THE LAW OF CYBER INTERFERENCE IN ELECTIONS

ABSTRACT.

Cyberattacks are increasing in frequency, publicity, and impact, making significant cyber episodes are the hallmark of modern foreign policy. One sub-set of these cyber attacks has been state-supported interference in elections: ranging from email hacking and doxing in the 2016 U.S. presidential election, to cyber attacks on the Bundestag surrounding the 2015 German Parliamentary elections, to dissemination of "fake news" surrounding 2016 Italian referendum votes. But international law gives States limited means by which to respond to election interference. Faced with limited options for so-called "hacking back," state officials and international legal experts alike have championed creative interpretations of international law to allow retribution on state hackers: invoking countermeasures, or the notion that a rogue state can be brought, forcefully, into line with international legal obligations. This Note explores the international legal framework that apples to cyber interference in elections. It makes the normative argument that stretching countermeasures to encompass cyber episodes is not only wrong, but also dangerous. Unless modern understanding of sovereignty and the norm of non-intervention are updated for a networked age, countermeasures represent an impermissible expansion of the use of force.

WORD COUNT: 16,921

Table of Contents

I.

INTRODUCTION

The 2016 U.S. Presidential election was close. Despite Hillary Clinton's win in the popular vote—she would earn 65,844,610 votes to Trump's 62,979,636 votes[1]—Donald Trump took the Electoral College. [2] In the early morning hours of November 9, major news networks started to call the race.[3] It was over; Donald Trump would be the forty-fifth president of the United States of America.

The touchstone of the campaign was cyber: beginning, specifically, with Clinton's email practices while serving as U.S. Secretary of State.[4] Clinton's use of a private email server had been called foolish, likely to jeopardize U.S. national security, even criminal. [5] During the campaign, Trump personally invited the Russians to hack into the Clinton email servers: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," he said, adding "[b]y the way, they hacked—they probably have her 33,000 e-mails. I hope they do. They probably have her 33,000 e-mails that she lost and deleted because you'd see some beauties there. So let's see."[6]

On December 9, 2016, U.S. intelligence officials confirmed that Russia had indeed taken Donald Trump up on his offer; Russia had "hacked" the U.S. election.[7] This was reaffirmed by the June 8, 2017 testimony of James Comey, who confirmed the Russian hacking in no uncertain terms. "There should be no fuzz on this whatsoever," Comey stated. "The Russian interfered in our election during the 2016 cycle. They did it with purpose. They did it with sophistication. They did it with overwhelming technical

---

[1] *Presidential Election Results: Donald J. Trump Wins*, N.Y. TIMES (Dec. 20, 2016), http://www.nytimes.com/elections/results/president. The numbers quoted represent the most recent figures reported, and were last edited on December 21, 2016.

[2] *Presidential Election Results: Donald J. Trump Wins*, N.Y. TIMES (Dec. 20, 2016), http://www.nytimes.com/elections/results/president.

[3] Matt Flegenheimer and Michael Barbaro, *Donald Trump is Elected President in Stunning Repudiation of the Establishment,* N.Y. TIMES (Nov. 9, 2016), http://www.nytimes.com/2016/11/09/us/politics/hillary-clinton-donald-trump-president.html.

[4] *Hillary Clinton: Private Email Set Up For 'Convenience,'* BBC NEWS (Mar. 10, 2015), http://www.bbc.com/news/world-us-canada-31819843.

[5] Patrick Howley, *Hillary Clinton Email Scandal* Explained, BREITBART (Oct. 31, 2016), http://www.breitbart.com/2016-presidential-race/2016/10/31/hillary-clinton-email-scandal-explained/.

[6] Andy Sherman, *Hillary Clinton Claims Donald Trump Invited Russian President Vladimir Putin to Hack Americans*, Politifact (Sept. 26, 2016), http://www.politifact.com/truth-o-meter/statements/2016/sep/26/hillary-clinton/hillary-clinton-claims-donald-trump-invited-russia/.

[7] David E. Sanger and Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?_r=0 ("American intelligence agencies have concluded with "high confidence" that Russia acted covertly in the latter stages of the presidential campaign to harm Hillary Clinton's chances and promote Donald J. Trump, according to senior administration officials.").

efforts. And it was an active-measures campaign driven from the top of that government."[8] In short, said Comey, it was "very, very serious"—and an "attack."[9]

But was it an attack? Comey saw no evidence of tampering with ballot boxes.[10] There was no physical destruction of voter equipment. There were no fake votes. Rather, there was an information campaign—something not normally thought of as an act of war. Yet, consensus built that the Russian interference *did* constitute something that the United States could justifiably call an attack. For example, Senator Warner: "[A] foreign adversary attacked us right here at home, plain and simple, not by guns or missiles, but by foreign operatives seeking to hijack our most important democratic process—our presidential election."[11] And James Comey agreed. "This is such a big deal," he said, because "we have this big, messy, wonderful country where…nobody tells us what to think, what to fight about, what to vote for, except other Americans …. But we're talking about a foreign government that, using technical intrustion, lots of other methods, tried to shape the way we think, we vote, we act."[12] In other words, Russia violated U.S. sovereignty. And, some scholars and policymakers are beginning to argue, such a violation is a sufficient trigger for war.

International Law and Cyber Interference

At issue in the Comey testimony, and the scholarly debates more generally, is something of an international legal tripwire: whether Russian cyber-interference[13] constitutes an "attack" as understood in international law. This question is important because if the answer is yes, then the United States is legally permitted to use force on Russia in response. If the answer is no, the United States cannot legally use force in response—or at least not based on the U.N. Charter.

The standard for the use of force in international law is deliberately high. The laws of war were constructed in a time where bullets, cannons, and kinetic warfare were not only the norm—they were all that was known. The laws therefore contemplate kinetic effects as a trigger for the retaliatory use of force. So if a State blows up a power plant? It's snagged the tripwire, and, depending on the severity of the attack, the victim State is

---

[8] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[9] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[10] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[11] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[12] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[13] It is important, at the outset, to define the use of terms in this paper. I use the term "cyber interference" as a broader, catch-all: for any state-sponsored interference in elections, without doing the careful work of classifying that interference under the relevant bodies of law that apply. I will use the term "cyber interference" throughout the paper as a framing mechanism. By contrast, I use the term "cyber attack" only to refer to those cyber interferences that meet the standard for use of force in Article 2(4) of the U.N. Charter

justified to resort to self-defense measures (*jus ad bellum*) or else a reciprocal attack under the law of armed conflict (*jus in bello*). But what happens if a State makes an impact that is invisible, unseen, or just not kinetic in nature? More and more modern examples are falling "below the threshold": the Sony attack,[14] the DNC hack. The issue: narrowly construed, carefully-read international law does not give states the ability to defend themselves in response.

States cannot tolerate being hamstrung by international law. In the face of limited options for responding to cyber election interference, international legal practitioners[15] and scholars have argued that international law contemplates other acceptable ways of using force on another state. Desperate for lawful avenues to "hack back," these experts argue for another rationale for using reciprocal force in the context of cyberattacks—the use of countermeasures[16] through violations of two norms: violations of sovereignty, and the norm of non-intervention.

A *countermeasure* is an act by a victim State against another State that would ordinarily be unlawful, but is justified as medicine for the offending State's unlawful activity. It's tit-for-tat: the deeper logic being that one illegal act can justify another, only if the responsive illegal act is narrowly tailored to bring the offending State back into line with its international legal obligations. To engage in countermeasures, a State must identify what internationally wrongful act justifies the illegal response. The Russian hacks could be characterized one of two ways: as a violation of the sovereignty of the United States, or as a violation of the norm of non-intervention.

But perhaps too much attention is being paid to the doctrine of countermeasures, and too much effort is paid to attempt to fit hacking into a "use of force" argumentation. Instead, States might have a broader range of tools at their disposal if they more critically broke cyber interference in elections down into their component parts. That is because the law that applies to espionage is different from that which applies to destruction of votes, and each of these are different from that which applies to misinformation campaigns. And for every distinct body of law, States have, at their disposal, a separate means of seeking a remedy. This Note argues that States have not spent enough time thinking creatively about precisely what remedies are available to them, beyond those involving the use of force.

Part I explores why cyber interference in elections matter. It then outlines the episodes of cyber interference that affected the United States, Germany, and Italy. By explaining the content of these attacks, comparing their similarities and their differences, and outlining the states' preliminary attempts to seek retribution for the hacks, this Part sets the stage for a careful parsing of the different forms of election interference.

---

[14] Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

[15] The Tallinn 2.0 manual embraces this position. *See* Ashley Deeks, *Tallinn 2.0 and a Chinese View on the Tallinn Process*, LAWFARE (May 31, 2015), https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

[16] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10 (2001) [hereinafter Draft Articles]. The Draft Articles "are considered by courts and commentators to be in whole or in large part an accurate codification of the customary international law of state responsibility." JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 43 (2013).

Part II outlines four categories of cyber interference in elections. Taking the examples from Part I, it explains the many forms cyber election interference can take. These forms range from doxing to meddling with vote counts, to efforts that undermined confidence in the election outcomes. This framework structures the subsequent analysis of how, precisely, international law applies to cyber interference in elections.

Part III sets forth the international legal basis by which states are permitted to use force. First, it examines the laws of war: outlining the apparatus in the laws of war by which states are authorized to use force on other states. It aims to give the general structure of the international legal threshold for war contained in U.N. Charter Article 51 and Article 2(4). It then traces the historical development of the countermeasures doctrine, and the content, relationship, and standards for violations of sovereignty and the norm of non-intervention.

Part IV applies applicable international law to cyber interference in elections. It analyzes the four kinds of cyber interference proposed in Part II under the relevant bodies of international law outlined in Part III. In doing so, it identifies the clear-cut violations of international law, and then the murky legal areas. In particular, Part IV discusses the thorny issue of what to do with the *dissemination of information* in international law, and whether the most actively proposed solution by international legal scholars to this kind of "below-the-threshold" (of U.N. Charter Article 2(4)) cyber interference—that is, the use of countermeasures—is appropriate.

