradition process to bring perpetrators back to the United States for justice is unworkable. The United States only maintains extradition agreements with two-thirds of states and they are filled with varying terms – some require extradition, some permit it, some only allow it for U.S. citizens, some provide exceptions for political requests, and many prevent extradition of their own citizens.[122] Moreover, U.S. or joint investigatory processes, including valid international searches and seizures, are complex and present political questions of their own.[123] Combined with the difficulties of using CYBERCOM acquired intelligence in the judicial process, the likelihood of acquiring legally permissible evidence is low. Although seizure of hostile actor assets or unilateral sanctions is possible, the costs the impose on a state directing such hostile operations is low compared to the strategic benefits it stands to gain.

Further, maintaining the status quo of countering cyber election campaigns with cyber tools has proven not to stop hostile actors from continuing such actions. Left on their own, CYBERCOM will continue their great efforts that include daily contact with hostile actors to mitigate the threat and prevent cyber election meddling. Such action provides some reassurance but the continued conflict in the cyber domain may just as likely create a spark that ignites a war. With no regulation, each state will continue to push the bounds of cyber conduct until someone crosses an unseen red line. The risk of crossing the red line justifies detailed boundaries. The United States should use a lawfare line of effort to counter election meddling, which will support imposition of greater costs on adversaries through a clear international cyber law regime. That regime can proscribe election meddling while also maintaining a structure for effective, timely operations against VEOs. Opposing great power competitors and regional destabilizing actors

seeking to undermine the American electoral system requires clear laws whose violation carry a tiered, escalatory, and responsive capability.

The *Tallinn Manual* offers an array of rules and a framework to help decision makers evaluate response options. Even if the international community affirmatively incorporated the manual's application as international law, significant ambiguity remains in evaluating cyber uses of force, sovereignty violations or breaches of the rule of nonintervention. That ambiguity will continue to allow hostile actors to use the law as a shield from attribution and legitimately argue that no legal violation exists for such operations. Tough rhetoric in policy papers or strategy documents sets the stage to combat election meddling. Yet, the United States must lead in this respect and use the international order it helped establish after World War II. Central to that order is a legal framework meant to manage international relations and prevent future wars. Legal silence on the issue of election meddling and the laws applicable to cyberspace will ensure that either significant threats to the American way of life continue or that increased low-level hostilities persist without an identifiable escalation ladder for deterrence.

A near-term pronouncement on appropriate, substantial responsive actions backed by the will to enforce it will give pause to hostile actors. In conjunction with mid-term and long-range actions to further develop international norms, CIL, and treaty obligations, the United States can mitigate the threat in the future by imposing the necessary costs. First, it will support U.N. and multilateral sanctions against hostile actors. More importantly, it can justify increased countermeasures over those currently employed by the United States (including cross-domain deterrence), establish stricter state accountability for state-affiliated cyber actors, and elevate meddling operations as appropriate to a use of force or armed attack designation. Though such elevation may initially appear to increase the likelihood of armed conflict, its presence as a

viable, painful deterrent against infringement on a state's political independence will reduce the frequency and severity of meddling.

A strict paradigm will not curb state sovereignty or impose election requirements on states. In actuality, such prohibition grants broader sovereignty rights to the states as it extends clear rights to state cyber domains and gives states the necessary power to respond to cyber sovereignty breaches. Furthermore, state free speech concerns are overblown. The United States clearly identified Russian actors during the U.S. 2016 and 2018 campaigns, and acted to prevent their meddling in the 2018 campaign without infringement on its own citizenry. Though a hypothetical situation could present challenges in discerning between citizens' free speech and foreign meddling, current hostile actors have not sought to exploit that vector.