And it is this argument that Part V squarely engages with. Many scholars and practitioners advocate for the use of countermeasures doctrine as a means of addressing less clear-cut violations of international law, like dissemination of information in elections. And such advocacy has become particular vociferous since the February 8, 2017 publication of the *Tallinn 2.0 Manual on the International Law Applicable to Cyber* operations. But such an argument is misguided: even downright dangerous. Part V takes a harder look at what risks are inherent in an expanded use of countermeasures, identifying three reasons that countermeasures are *not* the answer.

The Note then lays out several solutions to the problem. Countermeasures are *not* the answer for these tougher cases of election interference: but that doesn't mean that international law is without solutions to thorny issues of cyber interference with elections. This Part picks up the various sources of law outlined in Part III to identify avenues for redress, protection, and retribution that may have been missed in the frenzied focus on countermeasures doctrine as a means of addressing cyber interference. As such, it offers states alternative means to protect their sovereignty, without expanding internationally lawful grounds upon which to resort to violence.

The stakes of this argument could not be higher. At issue is the development of international law, which is spinning into dangerous territory: territory which permits the use of force in far-flung contexts. It risks rendering existing portions of international law meaningless. It risks escalation of violence in a never-ending tit-for-tat loop. And it risks limiting states' freedoms to peacefully intervene in other states for purposes that have been long-recognized: humanitarian intervention, bolstering of civil society, and protection of human rights.

The United States has long been a leader in the development of international law. Now, more than ever, it is critical to thoughtfully examine how the arguments made could be applied in contexts, and situations, beyond the one we face.

I. PROLIFERATION OF CYBER-INTERFERENCE IN ELECTIONS

Cyber election interference is a global threat. In the past two years, several Western states experienced election interference constituting a serious impediment to their ability to hold free and fair elections. This Part outlines the types of cyber interference that have affected states. In doing so, it intends to give a sense of the scope and the types of election interference, in order to foreshadow the categorization of cyber interference in Part II, and the application of international law to these categories in Part III. In addition, through demonstrating the pervasive nature of the problem, it intends to foreshadow the stakeholders in potential policy solutions outlined in Part V.

A. Why Does Cyber Election Interference Matter?

Cyber interference is not a new phenomenon. But what makes cyber election interference distinct from general cyber attacks is the (i) nature of the target, (ii) the nature of the attack, (iii) the nature of the damage, and (iv) the lack of an appropriate remedy, either in international law or in domestic law.

Nature of the Target

Other cyber attacks have functioned much like a kinetic attack; a state has used lines of code to damage, destroy, or cause to malfunction a piece of equipment in another state for the attacking state's benefit. Some of these benefits have been out of military necessity; for example, the alleged United States hack of the Iranian centrifuge system in order to secure more time to negotiate a nuclear agreement favorable to U.S. interests. Other cyber attacks have targeted private corporations as petty punishment; for example, North Korea's efforts to hack and destroy the Sony computer system in order to gain personal retribution for the release of a film offensive to North Korean leaders.

Cyber election interference is distinct in at least two ways. First, the targets are publically owned, not privately owned. As such, any attack on an arm of the state raises questions about violations of sovereignty, both in the abstract, nature-of-a-state sense, and in the concrete, violations of borders and invasion of territory sense.

Second, and distinctly, some of the targets are not computers. They are citizens. Unlike in the Sony hack or Stuxnet, the intrusive piece of data is propaganda—designed not to affect computer systems, but rather individuals. Information, whether true of false, is released to make a sovereign's citizens function differently, and thus damage the state. It is the intimate target of cyber interference in elections, touching the state's apparatus and its citizens, that makes it distinct from other forms of cyber attacks.

Nature of the Attack

Cyber election interference shares some traits to other commonly known cyber attacks. However, it is distinct in one substantial way; cyber interference in elections constitutes not only hacking, but also information campaigns. The majority of cyber attacks that states have faced in the past have largely involved kinetic damage to a

particular, physical asset. To instead have civilian hearts and minds targeted and affected by another state's cyber operations is novel.

But cyber election interference shares similar characteristics to other cyber attacks, though the stakes of the problems are higher in the election context. Cyber attacks are generally not visible, which generally raises concerns both about (i) identifying the attack close to the moment in time that it occurs, and (ii) correctly attributing the attack to the attacker, in order to exact punishments and demand recompense.

Being blind to the moment of the attack and the identity of the hacker raise particular concerns in the election context. First, because elections are held at a particular moment in time, identifying security breaches and improper influences as close to the moment of their introduction is critical to ensure election integrity. A later identification of the problem has the potential to provoke a crisis of constitutional proportions—for example, a belated announcement that votes were improperly tabulated, and the victory should have been given to another candidate would raise questions even larger than those of *Bush v. Gore*. "What better way to destabilize a country without a shot being fired?," one security professional asked in response to Russian interference in the U.S. elections.[17]

Second, the thorny issue of identification of hackers becomes even more concerning in the international context. To the extent that international law does speak to cyber election interference, states cannot either exact retribution or ask for reparations without a clear idea of both (i) who the actor is, and (ii) whether or not the actor was under state control. Neither of those factors are clearly visible in the cyber election interference context, but the stakes are higher as the consequences for election interference may be higher than those of a hack in the private sector.

Nature of the Damage

Unlike in an attack such as Stuxnet, the scope of the damage from cyber election interference has the potential to be unquantifiable. Contrast this to the situation in Stuxnet, where the damage was confined (at least originally) to the Iranian nuclear program centrifuges. The scope of cyber election interference, however, has the potential to be far broader. A hack of state voting systems might be bounded to the physical computer systems, but the dissemination of fake news to influence citizen votes, however, is difficult to map or quantify.

Moreover, cyber interference in election, once known, has the potential to undermine citizen confidence in the democratic process and in the integrity of their government. Cyber election interference keeps citizens from being able to meaningfully participate in their chosen form of government. And if citizens are not able to meaningfully participate in a democratic government, the democracy itself is threatened.

Lack of an Appropriate Remedy

[17] Lily Hay Newman, *The Real Hacker Threat to Election Day? Data Deception and Denial*, Wired (Nov. 7, 2016), https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

Both hacks on public apparatus and attacks on citizens raise substantial questions and justifiable concerns about improper intrusion into objects of, and subjects of, state power. When these kinds of questions are raised in the physical world, states do not hesitate to go to war to protect such critical targets. It is by the same logic that similar arguments are raised in the context of cyber election interference.

Yet international law does not permit sovereigns to lawfully use force in response to such intrusions. The lack of a remedy has the potential to motivate states to (i) use force unlawfully, or else (ii) stretch existing international law to places where it does not naturally, or justifiably, extend.

Key Distinctions Summarized

The single greatest difference between cyber election interference and other cyber attacks is the propensity of states to target civilians alongside systems. In doing so, the attack becomes difficult to identify, quantify, control, and remedy. Sections I.B through D will chart the propensity of Russia to use citizens to influence elections. Part II will then categorize the various types of election interference, and Part III will identify those particular instances of election interference that are least adequately addressed by international law.

B. Mapping Cyber Election Interference

1. Cyber Election Interference in the United States

The highest-profile example of cyber-interference in elections is Russia's interference in the 2016 U.S. election. As of the time of this writing, reports analyzing the hack have indicated that Russia interfered in four major ways: through theft of information, selective dissemination of information, a propaganda campaign, and efforts to hack into voting systems across the country.

Analysis exploring why Russia might "hack" the U.S. election has focused on Putin's past frustration with U.S. efforts to promote civil society, which Putin saw as unreasonable intrusion on Russian sovereignty. In the *New York Times*, David Sanger notes that Putin publicly accused Clinton of instigating protests in Moscow in 2011, and blamed Clinton for encouraging anti-Russian revolts during the 2003 Rose Revolution in Georgia and the 2004 Orange Revolution in Ukraine—each of which Putin saw as unwarranted intrusion into Russia's geographic sphere of influence, rather than as democracy promotion. [18] In this manner, Russian interference in the U.S. election can be seen as a tit-for-tat response.

---

[18] *See* Eric Lipton, David E. Sanger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html; *see also Putin's Revenge*, POLITICO MAGAZINE (Dec. 2016), http://www.politico.com/magazine/story/2016/12/russia-putin-hack-dnc-clinton-election-2016-cold-war-214532. For more information about international law's protections for and limitations on intervention in other states, see [SOURCE REDACTED FOR SUBMISSION].

Cyber-Intrusions and Theft of Information

Russia used various cyberespionage teams to hack into computers and email systems in the 2016 U.S. election. Additionally, we know that Russian cyberespionage teams took some of the information it found in these computers and systems, because some of the information and emails it discovered through unauthorized access were later published.

A Russian cyberespionage team, colloquially known as "Cozy Bear" or "A.P.T. 29," [19] hacked computers at the Democratic National Committee and penetrated the email account of Clinton's presidential campaign chair, John Podesta.[20] Russia also hacked the Republican National Committee emails using a Russian unit called "Fancy Bear," or "A.P.T. 28."[21] In addition, Russia conducted a massive operation to target hundreds to thousands of non-governmental organizations and nonprofits.[22]

Selective Dissemination of Information

Second, Russia selectively disseminated some of the hacked emails. Russian intelligence officials took the emails and private documents procured through the hack, and posted them to WikiLeaks and other websites in July 2016.[23] R.N.C. emails, on the other hand, were not disseminated.

Russian dissemination of information arguably had significant impact on congressional races, and citizen trust in the democratic process more generally. The fallout from the dissemination of D.N.C. emails was immediate.[24] Debbie Wasserman Schultz, the chair of the D.N.C., was forced to resign, along with her top aides. [25] On the state level, confidential documents taken from the Democratic Congressional Campaign

---

[19] David E. Sanger and Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?_r=0.

[20] Craig Forcese, *"Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?* JUST SECURITY (Dec. 16, 2016), https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/.

[21] David E. Sanger and Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?_r=0. The intelligence community's finding is currently, actively, disputed by the R.N.C.; officials argue that Russia never hacked their emails. *Id.*

[22] *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

[23] Eric Lipton, David E. Sanger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[24] In one tweet, Trump quipped: ""The new joke in town is that Russia leaked the disastrous D.N.C. e-mails, which should never have been written (stupid), because Putin likes me." Donald Trump (@realDonaldTrump), TWITTER (July 25, 2016, 4:31 AM), https://twitter.com/realDonaldTrump/status/757538729170964481.

[25] Eric Lipton, David E. Sanger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Committee relating to congressional races in a dozen states were published,[26] tainting many affected races with accusations of scandal.[27]

"Fake News"

Third, Russia engaged in "information warfare" campaigns.[28] Sites like RT News and Sputnik, both state-funded Russian sites, shared fake news. Their stories, which attacked Clinton and U.S.-Russian relations, were widely circulated on social media. They were likewise shared by conservative talk-show hosts and activists, "often not knowing the accuracy of the reports."[29] In addition, the Kremil was identified by U.S. intelligence agencies as breaching the websites of the boards of elections for Arizona and Illinois.[30]

Breach of Voter Registration Systems

Fourth, Russia allegedly targeted the voter registration systems in over 20 state election systems. Four of the twenty systems were, in fact, breached.[31]

Recent reports indicated that Russian interference in the election went far beyond misinformation campaigns, and instead constituted attempts to breach the core systems of American voting apparatus.[32] A classified National Security Agency report, published online by *The Intercept*, states that Russian hackers who were part of the GRU military agency attempted sent spear-phishing emails to over 100 local election officials at VR systems, a Florida-based technology firm that sells equipment and software for voter registration.[33]

---

[26] Eric Lipton, David E. Sanger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[27] Eric Lipton, David E. Sanger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[28] David Sanger, *U.S. Officials Defend Integrity of Vote, Despite Hacking Fears*, N.Y. TIMES (Nov. 25, 2016), http://www.nytimes.com/2016/11/25/us/politics/hacking-russia-election-fears-barack-obama-donald-trump.html.

[29] David Sanger, *U.S. Officials Defend Integrity of Vote, Despite Hacking Fears*, N.Y. TIMES (Nov. 25, 2016), http://www.nytimes.com/2016/11/25/us/politics/hacking-russia-election-fears-barack-obama-donald-trump.html.

[30] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[31] Danielle Kurtzleben, *Contrary to Trump's Tweet, Russian Hacking Came Up Before Election (A Lot)*, NATIONAL PUBLIC RADIO (Dec. 12, 2016), http://www.npr.org/2016/12/12/505261053/13-times-russian-hacking-came-up-in-the-presidential-campaign.

[32] Deb Riechmann and Russ Byoum, *Report: Russian Hackers Attacked Election Software Supplier*, Time (June 5, 2017), http://time.com/4806709/russia-hack-election-donald-trump-nsa-reality-winner/.

[33] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

2. Cyber Election Interference in Italy

Spread of false information via social media affected the 2016 Italian elections.[34] Buzzfeed and the Italian newspaper La Stampa reported that blogs, social media accounts and websites in Russia spread fake news across their virtual networks. The news was targeted against Prime Minister Renzi.[35] And it was viral; half of the most popular news stories related to the referendum and shared on social media were fake.[36] Renzi did lose the election, triggering concerns that the instability might trigger a deeper crisis in the vulnerable Italian banking sector.[37]

3. Cyber Election Interference in Germany

Long before the U.S. Central Intelligence Agency concluded that Russia had interfered in the U.S. presidential election with the aim of assisting Donald Trump, German intelligence officials began reporting "active measures" from Russia to influence German public opinion.[38] With an election coming in September 2017, government officials have reported that Russia is attempting to unseat German Chancellor Angela Merkel, who has visibly critiqued Russian policies in Syria and Ukraine.[39] Merkel has herself acknowledge Russian interference as "possible" in at least two respects: both in information warfare, and in cyberattacks.

The information warfare had already had extreme diplomatic consequences. One fake news story in particular captivated public consciousness: a fake news item about refugees from the Middle East gang-raping a 13 year-old Russian girl in Berlin went viral. Protests in response to the story grew so violent that even Frank-Walter Steinmeier, Germany's foreign minister, was forced to make a statement debunking the propaganda.[40] But the corrections had little impact; the fake news had been "laundered and [entered] the public consciousness as fact."[41]

---

[34] Jason Horowitz, *Spread of Fake News Provokes Anxiety in Italy*, N.Y.Times (Dec. 2, 2016), https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html.

[35] Alberto Nardelli and Craig Silverman, *Italy's Most Popular Political Party is Leading Europe in Fake News and Kremlin Propaganda*, Buzzfeed (Nov. 29, 2016), https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fak?utm_term=.cnnVK073G#.xeaRkyLGQ.

[36] Ivana Kottasova, *Did Fake News Influence Italy's Referendum?*, CNN (Dec. 5, 2016), http://money.cnn.com/2016/12/05/media/fake-news-italy-referendum/.

[37] *Matteo Renzi's Referndum Defeat Risks Italy Political Crisis*, BBC (Dec. 5. 2016), http://www.bbc.com/news/world-europe-38204189.

[38] Janosch Delcker, *Russian Hacking Looms Over Germany's Election*, Politico (Dec. 30, 2016), http://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/.

[39] Janosch Delcker, *Russian Hacking Looms Over Germany's Election*, Politico (Dec. 30, 2016), http://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/.

[40] Damien McGuinness, *Russia Steps into Berlin 'Rape" Storm Claiming German Cover-up,* BBC News (Jan. 27, 2016), http://www.bbc.com/news/blogs-eu-35413134.

[41] Lucian Kim, *Russia Having Success in Hybriad War Against Germany*, Reuters (Feb. 7, 2016), http://blogs.reuters.com/great-debate/2016/02/07/russia-having-success-in-hybrid-war-against-germany/.

But the Russian campaign, allegedly, was not cabined to information warfare alone. The German intelligence agencies claimed that Russia had hacked into the Bundestag, the lower house of the German parliament. And Angela Merkel alluded to a link between hacks on the major German telecommunications group Deutsche Telecom, affecting 900,000 customers, with Russian interference.

4. Cyber Election Interference in France

Hackers in France stole and published gigabytes of leaks from center-left French candidate Emmanuel Macron on the eve of the French election.[42] The hackers were tied to the APT28 or "Fancy Bear" group, which also targeted German Chancellor Angela Merkel.[43]

5. Cyber Election Interference in Russia

Factions of Russian hackers have engaged in cyber interference at home, too.[44] Homegrown attacks have largely been through denial of service (DDOS), where malware-infected computers flood target servers with "junk traffic," overwhelming the sites and causing them to either become slow and unresponsive, or else entirely unavailable.[45] In the late 2000s, pro-Russian hackers used DDOS to target the site of opposition leader Garry Kasparov in the 2007 campaign for president. In 2011, Russian hackers did the same to opposition media outlets like the election monitoring NGO, Golos.[46]

6. Cyber Election Interference in Ukraine

Russian hackers have even attempted to publish false election results. In 2014, a pro-Russian hacker group called CyberBerkut compromised the website of the Ukrainian Central Election Commission. They modified the website to declare the winner to be

---

[42] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[43] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[44] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[45] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[46] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

ultra-right candidate Dmytro Yarosh. The Commission results saw the modification less than an hour before the results were scheduled to be released.[47]

C. *"We Need To Take Action. And We Will."*[48]

In the midst of the revelation of Russia's election-hacking, President Obama promised a "proportional" response: " I think there is no doubt that when any foreign government tries to impact the integrity of our elections, we need to take action. And we will — at a time and place of our own choosing."[49]

The question of what constitutes a proportional response, however, is complicated. This is because international law does not have a single mechanism addressing and punish hackers who engage in election interference. Cyber election interference is complicated, and can range from changing votes in a ballot box to spreading propaganda for or against a candidate. And while international law has solutions to *some* forms of cyber-interference, it does not have solutions for *all* forms. Particularly when it comes to the spread of information, international law leaves states largely without recourse.

Some scholars disagree, arguing that states can legally make a "proportional response" not only for kinetic attacks on voting systems, but also for information warfare. They argue that the United States is justified in using force against the Russians—either in the cyber-realm, or in the physical world—in response to the spread of "fake news."[50] Others say that the United States hands are tied. They argue that Russian hacking, while unfortunate, is only an example of espionage (and not war),[51] leaving the United States only permitted to retaliate using criminal law, or other covert actions. They have taken the opportunity to renew calls for a cyber treaty, arguing that existing law limits U.S.

---

[47] Andy Greenburg, *Everything We Know About Russian Election-Hacking*, Wired (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[48] Scott Detrow, *Obama on Russian Hacking: 'We Need to Take Action. And We Will."* NATIONAL PUBLIC RADIO (Dec. 15, 2016), http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will.

[49] Scott Detrow, *Obama on Russian Hacking: 'We Need to Take Action. And We Will."* NATIONAL PUBLIC RADIO (Dec. 15, 2016), http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will.

[50] Yochi Dreazen, *I've Spent 15 Years Covering National Security. I've Never Seen Anything Like the Russian Hack*, VOX (Dec. 20, 2016), http://www.vox.com/world/2016/12/20/14001118/putin-russia-hack-dnc-clinton-trump-election-podesta-emails ("Part of me thinks we should consider this to be an act of war, no different than if Putin had launched a cyberattack that took down the electrical grid or the banking system.".)

[51] Yochi Dreazen, *I've Spent 15 Years Covering National Security. I've Never Seen Anything Like the Russian Hack*, VOX (Dec. 20, 2016), http://www.vox.com/world/2016/12/20/14001118/putin-russia-hack-dnc-clinton-trump-election-podesta-emails ("Part of me thinks we should consider this to be a case of espionage (stealing the documents in the first place) paired with an unusually sophisticated propaganda effort (leaking the sexiest material slowly to dominate the news cycle in the final weeks before the election).").

options for legal responses. [52] A third camp thinks that the hacks are "something new entirely — a hybrid that is more than mere spying but less than an outright assault."[53] Many of in the third camp argue that the United States can use cyber tools to "punish" Russian hackers or damage their hardware, putting most of the pressure on the United States to use domestic tools to achieve their recourse.[54]

Russia, meanwhile, makes a vociferous argument that its actions are neither unlawful, nor unique. Russia argues that by several metrics, its interference in elections is justified. First, it argues that its actions are proportional. It argues that the same tactics are used in Western media in the United States and Europe to produce lies about Russia, as it now uses in disseminating news.[55] Second, it cites to U.S. interference in elections in Chile, Nicaragua, and Iran, among other states.[56] Even if it is interfering in elections, Russia argues, then this is no worse than the United States' past interferences. Third,

---

[52] Ido Kilovarty and Itamar Mann, *Toward a Cyber-Security Treaty*, JUST SECURITY (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty/ ("But international law offers little by way of remedies against state-sponsored exposure of foreign secret information. The analysis typically focuses on the international legal duty of non-intervention – a fundamental but indeterminate concept of international law. ... Rather than rehashing the discussion of the laws of war, policymakers and lawyers in Washington should take this opportunity to reevaluate another option: a cyber-specific treaty.").