Treaty development in this area could appear fruitless given the quickness of cyber domain evolution and number of significant actors employing election meddling operations. Such arguments are flawed. A treaty will take time to enact but it will still create a better starting point for future derivation than utilizing law that never conceptualized a cyber domain. Treaty development does not need to wait until ambiguity erupts into conflict; waiting will only cost lives and provide an uncertain chance at domain stability. Furthermore, Russia and China have already indicated a desire for a legal code of conduct. If the United States fails to act, then Russia and China will exploit the opportunity to provide global leadership and increase their spheres of influence. Russia and China will likely posture as though they are providing clarity to the environment but will set amorphous standards that allow them to continue their strategic influence campaigns at low cost. United States-led treaty efforts will ensure a viable long-term solution without ceding advantages to competitors. Coupled with advancing a clear position in the interim, the United States can mitigate current and future threats.

Endnotes

[1] Increasing Int Cooperation, 2018 CFR 2
[2] Increasing Int Cooperation, 2018 CFR 2
[3] Increasing Int Cooperation, 2018 CFR 2
[4] Dan Efrony, and Shany Yuval, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *The American Journal of International Law* 112, no. 4 (2018) 586.
[5] Alina Polyakova, *Want to Know what's next in Russian election interference? Pay attention to Ukraine's elections*, Brookings, Mar. 28, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/03/28/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/.
[6] Alina Polyakova, *Want to Know what's next in Russian election interference? Pay attention to Ukraine's elections*, Brookings, Mar. 28, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/03/28/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/.
[7] Mark Clayton, *Ukraine Election narrowly avoided 'wanton destruction' from hackers*, The Christian Science Monitor, June 17, 2014
[8] Mark Clayton, *Ukraine Election narrowly avoided 'wanton destruction' from hackers*, The Christian Science Monitor, June 17, 2014,
[9] Mark Clayton, *Ukraine Election narrowly avoided 'wanton destruction' from hackers*, The Christian Science Monitor, June 17, 2014,
[10] Tom McCarthy, *How Russia used social media to divide Americans*, The Guardian, Oct. 17, 2017, https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook.
[11] Efrony, *A Rule Book on the Shelf*, *609*-10.
[12] Efrony, *A Rule Book on the Shelf*, 610.
[13] Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, (Washington, DC, Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[14] Jonathan Landay and Mark Hosenball, *Russia, China, Iran sought to influence U.S. 2018 elections: U.S. spy chief*, Dec. 21, 2018, https://www.reuters.com/article/us-usa-election-interference/russia-china-iran-sought-to-influence-us-2018-elections-us-spy-chief-idUSKCN1OK2FS; Erica D. Borghard, *What a U.S. Operation Against Russian Trolls Predicts About Escalation in Cyberspace*, War on the Rocks, Mar. 22, 2019, https://warontherocks.com/2019/03/what-a-u-s-operation-against-russian-trolls-predicts-about-escalation-in-cyberspace/; Ellen Nakashima, *U.S. Cyber Command operation disrupted internet access of Russian factory on day of 2018 midterms*, The Washington Post, Feb. 27, 2019,
[15] Executive Order 13848, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election*, Sept. 12, 2018, https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.
[16] Joe Uchill, *Democrats allege new Russian hack attempts against the DNC*, Axios, Jan 18, 2019, https://www.axios.com/democrats-dnc-hacking-russia-0814744d-c885-411c-a73e-234699229879.html
[17] Cybersecurity and Infrastructure Security Agency, *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Mar. 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.
[18] Cybersecurity and Infrastructure Security Agency, *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Mar. 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.
[19] David E. Sanger, "Same Goal, Different Playbook: Why Russia Would Support Trump and Sanders," *New York Times*, Feb. 22, 2020, https://www.nytimes.com/2020/02/22/us/politics/russia-election-meddling-trump-sanders.html.
[20] Alyza Sebenius, *Microsoft Says Iran Tried Hack of U.S. Presidential Campaign*, Bloomberg: Cybersecurity, Oct. 4, 2019, https://www.bloomberg.com/news/articles/2019-10-04/microsoft-says-iran-tried-to-hack-a-u-s-presidential-campaign
[21] Alyza Sebenius, *Microsoft Says Iran Tried Hack of U.S. Presidential Campaign*, Bloomberg: Cybersecurity, Oct. 4, 2019, https://www.bloomberg.com/news/articles/2019-10-04/microsoft-says-iran-tried-to-hack-a-u-s-presidential-campaign.