[53] Yochi Dreazen, *I've Spent 15 Years Covering National Security. I've Never Seen Anything Like the Russian Hack*, VOX (Dec. 20, 2016), http://www.vox.com/world/2016/12/20/14001118/putin-russia-hack-dnc-clinton-trump-election-podesta-emails

[54] *See* James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POLICY (Oct. 12, 2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/ ("[T]he United States could use its own offensive cyber-tools to punish Russian hackers by knocking them off-line or even damaging their hardware. This response would be open to objections that it represents an unwarranted escalation. But under prevailing international law, if a nation has information of a nexus of offensive activity, has requested it to stop, and the offending nation declines to do so, that offensive center is liable for attack. The burden of proof for attribution would be higher in crafting such a response; it would be viable only if Washington had definitive information on the command and control centers that launched the hacking activity."); *see also* Eric Lipton, David E. Danger and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0 ("But by late August, Admiral Rogers, [Director of the National Security Agency and commander of the United States Cyber Command], was pressing for a more muscular response to the Russians. In his role as director of the Pentagon's Cyber Command, he proposed a series of potential counter-cyberstrikes. While officials will not discuss them in detail, the possible counterstrikes reportedly included operations that would turn the tables on Mr. Putin, exposing his financial links to Russia's oligarchs, and punching holes in the Russian internet to allow dissidents to get their message out. Pentagon officials judged the measures too unsubtle and ordered up their own set of options."); *see id.* ("An American counterstrike, said Michael Morell, the former deputy director of the C.I.A. under Mr. Obama, has "got to be overt. It needs to be seen."A covert response would significantly limit the deterrence effect, he added. "If you can't see it, it's not going to deter the Chinese and North Koreans and Iranians and others."). For a thoughtful analysis of the legality of ADM Stravridis's proposal, see Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SECURITY (Oct. 14, 2016), https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/.

[55] Lidian Kim, *Russia Having Success in Hybrid War Against Germany*, Reuters (Feb. 7, 2016), http://blogs.reuters.com/great-debate/2016/02/07/russia-having-success-in-hybrid-war-against-germany/.

[56] Ishaan Tharoor, *The Long History of the U.S. Interfering With Elections Elsewhere,* Wash. Post (Oct. 13, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/?utm_term=.6f0d0b7aea38.

Russia has repeatedly accused the United States of impermissibly interfering in Russia's internal affairs.[57]

Officials in the United States government appear as divided as academics are, disagreeing whether the counteraction would be secret, covert, or public; a cyber response in kind or a retaliation in the physical world like sanctions or indictments.[58] Former White House press secretary Josh Earnest signaled, in response to pressing questions on the matter, that the unclear rules of the road in cyber conflict deserved some of the blame: "In many ways, the cyber realm is one where the rules of the road have not been established."[59]

II. WHAT CONSTITUTES CYBER INTERFERENCE IN AN ELECTION?

A. Categories of Interference

One of the difficulties of analyzing cyber election interference is that diverse actions has been lumped together under the umbrella term "hacking." But as illustrated in Part I, states have been affected by a variety of cyber interference in their elections, ranging from misinformation campaigns, to theft of information, to damage to voting machines. International law makes accessible different kinds of protections, and retributions, for each kind.

Parsing cyber interference into four categories begins to make clear where international law is currently equipped to address cyber interference—and where it is not yet. This Part categorizes election interference into four categories, in advance of clarifying in Part III what international legal instruments can be brought to bear on each distinct form of state action. This anticipates the Note's analysis of what remedies can best be brought to bear in addressing those instances of cyber election interference that are not well-suited to existing international legal protections.

1. Category One: Physical Destruction of Voting Equipment

A first category of election interference is physical destruction of votes or voter equipment. U.S. election systems are electronic, and vastly out-of-date.[60] A cyber attack could exploit vulnerabilities in the voting systems to cause them to either suffer from

---

[57] Will Englund, *The Roots of the Hostility Between Putin and Clinton*, Wash. Post (July 28, 2016), https://www.washingtonpost.com/world/europe/the-roots-of-the-hostility-between-putin-and-clinton/2016/07/28/85ca74ca-5402-11e6-b652-315ae5d4d4dd_story.html?utm_term=.cb4b59d266bf.

[58] Claude Barfield, *Russian Hacking: No Good Choices but Action Is Needed,* AMERICAN ENTERPRISE INSTITUTE (Oct. 20, 2016), https://www.aei.org/publication/russian-hacking-no-good-choices-but-action-is-needed/.

[59] *Press Briefing by Press Secretary Josh Earnest, 10/17/2016*, WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Oct. 17, 2016), https://www.whitehouse.gov/the-press-office/2016/10/17/press-briefing-press-secretary-josh-earnest-10172016.

[60] Brian Barrett, *America's Electronic Voting Machines are Scarily Easy Targets*, Wired (Aug. 2, 2016), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

physical damage, or else be out of use—either through a malware infection of a denial of service attack. This kind of *physical* damage makes it easier to argue that the laws of war are applicable to this form of cyber interference.

Experts have commented that this form of attack is possible, due to out-of-date voting infrastructure across the United States. In the U.S. election system, the major subsystems—voter registration, election preparation, ballot casting, vote casting, and vote reporting—each are vulnerable to this type of attack.[61] For the systems that are connected to the internet (the voter registration or the vote reporting systems), a DDOS attack would be possible. But even on the ballot and vote casting machines, out of date infrastructure renders them vulnerable to a physical attack. For example, most U.S. voting machines run Windows XP (for which security patches have been non-existent for at least three years).[62] Researchers have noted that they are susceptible to malware or a denial of service attack.[63]

2. Category Two: Meddling with a vote count

Cyber election interference could involve meddling with the vote count. In the United States, because polling places report tallies digitally to vote collection centers, it would be possible for attacks to target that particular point in the chain: intercepting the true information, and substituting a false vote count, for example.[64] Though the United States incorporates a number of fail-safe procedures to protect against vote rigging, such as the use of provisional ballots, any reported vote-rigging has the potential to both inconvenience voters, slow down an election's results, and disrupt the public perception of the democratic process.

3. Category Three: Theft of Information

A third form of election interference is the theft of information. Russia, for example, used state resources to acquire sensitive information from the U.S. Democratic National Committee and the Republican National Committee.[65]

---

[61] Charles Stewart III and Merle King, *A Cyberattack could disrupt Tuesday's U.S. Elections—but Wouldn't Change the Results*, Wash. Post (Nov. 7, 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/11/07/a-cyberattack-could-disrupt-tuesdays-u-s-elections-but-wouldnt-change-the-results/?utm_term=.4ce5919a6ea1.

[62] Brian Barrett, *America's Electronic Voting Machines are Scarily Easy Targets*, Wired (Aug. 2, 2016), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

[63] Lily Hay Newman, *The Real Hacker Threat to Election Day? Data Deception and Denial,* Wired (Nov. 7, 2016), https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

[64] Lily Hay Newman, *The Real Hacker Threat to Election Day? Data Deception and Denial,* Wired (Nov. 7, 2016), https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

[65] Josh Meyer, *Russia Hack of U.S. Politics Bigger Than Disclosed, Includes GOP*, N.B.C. News (Oct. 8, 2016), http://www.nbcnews.com/news/us-news/russia-hack-u-s-politics-bigger-disclosed-includes-gop-n661866. The information campaign included the theft of emails and data from Capitol Hill staffers, political campaign and party organizations, election and foreign policy wonks, staffers from top Republican and Democratic candidates for president, and associates of Secretery of State Hillary Clinton.

Stealing this information can be useful to another state in several ways. First, a state may simply hold on to this information as valuable intelligence. Or a state might disseminate the information, leading to public doubt of the democratic process. But it's not always clear that a state's goal is coercive in nature when it steals information—a point important for the outcome of this paper's later legal analysis.

4. Category Four: Information campaigns

As explained in Part I, information campaigns are a distinctive feature of cyber election interference. Other cyber attacks on the private sector have included theft of information for business purposes; [66] state attacks on other states have included destruction of equipment, as in Stuxnet. However, information campaigns through cyber interference are a novel form of attack, and one that has gained notoriety through the recent wave of election interference.

It is worth noting that information campaigns can take at least three forms. First, there is what is known as "doxing"—what I will call the dissemination of true information. Second, there are propaganda campaigns—what I define as the dissemination of normative argument. Third, there are misinformation campaigns—what is colloquially referred to as "fake news," in which false information is spread among a populace.

There is often overlap between the three categories; fake news can also contain a normative argument, and doxing can be included among fake news. But it is helpful for the subsequent legal analysis to parse the flavors of information warfare, in order to more thoughtfully consider what legal rights and obligations attach to each of the three kinds of information warfare.

Information campaigns affecting elections are of particular concern in the digital age. Twitter bots can quickly spread information to susceptible voters.[67] And, as of yet, voters—and not platforms—are responsible for gauging the truth of the information they read on social media. Sites such as Facebook, Google, and Twitter do not currently filter or flag fake news, though they have begun to publically discuss the issue.[68]

The spread of fake news creates what Bruno Kahl, head of Germany's foreign intelligence service, calls "political uncertainty." Dissemination of news has the potential to disrupt elections, cause voters to doubt the democratic nature of outcomes, or cause voters to change their votes entirely.[69]

---

[66] Riley Walters, *Cyber Attacks on U.S. Companies Since November 2014*, Heritage (Nov. 18, 2015), http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014.