[22] Julian E. Barnes and Thomas Gibbons-Neff, *U.S. Carried Out Cyberattacks on Iran*, New York Times, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
[23] Janosch Delcker, *Russian Hacking looms over Germany's election*, Politico, Dec. 19, 2016, updated Jan. 28, 2018, https://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/.
[24] Janosch Delcker, *Russian Hacking looms over Germany's election*, Politico, Dec. 19, 2016, updated Jan. 28, 2018, https://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/.
[25] Miracola, Sergio. "Chinese Hybrid Warfare." Instituto Per Gli Studi di Politica Internazionale (ISPI), December 21, 2018, https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853.
[26] Kelly Olsen, *The big winner in Taiwan's weekend elections? China*, CNBC, Nov. 25, 2018, https://www.cnbc.com/2018/11/26/taiwan-election-china-is-big-winner-as-tsai-ing-wens-dpp-party-loses.html.
[27] Kanupriya Kapoor, *Indonesia says cyber attack won't disrupt elections*, Reuters, Mar. 13, 2019, https://www.reuters.com/article/us-indonesia-election/indonesia-says-cyber-attacks-wont-disrupt-elections-idUSKBN1QU135.
[28] Edwin Y. Chua, "Political Warfare with Other Means: 2017 Cyber Attacks on Qatar." Joint Force Quarterly 91, (4th Quarter) 35.
[29] Diane Bartz, *UAE arranged for hacking of Qatar government sites, sparking diplomatic row: Washington Post*, Reuters, Jul. 16, 2017, https://www.reuters.com/article/us-usa-qatar-report/uae-arranged-for-hacking-of-qatar-government-sites-sparking-diplomatic-row-washington-post-idUSKBN1A200H.
[30] US Department of Defense. *Statement for the Record: Worldwide Threat Assessment Of The US Intelligence Community* (Washington DC: Director of National Intelligence, January, 2019) 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[31] US Department of Defense. *Worldwide Threat Assessment*, 5.
[32] US Department of Defense. *Worldwide Threat Assessment*, 5.
[33] US Department of Defense. *Worldwide Threat Assessment*, 7.
[34] US Department of Defense. *Worldwide Threat Assessment*, 7.
[35] MajGen Charles J. Dunlap, "Lawfare Today: A Perspective," *Yale Journal of International Affairs*, Winter (2008), 146, 147, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5892&context=faculty_scholarship.
[36] MajGen Charles J. Dunlap, *Lawfare*, 147.
[37] The one treaty existing that covers some aspects of cyberspace is the Buudapest Convention on Cybercrime of 2004 that focuses on copyright, computer fraud, and child pornography. See, "Convention on Cybercrime." November 23, 2001, ETS No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156d.
[38] United Nations Resolution, *Identification of Customary International Law*, A/CN.4/L.908, May 17, 2018, https://legal.un.org/docs/?symbol=A/CN.4/L.908.
[39] Michael N. Schmitt, ed. *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2d ed. (Cambridge University Press, 2017).
[40] CCDCOE, About Us, https://ccdcoe.org/about-us/.
[41] Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) 1.
[42] The White House, *International Strategy for Cyberspace*, (Washington, DC, 2011) 9, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[43] The White House, *International Strategy for Cyberspace*, 10.
[44] Schmitt, ed. *Tallinn Manual 1*, 4-5.
[45] Schmitt, ed. *Tallinn Manual 2.0*, 1-2.
[46] Schmitt, ed. *Tallinn Manual 2.0*, 2-4.
[47] United Nations Group of Governmental Experts, *Report on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security*, P 15, U.N. Doc. A/70/174 (July 22, 2015) https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
[48] United Nations Charter, Art. 2(4), https://www.un.org/en/sections/un-charter/chapter-i/index.html.
[49] UN Charter, Art. 51, https://www.un.org/en/sections/un-charter/chapter-vii/index.html.
[50] Schmitt, ed. *Tallinn Manual 2.0*, Rule 71, 399-344.
[51] Schmitt, ed. *Tallinn Manual 2.0*, Rule 71, 341-44.
[52] Schmitt, ed. *Tallinn Manual 2.0*, Rule 71, 341-44; Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (Summer 2018), 66.

[53] Schmitt, '*Virtual' Disenfranchisement*, 66.
[54] Efrony, *A Rule Book on the Shelf*, 614; William M. Arkin, Ken Dilanian and Cynthia McFadden, *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC News, Dec. 19, 2016, https://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116.
[55] Efrony, *A Rule Book on the Shelf*, 615; The White House, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*, Dec. 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.
[56] Efrony, *A Rule Book on the Shelf*, 619.
[57] DoD Law of War Manual 1.11.5.2.
[58] Schmitt, ed. *Tallinn Manual 2.0*, Rule 69, 330-37.
[59] Schmitt, ed. *Tallinn Manual 2.0*, Rule 69, 332-33.
[60] Schmitt, ed. *Tallinn Manual 2.0*, Rule 69, 332-33.
[61] Schmitt, ed. *Tallinn Manual 2.0*, Rule 69, 331.
[62] Samantha Besson, *Sovereignty*, Oxford Public International Law, April 2011, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472.
[63] Schmitt, ed. *Tallinn Manual 2.0*, Rule 1-4, 11-26.
[64] Schmitt, '*Virtual' Disenfranchisement*, 41-42; Group of Governmental Experts, *Report on Dev. in the Field of Info. and Telecomm.*
[65] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 20.
[66] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 20.
[67] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 20-21.
[68] Schmitt, '*Virtual' Disenfranchisement*, 45.
[69] Schmitt, '*Virtual' Disenfranchisement*, 45.
[70] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 21-22.
[71] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 22.
[72] Schmitt, '*Virtual' Disenfranchisement*, 46.
[73] Schmitt, '*Virtual' Disenfranchisement*, 46.
[74] Schmitt, '*Virtual' Disenfranchisement*, 47.
[75] Schmitt, ed. *Tallinn Manual 2.0*, Rule 4, 22.
[76] Schmitt, '*Virtual' Disenfranchisement*, 45.
[77] Gary Corn and Robert Taylor, "Symposium On Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty In The Age of Cyber," *American Journal of International Law Unbound*, 111 (2017) 207, 208.
[78] Corn, *Symposium On Sovereignty*, 207, 208, 210.
[79] Corn, *Symposium On Sovereignty*, 207, 210.
[80] Corn, *Symposium On Sovereignty*, 207, 209.
[81] Corn, *Symposium On Sovereignty*, 207, 209.
[82] US Department of Justice, "Grand Jury Indicts 12 Russian Intelligence officers for Hacking Offenses related to the 2016 Election," news release, July 13, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election; Joe Uchill, "Democrats allege new Russian hack attempts against the DNC," *Axios*, Jan 18, 2019, https://www.axios.com/democrats-dnc-hacking-russia-0814744d-c885-411c-a73e-234699229879.html.
[83] Corn, *Symposium On Sovereignty*, 207, 211.
[84] Gary Corn, "Tallinn Manual 2.0 – Advancing the Conversation," *Just Security*, February 15, 2017, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.
[85] Corn, *Tallinn Manual 2.0.*
[86] *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment, 1986 ICJ 14 (27 June), para 202-03, 205, https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.
[87] *Military and Paramilitary Activities in and Against Nicaragua*, Merits, Judgment, para 205.
[88] United Nations, *Non-interference in electoral processes*, General Assembly, A/RES/48/124, (Dec 20, 1993) https://www.un.org/unispal/document/auto-insert-183404/; Schmitt, *Virtual Disenfranchisement*, 49.
[89] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House, December 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf; Schmitt, '*Virtual' Disenfranchisement,* 49.