[67] Lily Hay Newman, *The Real Hacker Threat to Election Day? Data Deception and Denial,* Wired (Nov. 7, 2016), https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

[68] Nick Wingfield, Mike Isaac, and Katie Benner, *Google and Facebook Take Aim at Fake News Sites*, N.Y.Times (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html.

[69] Kathy Gilsinan and Krishandev Calamur, *Did Putin Direct Russian Hacking? And Other Big Questions*, The Atlantic (Jan. 6, 2017), https://www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/.

a) *Doxing, or dissemination of true information*

The first form of cyber interference in an election is the dissemination of true information. Another state can choose to spread information that is verifiable—either because it was gathered as intelligence, because it was stolen in a hack, or because it was garnered in some other way.

There were frequent examples of this practice during the 2016 U.S. election. For example, WikiLeaks posted 20,000 emails sent or received by top officials of the Democratic National Committee.[70] It also released a series of hacked emails from Clinton's campaign manager, John Podesta.[71]

b) Misinformation campaigns, or dissemination of false information

The second form of information campaign is a misinformation campaign, in which untrue information is spread in order to influence elections. Here, the important element is the *coercive* nature of the spread of information. By spreading information that is either false of else misleading, states indicate that their only purpose is to change voters' minds, actions, or inclinations.

For example, during the 2016 U.S. Presidential election, forged documents appearing to come from a senator on the Senate Homeland Security Committee circulated that included a fabricated warning of a cyber attack changing vote counts.[72] Another story went viral on Facebook: that Pope Francis had endorsed Donald Trump.[73] *Buzzfeed* published in full an unverified dossier of allegations regarding Donald Trump's relationship with Russia.[74]

Other false information that *could* impact an election would be disseminating information that polling places are closed; telling voters the wrong polling location, hours, requirements, or even election day; or creating fake stories that warn about the tainting of election results.

c) Propaganda campaigns, or dissemination of normative argument

---

[70] Michael D. Shear, Matthew Rosenberg, *Released Emails Suggest the D.N.C. Derided the Sanders Campaign,* N.Y.Times (July 22, 2016), https://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html.

[71] Dan Berman and Dan Merica, *WikiLeaks Posts More John Podesta Emails*, CNN (Oct. 10, 2016), http://www.cnn.com/2016/10/10/politics/podesta-emails-wikileaks/.

[72] Lily Hay Newman, *The Real Hacker Threat to Election Day? Data Deception and Denial,* Wired (Nov. 7, 2016), https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

[73] Nick Wingfield, Mike Isaac, and Katie Benner, *Google and Facebook Take Aim at Fake News Sites*, N.Y.Times (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html.

[74] Ken Bensinder, Mirian Elder, and Mack Schoots, *These Reports Allege Trump Has Deep Ties to Russia*, BuzzFeed (Jan. 10, 2017), https://www.buzzfeed.com/kenbensinger/these-reports-allege-trump-has-deep-ties-to-russia?utm_term=.ynWK7npbq#.awyzLXDJl.

A third information campaign is the dissemination of normative argument. For example, Voice of America—and its affiliated broadcaster Radio Martí, Radio Free Europe/Radio Liberty and Radio Free Asia —work to "provide reliable news reports in multiple languages to countries that lack a viable independent media and to promote democratic values abroad."[75]

This kind of propaganda campaigns can be intended to change regime structures, incentivize democratic participation, or improve access to information. To that extent, propaganda is coercive in nature as well.

III. INTERNATIONAL LAW APPLICABLE TO ELECTION INTERFERENCE

There is no one cogent body of law that addresses cyber interference in elections.[76] It is only through parsing each *kind* of cyber interference, and each separate body of law that has been applied to cyber attacks, then placing each separate form of attack within the appropriate body of law, do states' responsive options become clarified.

This Part outlines the various bodies of international law that have traditionally been applied to cyber attacks, as well as other sources of law that could be brought to bear on cyber election interference in particular. What becomes apparent through this process is (i) the laws of war tend to require such extensive, physical damage to a state in order to be used, that they often will not be applicable in the case of cyber interference; (ii) human rights treaties, such as the ICCPR, protect citizen rights but have limited means by which states can enforce these rights, and (iii) customary international law may stretch to concepts implicated in election interference, but doing so risks irresponsibly broadening the ability of states to resort to violence. Each of these concerns is taken up in detail in Part IV.

A. International Law – Treaty Protections

To an outside eye, it seems simple; if another state is interfering in a state's democratic process—to such a degree as to change the results of its election—then the interfered-with state should have the right to defend itself. That defense might reasonably include the right to go to war to defend its territorial sovereignty, or its national identity. But international law was constructed such as to incorporate a deliberately high threshold to deter states from going to war. These standards, incorporated into the U.N. Charter, have become something of a puzzle to scholars of international law. Most scholars agree that very few, if any, cyber attacks could ever "cross the threshold" into acts that would give states a justified reason for going to war.

In order to lawfully use force, there are three thresholds in international law: first, acts that constitute a "use of force" under U.N. Charter Article 2(4); second, acts that

---

[75] David Folkenflik, *An Obama-Backed Change at Voice of America has Trump Critics Worried*, National Public Radio (Dec. 14, 2016), http://www.npr.org/sections/thetwo-way/2016/12/14/505482691/an-obama-backed-change-at-voice-of-america-has-trump-critics-worried.

[76] *See, e.g.,* David E. Sanger, *U.S. Wrestles With how to Fight Back Against Cyberattacks*, N.Y.Times (July 30, 2016), https://www.nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyberattacks.html?_r=0.

constitute an "armed attack" under U.N. Charter Article 51; and third, acts that are violations of customary international law, for which states may resort to countermeasures.

1. The Laws of War

a) U.N. Charter Article 2(4): "Use of Force"

The U.N. Charter limits states' abilities to use force. Article 2(4) directs that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." [77] Article 2(4) is understood to be an absolute prohibition on the use of armed force against any other state.[78] And this ban on aggression is regarded as the heart of the U.N. Charter, and the basic rule of contemporary public international law.[79] When a State's conduct rises to the threshold of "use of force," the law of armed conflict is triggered; in other words, victim States are legally entitled to go to war.[80]

b) U.N. Charter Article 51: "Self-defense"

There are two exceptions to Article 2(4)'s ban on the use of force. The first are actions authorized by the U.N. Security Council under Chapter VII of the U.N. Charter.[81]

---

[77] U.N. Charter art. 2, para. 4. The original intent of the authors of the text "was to state in the broadest terms an absolute all-inclusive prohibition [against the use of force]; the phrase 'or in any other manner' was designed to ensure that there should be no loopholes.'" Edward Gordon, *Article 2(4) in Historical* Context, 10 Yale J. Int'l L. 276 (1985), *citing* Brownlie, *The Use of Force in Self-Defense*, 37 Brit. Y.B. Int'l L. 183, 236 n.2 (1961).

[78] *See* David K. Linnan, *Self-Defense, Necessity and U.N. Collective Security: United States and Other* Views, 1 Duke J. of Comp. & Int'l L 63 (1991). Scholars have made arguments that the term "force" in the U.N. Charter applies not only to military attacks and armed violence, but other means of affecting states. Other interpretations of the term "force" have been coercion or interference. *See* Grigori Tunkin, Law and Force in the International System 82 (Progress Publishers trans., 1985) ("[i]n the literature of the socialist states on international law a broad interpretation of force is defended, while a narrow interpretation of that concept prevails in the literature of capitalist states according to which 'force' in the sense employed in the United Nations Charter refers only to armed force"). On the point of interference, *See* Quincy Wright, Subversive Intervention, 54 Am. J. Int'l L. 521, 528 (1960) ("Domain, like property in systems of national law, implies the right to use, enjoy and transfer without interference from others, and the obligation to each state to respect the domain of others. The precise definition of this obligation is the major contribution which international law can make toward maintaining the peaceful co-existence of states."). For a general outline of the interpretations of "force," *see* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 425-30 (2011).

[79] 1 The Charter of the United Nations: A Commentary 116-117 (Bruno Simma ed., 2002).

[80] *See* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operatinos Context*, in 4th International Conference on Cyber Conflict 283, 286 (C. Czosseck et al. eds., 2012) ("[A]n 'armed attack' is an action that gives States the right to a response rising to the level of a 'use of force,' as that term is understood in the *jus as bellum*.").

[81] Chapter VII of the U.N. Charter gives the United Nations Security Council authority to label threats and uses of force as illegal, then to determine what measures should be used to address the illegal behavior. According to Article 39 of the U.N. Charter, the Security Council must determine the existence of a threat to the peace, a breach of the peace, or an act of aggression. After such determinations are made, the Security Council may 1) make recommendations to maintain or restore international peace and security, 2) mandate non-military

The second are actions that constitute legitimate acts of individual or collective self-defense pursuant to Article 51 of the U.N. Charter or customary international law. And states have discovered a third exception, too: states are permitted to conduct operations within the sovereign territory of another state, with that state's consent.

U.N. Charter Article 51 provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[82] It is understood that Article 51 creates an exception to Article 2(4)'s strict prohibition on the use of force,[83] and that "armed attack" is a narrower category than "threat or use of force."[84]

c) The Limitations of the U.N. Charter

The U.N. Charter creates an especially high bar for the use of force in international conflicts: Article 2(4) prohibits it, and Article 51 carves out a limited exception to the rule. What Matthew Waxman calls "translation problems inherent in a U.N. Charter built for a different era of conflict."[85] But what this means is that states have an exacting standard that they must meet before they are allowed to use force in retaliation for another state's unlawful acts. And because the U.N. Charter conceptualizes attacks in a kinetic sense, attacks that don't result in physical destruction—for example, cyber attacks—are unlikely to rise to the level required.

2. International Human Rights

If hacking isn't punished under international law, citizens' individual rights to participate in their states' political process is. Election interference has additional protections within international human rights law. In particular, the right to privacy, and states' obligations to hold "genuine periodic elections" are found in the International Covenant on Civil and Political Rights (ICCPR), to which a whopping 169 states are party.[86] The rights enshrined in the ICCPR are protected, and states cannot easily derogate from their obligations therein. And—given that the title has to do with political rights—several relate to the issue of cyber interference in elections.

---

measures such as diplomatic or economic sanctions pursuant to Article 41, or 3) mandate military enforcement measures pursuant to Article 42.

[82] U.N. Charter art. 51.

[83] *See* Thomas M. Franck, Recourse to Force: State Action Against Threats and Armed Attacks 45-52 (2002).

[84] Not all scholars agree that the "use of force" and "armed attack" are distinct standards. The Tallinn Manual, by contrast, notes the view that "the distinction between the two concepts is either so narrow as to be insignificant or non-existent," such that "any illegal use of force can qualify as an armed attack." Tallinn Manual r. 11 cmt. 7. This view is most prominently espoused by the United States. However, this view is the minority perspective in current customary international law.

[85] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 425 (2011).

[86] International Covenant on Civil and Political Rights, United Nations Treaty Collection, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en.

a) Right to Privacy

Several provisions of the International Covenant on Civil and Political Rights (ICCPR) could be implicated in election interference. First: the ICCPR guarantees individuals a right to privacy, requiring that individuals are not "subjected to arbitrary or unlawful interference with [their] privacy."[87] To that extent, hacks that are made public, or even those that are kept privately, but discovered, might be considered an arbitrary interference in a citizen's privacy.

b) State Obligations to Hold "Genuine Periodic Elections"

Citizens of states that are signatories to the ICCPR also have guaranteed rights to genuine elections—a right that could be restricted if states do not adequately protect their voting infrastructure (commonly termed due diligence obligations) from unlawful interference. The ICCPR obligates states to hold "genuine, periodic elections" without "unreasonable restrictions." Article 25 of the ICCPR states:

> Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions:
>
> (a) To take part in the conduct of public affairs, directly or through freely chosen representatives;
>
> (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the voters;
>
> (c) To have access, on general terms of equality, to public service in his country.[88]

An election that is not genuine (because a vote count was tampered with), or where not everyone has access to themselves be considered for public service (because an election is "rigged") risks falling afoul of these provisions.

c) Prohibition of "Propaganda for War"

Finally, Article 20 of the ICCPR prohibits "propaganda for war."[89] The Commentary on this Article clarifies that this principle: "extends to all forms of propaganda threatening or resulting in an act of aggression or breach of the peace," and is directed "against any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, whether such propaganda or advocacy has aims which are internal or external to the State concerned. "[90] So, a state that creates propaganda that has the result of breaching the peace, whether that peace is breaches at home—or abroad—may find themselves in violation of that obligation.

---

[87] ICCPR, art. 17.

[88] ICCPR, art. 25.

[89] ICCPR, art. 20.

[90] General Comment No. 11, Prohibition of Propaganda for War and Inciting National, Racial or Religious Hatred (Art. 20): .29/07/1983, Office of the High Commissioner for Human Rights.

B. International Law – Customary International Law Protections

Most commentators agree that the vast majority of cyber attacks do not meet the high threshold required under the U.N. Charter. The next appropriate inquiry, then, is whether an attack violates customary international law.

The Draft Articles for State Responsibility hold that a state is responsible for breaches of international obligations that are attributable to it. When states are responsible for misconduct, the state is in turn required to remedy that misconduct: first, by ceasing the misconduct, and second through making reparations—through restitution (returning the situation to the *status quo ante*), compensation, or satisfaction (acknowledging the breach and apologizing for it).

So, the first question is: what international obligations can be breached through cyber interference in elections? And the second—more difficult—question: if a state does not remedy its misconduct, what options are legally available to the victim state to be made whole?

This is where the notion of "countermeasures" is brought to bear. The Draft Articles on State Responsibility, which are customary international law, say that states may use an act of force to bring another state back into line with their international legal obligations. But for a countermeasure to exist, a state first has to identify an "internationally wrongful act" under the Draft Articles that would be sufficient to constitute a retributive act.

In arguing that countermeasures are a permissible response for states to take in the wake of election interference, states have pointed to two potential internationally wrongful acts that are implicated by election interference. The first is a violation of the norm of non-intervention; the second is a violation of the principle of sovereignty.

1. The Norm of Non-Intervention

At its core, the norm of non-intervention forbids states from interfering in the internal or foreign affairs of other states.[91] But not all intervention is prohibited. And little work has been done to either define what differentiates a lawful from an unlawful interference in another state.

The leading case defining the norm of non-intervention and violations of sovereignty is *Military and Paramilitary Activities in and against Nicaragua Case (Nicaragua v. United States of America)*. In the *Niacargua* case, the International Court of Justice addressed the limitations on States' ability to interfere in the internal affairs of another state. According to the Court, the principle of non-intervention involves "the right of every sovereign State to conduct its affairs without outside interference."[92] As such, abiding by the principle of non-intervention means states are forbidden from "intervene[ing] directly or indirectly in internal or external affairs of other States."[93] The

---

[91] *See* Philip Kuunig, *Intervention, Prohibition of,* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L.¶ 9 (Apr. 2008), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL.

[92] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[93] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

Court found that this principle amounted to a rule of customary international law, finding numerous expressions of State *opinion juris* on the matter, as well as documents and resolutions at international organizations that further evidenced this belief.[94]

The Court described a test for determining whether or not the norm of non-intervention had been violated in this manner. "[A] prohibited intervention," the Court said, "must be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely (for example the choice of a political, economic, social and cultural system, and formulation of foreign policy)."[95] Some of this kind of intervention, the Court implied, would be permitted; only certain forms of intervention of this kind are wrong. "Intervention is wrongful," only, said the Court, "when it uses, in regard to such choices, methods of coercion, particularly force, either in the direct form of military action or in the indirect form of support for subversive activities in another State."[96]

The Court, therefore, defined the following elements as inherent in the principle of non-intervention. First, (1) coercion, and particularly force, must be used, (2) it must be used in support of "subversive activities," with the subversion being towards a state's sovereign rights (such as political, economic, social or cultural system), and (3) it must be directed against another state. The Court later uses language to define coercion as "particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[97]

2. Violations of Sovereignty

The Court in *Nicaragua* spoke about the principle of sovereignty as a separate right under customary international law. But it did so poorly, with little articulation as to where the boundary of sovereignty and the norm of non-intervention lie. (And, in fact, the *Tallinn Manual 2.0* has embraced, and exacerbated, this confusion.[98])

The Court stated, "the concept of sovereignty, both in treaty-law and in customary international law, extends to the internal waters and territorial sea of every State and to the airspace above its territory."[99] This implies that the Court understands sovereignty to be a concept linked closely to physical territory.

---

[94] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[95] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[96] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[97] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[98] Andrew Keane Woods, *The Tallinn Manual 2.0, Sovereignty 1.0*, Lawfare (Feb. 8, 2017), https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10.

[99] http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

3. Countermeasures Doctrine

The precise bounds of sovereignty and non-intervention are critical because of the notion of countermeasures. Countermeasures are contemplated in the Draft Articles on State Responsibility. The doctrine allows states to use force to bring an unlawful state back in line with their international legal obligations. This action can be violent: a kinetic attack, like a bombing, could theoretically constitute a countermeasure. Under the Draft Articles on State Responsibility, states are authorized to take what countermeasures against a state committing an internationally wrongful act. Because the I.C.J. has said that the norm of non-intervention and the principle of sovereignty amount to customary international law, states can allege a violation of either as a justification for undertaking a countermeasure.

For a state's use of force to be lawful under countermeasures, the countermeasures must be proportionate to the violation. They must also be intended to bring the out-of-line state back into line, and not intended to punish or exact vengeance.[100] Importantly, in some circumstances, a state can retaliate in a different format of attack; in other words, "a state doesn't have to fight cyber with cyber."[101]

But in order to use countermeasures, states must be able to identify an internationally wrongful act. To that extent, the standard that is accepted by other states as the customary international law for violations of sovereignty, or violations of the norm of non-intervention is essential. The test for the norm of non-intervention articulated by the I.C.J., and the extension of the idea of sovereignty in the recent *Tallinn 2.0*, are different in kind. On the one hand, the *Nicaragua* test for a violation of the norm of non-intervention is broad, sanctioning the use of force in venues and circumstances far beyond those that the founder of the international order intended.[102] And, making matters worse, the *Tallinn 2.0* articulation of violations of sovereignty stretches whatever bounds the *Nicaragua* case placed on the concept of sovereignty beyond physical borders towards a norm of non-intervention-like conception of the state as political entity. If these tests are accepted as the standard for using force, then many states will be able to conduct countermeasures for not only cyber-attacks, but many other actions that touch on the sovereign nature of the state.

---

[100] Kristen E. Eichensehr, *International Law Permits a Measured Military Response to Cyberattacks*, N.Y.Times (Dec. 23, 2014), http://www.nytimes.com/roomfordebate/2014/12/23/when-does-a-cyberattack-warrant-a-military-response/international-law-permits-a-measured-military-response-to-cyberattacks.

[101] Kristen E. Eichensehr, *International Law Permits a Measured Military Response to Cyberattacks*, N.Y.Times (Dec. 23, 2014), http://www.nytimes.com/roomfordebate/2014/12/23/when-does-a-cyberattack-warrant-a-military-response/international-law-permits-a-measured-military-response-to-cyberattacks.

[102] It is also worth noting that the I.C.J. considered whether or not countermeasures were lawful in *Nicaragua* and concluded that they were not. The Court said: "Having found that intervention in the internal affairs of another State does not produce an entitlement to take collective counter-measures involving the use of force, the Court finds that the acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force." Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27). As such, this Note argues that Mike Schmitt's understanding of countermeasures fundamentally misreads, or perhaps missed, this element of the case.

C. Outside Treaty and Custom: Espionage

If war is not permitted either through treaty or through custom, then individuals might also find that the theft of information through hacking might be punished, in some manner, by international law. But the difficulty is that international law would likely classify this action as espionage.

Espionage operates outside any bodies of international law. In fact, the *Tallinn Manual* defines cyber espionage as nonviolent operations that do not qualify as an attack.[103] But acts that pertain to espionage—say, the theft of information—can be prosecuted under domestic criminal law.[104]

IV. WHAT CYBER ELECTION INTERFERENCE IS LAWFUL?

Part III outlined the protections in treaty and customary international law that are relevant to the question of cyber attacks. But this Part shows that when it comes to *cyber election interference*, some international law that has been relevant for general cyber attacks simply does not apply. It also identifies that while international law provides clearer answers or applications as to Categories 1, 2, and 3 (physical destruction of voting equipment, meddling with a vote count, and theft of information), it does *not* provide as much clarity in addressing Category 4: Information Campaigns.