[90] *Military and Paramilitary Activities in and Against Nicaragua*, Merits, Judgment, para 205.
[91] Schmitt, ed. *Tallinn Manual 2.0*, Rule 66, 317.
[92] Schmitt, '*Virtual' Disenfranchisement,* 50.
[93] Schmitt, ed. *Tallinn Manual 2.0*, Rule 66, 319-21; Rule Book on the Shelf, 642; Schmitt, *Virtual Disenfranchisement*, 51-53
[94] Schmitt, '*Virtual' Disenfranchisement,* 51-53.
[95] David E. Sanger, "Same Goal, Different Playbook: Why Russia Would Support Trump and Sanders," *New York Times*, Feb. 22, 2020, https://www.nytimes.com/2020/02/22/us/politics/russia-election-meddling-trump-sanders.html.
[96] Efrony, *A Rule Book on the Shelf*, 635-36.
[97] Efrony, *A Rule Book on the Shelf*, 636-67.
[98] Efrony, *A Rule Book on the Shelf*, 586.
[99] Jeremy Wright, "Cyber and International Law in the 21st Century," (speech, May 23, 2018,) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[100] Wright, *Cyber and International Law.*
[101] United Nations General Assembly, *Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, (January 9, 2015*)* A/69/723, https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-150113-CodeOfConduct-1.pdf.
[102] ASEAN, *Chairman's Statement of the 2nd ASEAN Ministerial Conference on Cybersecurity*, Singapore, Sept. 18, 2017, https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/2nd-AMCC-Chairmans-Statement-cleared.pdf.
[103] ASEAN, *Chairman's Statement*.
[104] Paris Call, https://pariscall.international/en/.
[105] Paris Call, *Principles*, https://pariscall.international/en/principles.
[106] The White House, *National Cyber Strategy of the United States of America*, (Washington, DC, 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[107] NATO Cooperative Cyber Defence Centre of Excellence, Strategy and Governance, https://ccdcoe.org/library/strategy-and-governance/; *National Cyber Strategies*, European Union Agency for Cybersecurity, (last visited March 15, 2020) https://www.enisa.europa.eu/topics/national-cyber-security-strategies.
[108] United Nations, A/RES/73/179, Dec. 17, 2018, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179.
[109] United Nations General Assembly, *Letter*, 3-4.
[110] United Nations Office of Disarmament Affairs, *Fact Sheet: Developments in the Field of Information and Telecommunications In The Context of International Security*, United Nations, July 2019, https://www.un.org/disarmament/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.
[111] United Nations Office of Disarmament Affairs, *Fact Sheet.*
[112] United Nations Office of Disarmament Affairs, *Fact Sheet.*
[113] United Nations, *Group of Governmental Experts*, https://www.un.org/disarmament/group-of-governmental-experts/.
[114] Internet Governance Forum, *About the IGF*, United Nations, https://www.intgovforum.org/multilingual/tags/about.
[115] Internent Governance Forum, *Background Paper: The Internet Governance Forum (IGF)*, https://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf.
[116] Internent Governance Forum, *Background Paper.*
[117] Chair's Summary, "Fourteenth Meeting of the IGF, Berlin, 25-29 Nov 19," (Draft of 29Nov), 4, 6, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9299/1809.
[118] Chair's Summary, *Fourteenth Meeting*, 4, 6. https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9299/1809.
[119] United Nations Group of Governmental Experts, *Statement by the International Committee of the Red Cross*, Informal open-ended consultative meeting, Dec. 5, 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/icrc-statement-un-gge-december-2019.pdf.
[120] Global Commission on the Stability of Cyberspace, https://cyberstability.org/.

[121] Brad Smith, "The need for a Digital Geneva Convention," *Microsoft On the Issues*, February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00018k1n01i3tfomwyo20tis4co2l.
[122] Charles Doyle, *Extraterritorial Application of American Criminal Law*. CRS Report for Congress 94-166 (Washington, DC: Congressional Research Service, October 31, 2016), 31-32, https://fas.org/sgp/crs/misc/94-166.pdf.
[123] Doyle, *Extraterritorial Application*, 23-27.