States need the help of international law to address cyber election interference. When it comes to information campaigns, domestic laws such as libel or slander can punish an individual publisher or an individual speaker. However, states lack standing to sue, as well as the time and resources to target thousands of individual "fake news" sharers. Besides, such suits would be inapposite as to what the states are hoping to achieve. What states are looking for is something entirely distinct: the ability to punish states that deliberately wage an information campaign. That is not a right accorded under domestic law. Nor, it seems, is it a right accorded under international law.

States have struggled with international law's relative lack of ability to address information campaigns in the context of cyber election interference. Looking for a solution, some scholars have advanced the argument that the norm of non-intervention and the concept of sovereignty (principles under customary international law) are violated by information campaigns. As Section IV.D will explore, states have largely embraced this argument. As messy and inarticulate as the argument is, states may plausibly claim that an information campaign violated its sovereignty and unlawfully intervened in its domestic affairs; as such, a state would conceivably be authorized to utilize countermeasures to physically punish the state waging the information campaign.

This Note disagrees. Through identifying *why* the concepts of violations of the norm of non-intervention and violations of sovereignty are ill-suited to cyber election

---

[103] 1 The Tallinn Manual on the International Law Applicable to Cyber Warfare 92 (Michael N. Schmitt, ed., 2013) [hereinafter *Tallinn Manual*].

[104] Ashley Deeks, *I Spy, You Spy, We All Spy?*, Lawfare (Sept. 6, 2013), https://www.lawfareblog.com/i-spy-you-spy-we-all-spy.

interference, this Part sets the stage for a careful consideration in Part V as to (i) why states should resist the impulse to engage in countermeasures, and (ii) if not countermeasures, what tools a state might consider instead.

A. Category One: Physical Destruction of Voting Equipment

When cyber interference in an election gives rise to physical consequences in the "real world," then there is a chance it runs afoul of U.N. Charter Article 2(4). In the preparations for the *Tallinn Manual*, the International Group of Experts "unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter."[105]

But Part I illustrated that the threshold for meeting the conventionally-accepted requirements of Article 2(4) is exacting, requiring "the scale of the attack and its effects are comparable to a use of force or armed attack using conventional, noncyber means."[106]

Manipulation or destruction of voting equipment is unlikely to meet this requirement. To understand why, it's helpful to look at a recent example that illustrates the deep disagreement between states, experts, and stakeholders. In the Sony attack, experts disagreed whether the threshold for Article 2(4) had been met—and the Sony attack cost hundreds of millions of dollars in damage to computer equipment.[107]

In the wake of disagreement, it is important to find a solution outside the framework of the U.N. Charter that will allow a state affected by physical destruction of voting equipment a remedy for their harm.[108]

B. Category Two: Meddling with a vote count

Meddling with a vote count implicates the human rights guaranteed to citizens whose votes have been meddled with. Provisions under the ICCPR, including the state's obligation to hold genuine periodic elections are implicated, and citizens can utilize the complaint mechanisms in the ICCPR to seek a remedy.

Citizens who live in states where their votes have been tampered with, where propaganda has made their election less "genuine" or where they have been denied the opportunity to compete for public service have the potential to use the mechanisms provided within the ICCPR to seek a remedy. The ICCPR offers at least two forms of

---

[105] *Tallinn Manual*, at 54.

[106] Kristen E. Eichensehr, *International Law Permits a Measured Military Response to* Cyberattacks, N.Y.TIMES (Dec. 23, 2014), http://www.nytimes.com/roomfordebate/2014/12/23/when-does-a-cyberattack-warrant-a-military-response/international-law-permits-a-measured-military-response-to-cyberattacks.

[107] Peter Elkind, *Inside the Hack of the Century*, Fortune (June 27, 2015), http://fortune.com/sony-hack-final-part/.

[108] It's worth noting that the physical destruction of voting equipment appears to fall within the principles of the norm of non-intervention or violations of sovereignty expressed in *Nicaragua v. United States*. The idea of a remedy based on these doctrines is discussed more completely in Category Four, below.

remedy. First, individuals whose rights to a fair election have been compromised can bring a claim under the ICCPR. Second, states can bring a complaint under the ICCPR against another state that does not ensure the right to a fair election.

Even though meddling with a vote count is clearly unlawful, it is unlikely that citizens whose elections have been implicated will be able to procure a remedy via the ICCPR. The largest concern is one of jurisdiction. In order for citizens to be able to receive a remedy, states must submit to the jurisdiction of the Human Rights Committee or of the ICJ to adjudicate disputes. Many of the states that have been accused of cyber interference in elections are range in their relationship to these international institutions from skeptical to hostile, and have not submitted to further involvement by the Court in their internal affairs.

C. Category Three: Theft of Information

Individuals whose information has been seized in a hack can use domestic law (addressing the theft), or else international law under international human rights treaties, which offer limited remedies by which to redress the harm.

A theft of information affects two provisions of the ICCPR: the right to privacy, and the right to a genuine election. But the ICCPR's remedies are largely cabined to reporting violations to the Human Rights Committee, or appointing a Conciliation Committee.[109] There's also a less conciliatory route: if both states involved agree to submit the question to the jurisdiction of the International Court of Justice[110]--a remedy infrequently used, particularly by the states most affected through recent "election hacking." The probability of states being able to find recourse through this process is small; it is possible that Russia will revoke its grant of jurisdiction to the committee. Besides, however, cyber election interference is unique in that states require some speed in receiving a remedy for the interference. The HRC, which takes all due deliberation before issuing reports or creating remedies, may not be an adequate venue for states to redress their particular harms.

Individuals and states are unlikely to find a remedy within the international human rights structure established via the ICCPR. But that is not to say that the instruments are without value. Importantly, the ICCPR offers states a meaningful hook by which to bring other states into compliance with their international legal obligations. Even if the provisions providing a remedy are not complied with, a state can use the violations of the ICCPR as a means by which to name, shame, and exert diplomatic force on non-compliant states.

D. Category Four: Information campaigns

Information campaigns are the category where the international legal standards applicable are least clear. There is an argument that, at least under the current standard

[109] ICCPR arts. 40-42.

[110] ICJ Statute art. 40(1) and 36.

articulated in *Nicaragua*, information campaigns fall within the language of the norm of non-intervention. And perhaps this is why so much energy is coagulating around this norm, and countermeasures, as a solution: information campaigns are only increasing in frequency and in ferocity, but international law does not offer a compelling means by which to address them.

This paper parsed information campaigns into three categories: the spread of true information, the spread of false information, and the spread of propaganda. And this parsing of kinds of information campaigns gives rise to a series of questions. First, does law make any distinction between true or false information? And second, and more normatively, should it?

The difficult is that international law does not necessarily care about whether or not information is true; rather, it asks whether or not information was coercive. And this test results in strange outcomes for what information could be considered a violation of the norm of non-intervention, and what information campaigns are consonant with international legal obligations.

The difficulty arises because the dissemination of true information could either be for the purpose of changing civilian behavior, or for the purpose of educating civilians. However, the dissemination of propaganda or false information could *only* be spread for the purpose of changing civilian behavior, which in turn could affect the "political, economic, social and cultural system" in a manner that is coercive. As such, states are able to satisfy the definition of the norm of non-intervention articulated by the International Court of Justice. If the current definition of the norm of non-intervention, laid out in *Nicaragua*, is adopted, then states could make a plausible argument that dissemination of false information, propaganda, or even some instances of true information constitute a violation of the norm of non-intervention—and thus engage in countermeasures in retaliation.

V. SEEKING THE BEST REMEDY IN INTERNATIONAL LAW

Part IV illustrated the fractures in international law that incentivizes states to turn towards countermeasures in the *Draft Articles on State Responsibility* as the solution to "below-the-threshold" cyber events. The concern here is grave. The release of the *Tallinn 2.0* Manual made it clear that states were placing great weight on the development of countermeasures doctrine. But such development is myopic. It is dangerous to allow for countermeasures on the basis of either the norm of non-intervention, or violations of sovereignty, for three reasons.

This Part explores why countermeasures, as currently justified within international law, risk development of international law in a direction that could be feasibly used to repress much-needed NGO activity. This Note argues that the risks to the international system as a whole outweigh the utility of using the doctrine. In doing so, it stakes out an opposite position to leading scholars in the field.

But this Note does not leave states empty-handed. It suggests two alternative means through which states could resolve the serious difficulties presented by the current doctrine of countermeasures: first, through making concerted efforts to resolve the ambiguity surrounding the definitions of the norm of non-intervention and violations of sovereignty, which has the potential to put countermeasures doctrine back on the table as

a feasible solution for states to consider. Second, it speaks to the current moment as ripe for states to consider building a *new* treaty that squarely addresses information campaigns. With examples of state stakeholders, suggestions for content, and suggestions for timing, the Note argues that (i) this content *should* be addressed by international law, and (ii) states *can* feasibly address it through treatymaking.

A. Presently, Countermeasures are not the Answer

1. Catch-all, Ill-Defined Categories

Both the concept of sovereignty and that of non-intervention are not well-understood in international law. The current international legal test for a "violation of the norm of non-intervention," as articulated in *Nicaragua v. United States*, is so broad as to allow a great number of acts to be addressed with countermeasures. Many states' actions meet the test, as articulated in *Nicaragua*: acts with (1) a coercive element, (2) in support of "subversive activities" that implicate a sovereign right, including the "political economic, social, or cultural system" of the state, and (3) directed at another state. Many activities—including some necessary for the safety of the international system—can be swept into that definition.

The lines between where the norm of non-intervention falls and what, precisely, constitutes the notion of sovereignty are left unclear through the *Nicaragua* opinion. Two features of the Court's discussion help to yield insight as to what, if any, differences exist between the two concepts. First, the Court imbedded its discussion of sovereignty within its discussion of the norm of non-intervention, stating that non-intervention bears "on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy."[111] What it appears to be, however, is that sovereignty is subsumed within the norm of non-intervention; any violation of sovereignty would also violate the norm of non-intervention (though not the other way around).