Bibliography

Borghard, Erica D., "What a U.S. Operation Against Russian Trolls Predicts About Escalation in Cyberspace." *War on the Rocks*, March 22, 2019, https://warontherocks.com/2019/03/what-a-u-s-operation-against-russian-trolls-predicts-about-escalation-in-cyberspace/.

Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." *Council on Foreign Relations*, February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Chua, Edwin Y., "Political Warfare with Other Means: 2017 Cyber Attacks on Qatar." *Joint Force Quarterly* 91, (4th Quarter) 34-36.

Cybersecurity and Infrastructure Security Agency, "Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," news release, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

"Convention on Cybercrime." November 23, 2001, ETS No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156d.

Corn, Gary and Taylor, Robert. "Symposium On Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty In The Age of Cyber," *American Journal of International Law Unbound*, 111 (2017).

Corn, Gary. "Tallinn Manual 2.0 – Advancing the Conversation." *Just Security*, February 15, 2017, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

Doyle, Charles. *Extraterritorial Application of American Criminal Law*. CRS Report for Congress 94-166. Washington DC: Congressional Research Service, October 31, 2016. https://fas.org/sgp/crs/misc/94-166.pdf.

Dunlap, Charles J. "Lawfare Today: A Perspective." *Yale Journal of International Affairs*, Winter (2008), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5892&context=faculty_scholarship.

Efrony, Dan, and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *The American Journal of International Law* 112, no. 4 (2018).

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, 1986 ICJ 14 (27 June) https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

Miracola, Sergio, "Chinese Hybrid Warfare." *Instituto Per Gli Studi di Politica Internazionale*, December 21, 2018, https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853.

Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Washington, DC, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Polyakova, Alina, "Want to Know what's next in Russian election interference? Pay attention to Ukraine's elections." *Brookings*, March 28, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/03/28/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* Cambridge University Press, 2013.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2d ed., Cambridge University Press, 2017.

Schmitt, Michael N., "'Virtual' Disenfranchisement: Cyber Election meddling in the Grey Zones of International Law," Chicago Journal of International Law 19, no. 1 (Summer 2018).

Sebenius, Alyza, "Microsoft Says Iran Tried Hack of U.S. Presidential Campaign." *Bloomberg: Cybersecurity*, October 4, 2019, https://www.bloomberg.com/news/articles/2019-10-04/microsoft-says-iran-tried-to-hack-a-u-s-presidential-campaign.

Smith, Brad, "The need for a Digital Geneva Convention," *Microsoft On the Issues*, February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00018k1n01i3tfomwyo20tis4co2l.

The White House. *International Strategy for Cyberspace*, Washington, DC, 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House. *National Cyber Strategy of the United States of America*, Washington, DC, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

United Nations Charter, June 1945, https://www.un.org/en/charter-united-nations/index.html

United Nations General Assembly, *Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, (January 9, 2015) A/69/723, https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-150113-CodeOfConduct-1.pdf.

United Nations Group of Governmental Experts, *Report on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security*, U.N. Doc. A/70/174 (July 22, 2015) https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

United Nations Office of Disarmament Affairs, "Fact Sheet: Developments in the Field of Information and Telecommunications In The Context of International Security." *United Nations*, July 2019, https://www.un.org/disarmament/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

United Nations Resolution, *Identification of Customary International Law*, A/CN.4/L.908, May 17, 2018, https://legal.un.org/docs/?symbol=A/CN.4/L.908.

US Department of Defense. *Statement for the Record: Worldwide Threat Assessment Of The US Intelligence Community*, Washington DC: Director of National Intelligence, January, 2019.

US Department of Justice. *Grand Jury Indicts 12 Russian Intelligence officers for Hacking Offenses related to the 2016 Election*, news release, July 13, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

Jeremy Wright, "Cyber and International Law in the 21st Century," Speech. May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

US President, Executive Order 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election." *Federal Register*, September 12, 2018, https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.