Second, the Court made a distinction in its discussion of sovereignty that it did not also make in its discussion of the norm of non-intervention: a relationship to territory. The Court understood sovereignty to relate to land, sea, and physical borders. However, in its discussion of the norm of non-intervention, the Court discussed something broader—a philosophical conception of the state, including the ability to determine a political or economic system of governance or control.

But such a parsing of the relationship between the norm of non-intervention and violations of sovereignty is not universally accepted. Sovereignty has received particular attention in recent scholarship and commentary relating to cyber attacks. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (colloquially known as *Tallinn 2.0*) begins with a discussion of the general principle of sovereignty. "The principle of State sovereignty applies in cyberspace," it says.[112] And *Tallinn 2.0* then

---

[111] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

[112] 2 The Tallinn Manual on the International Law Applicable to Cyber Warfare 92 (Michael N. Schmitt, ed., 2017) [hereinafter *Tallinn 2.0*].

makes a claim that is distinct, in its understanding of what sovereignty is, from what international law has conventionally held: that sovereignty is not a purely territorial concept, but extends into a more liminal domain by far. "In particular," the Manual notes:

> States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure. Although territoriality lies at the heart of the principle of sovereignty, in certain circumstances, *States may also exercise sovereign prerogatives* such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those activities.[113]

This understanding of sovereignty is not consistent with the articulation of sovereignty and non-intervention in the *Nicaragua*. It rather collapses sovereignty and non-intervention into the same conceit, when they were rather understood by the Court to be separate concepts entirely. *Tallinn 2.0* therefore expands what constitutes a violation of sovereignty far beyond its original understanding—one that was cabined by borders and physical space.

Tallinn 2.0 gets it wrong. Insofar as the manual is articulating a "general principle" of law,[114] then the drafters have an obligation to divine that principle in a manner consonant with international law on the matter. And sovereignty is a fundamentally *territorial* concept: that states are imbued with sovereign rights on the basis of their territorial control. This was the reasoning in *Nicaragua*, where sovereignty was held to extend "to the internal waters and territorial sea of every State and to the airspace above its territory."[115] States do not, by contrast, have sovereign "prerogatives… in certain circumstances." Such an interpretation over-extends the doctrine, and thus incentivizes states to bring fairly broad claims as a justification for the use of countermeasures.

2. An Expansion of Lawful Violence

Second, the expansion of countermeasures risks erosion of the international legal order. The existing requirements for violations of the norm of non-intervention under *Nicaragua v. United States* are so broad as to allow too large a scope of interferences. Here is the concern: if a larger-than-expected number of state acts are classified as violations of non-intervention, then we run a risk of greater-than-expected resorts to violence under the countermeasures doctrine. But the international tripwire for the use of force, under UN Charter Article 2(4) and UN Charter Article 51, was deliberately set high. Embracing the doctrine of countermeasures gives states additional opportunities to escalate to violence as a permissible option on the table—the opposite of what the international legal order was designed to protect.

3. The Potential for Repression

Third, many actions necessary for international legal order fall within the existing test for the norm of non-intervention. If the test is whether or not an act is coercive, then

---

[113] *Tallinn 2.0* Rule 1.

[114] ICJ Statute 38(1)(c).

[115] http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

many activities that we understand to be lawful—such as the work of international Non-Governmental Organizations in promoting free and fair elections, promoting democracy, or supporting human rights, could also be considered a violation of the norm of non-intervention. This cannot be right, and the absurd outcome that could result from implementing this test illustrates the great need for the international community to reconceive its understanding of what the test for a violation of the norm of non-intervention should be.

The human rights consequences of allowing countermeasures on the basis of violations of sovereignty or the norm of non-intervention are immense. allowing for countermeasures in the face of intervention in other states risks labeling a whole host of other interventions—necessary interventions, like the functioning of human rights NGOs in other states, like Voice of America, or the Ford Foundation—to be swept up in the net, too. And the international legal order *depends* on these organizations being able to function, bolster domestic civil society, and participate in the creation and enforcement of international law. Embracing the current understanding of either a violation of sovereignty or the norm of non-intervention risks giving authoritarian states permission to conduct violent operations on any states that fund or promote NGOs engaging in "coercive" activities that touch the "cultural" affairs of another state. And many do so.

B. Solutions

This Note takes the position that countermeasures, as currently adopted to remedy a violation of sovereignty or the norm of non-intervention, is a dangerous development in international law. It broadens the scope of lawful violence beyond that intended by the framers of international order, it has the potential to have chilling effects on NGOs and states that spread information for promotion of civil society, and it allows states too broad of leeway to justify physical violence against one another. As such, it is not the best means of addressing cyber election interference via information campaigns.

But this Note argues that states *should* address cyber election interference, including information campaigns, under international law. Cyber election interference has the potential to affect states' sovereign rights to hold free and fair elections, protected both by the ICCPR and under states' own Constitutions. Domestic law leaves states unable to rectify foreign election interference. And international law, normatively, should concern itself with other states' actions that both (i) violate, and (ii) are *intended* to violate those rights guaranteed within the ICCPR, such a states' ability to engage in self-determination through a government of its choosing.

1. Refine Scope of Non-Intervention and Sovereignty for a Digital World

Countermeasures Doctrine Could be Redeemed

My first proposition is that the definitions offered by the International Court of Justice in the *Nicaragua* case, defining sovereignty and the norm of non-intervention, are insufficiently precise. These definitions cast far too broad a shadow. Because many

actions that constitute normatively *beneficial* work in support of civil society and international order could be construed as violations of sovereignty and the norm of non-intervention—such as the work of NGOs in election monitoring—the risk that these terms will be misapplied is too great. States should not have a plausible argument for using physical force against another state for their election monitoring, their publishing of international news, or their promotion of a free and fair press.

But this Note does not condemn the practice of countermeasures entirely. In fact, it believes that countermeasures may be a useful tool in the arsenal for states to utilize as a means of lawfully punishing a state for illegal interference in its sovereignty. What it argues, however, is that the definitions of sovereignty and non-intervention, as currently articulated, are too broad. Therefore, international law must change to accommodate a definition of sovereignty and the norm of non-intervention that aims to make more precise each definition.

How to Change the Content of International Law

International law is created by the agreement of the parties bound to it. Understanding the content of international law, therefore, requires constant surveying of the institutions that reflect state opinion.[116] The clearest articulations and best evidence of state understanding is reflected in treaties or other agreements, as well as through the opinions issued by international tribunals. [117] However, scholarly work and even the consistent and general practice of states can be used as evidence of the content of international law. [118]

As such, this Note suggests five means by which the definitions of the norm of non-intervention and a violation of sovereignty could be reexamined and reformulated, such that the present use of countermeasures as retribution for cyber election interference could be permissible. These solutions are ordered from the most impactful to the least impactful, though each of them has the potential to clarify and update the state understanding of the two rights.

First, a state could bring a case to the ICJ seeking clarification of the norms of non-intervention and violations of sovereignty. A State Party to the ICJ could choose to bring a case of cyber election interference before the ICJ, and ask for determination as to the definitions of sovereignty and non-intervention. A state may do this either through (i) submitting a bilateral agreement with another state party to the ICJ, requesting their jurisdiction over a dispute, or else (ii) submitting an application for the ICJ's jurisdiction against a Respondent State.[119] What makes this avenue less likely to succeed is that all cases of cyber election interference involve Russia, who would be unlikely to consent to the Court's jurisdiction. As such, this Note proposes a second, and more feasible option.

Second, a state or international organization could request an advisory opinion from the International Court of Justice. States alone have the capacity to appear before

---

[116] I.C.J. Statute, art. 38(b).

[117] I.C.J. Statute, art. 38(b).

[118] I.C.J. Statute, art. 38(b).

[119] *How the Court Works*, International Court of Justice, http://www.icj-cij.org/court/index.php?p1=1&p2=6.

the Court; however, international organizations have the potential to appear before the Court through a special procedure of advisory jurisdiction. In order to seek advisory jurisdiction of the ICJ, an international organization's director or secretary-general must file a written request to the Registrar.[120] If granted, the Court will list states and international organizations likely to be able to contribute to the Court's decision, and invite them to participate in written and oral proceedings. Although advisory opinions do not have binding legal affect, they nevertheless "carry great legal weight" and are intended to develop international law.[121] Organizations have typically used advisory opinions to bring controversial issues and cases before the Court; for example, some of the Court's two most notable advisory opinions pertain to the legality of a wall in occupied Palestinian territory,[122] and the legality of using nuclear weapons in armed conflict.[123]

This solution is one of the most promising, because it offers the ICJ a means by which to clarify, correct and update their own working language defining the norms of non-intervention and the right of sovereignty. As such, it will leave less confusion for states and practitioners in determining which of several competing definitions of the norms should be supported. With less room for state interpretation, it is more likely that states will follow the ICJ's understanding. Second, this procedure is not infrequently used; it is very well possible that an international organization—whether the Secretary General, or else another IO director—could be persuaded that this issue is significant and contentious enough to justify the ICJ's time and effort in clarifying.

The greatest drawback to pursuing this solution is that the opinion is, of course, advisory. Greater weight would be accorded the ICJ's opinion should it come from a case, brought by a state party. However, the potential for a state to subject itself to liability in international court in order to receive clarification as to the ICJ's understanding of the terms is dubious.

Third, a state could introduce a resolution in the United Nations General Assembly defining sovereignty and the norm of non-intervention. Such a document could reflect customary international law, even if the agreement is not ratified.[124]

Should none of the more binding means of changing the definitions of the norm of non-intervention or violations of sovereignty be pursued, scholars and practitioners have a chance to also contribute to the changing tide in state understanding of the right of sovereignty and the norm of non-intervention.

Fourth, and importantly, any update to the Tallinn Manual should correct its current articulation of the content of the norm of non-intervention and violations of

---

[120] *Advisory Jurisdiction*, International Court of Justice, http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=2.

[121] *Advisory Jurisdiction*, International Court of Justice, http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=2.

[122] *Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, International Court of Justice (ICJ), 9 July 2004, available at: http://www.refworld.org/cases,ICJ,414ad9a719.html [accessed 16 June 2017]

[123] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996, available at: http://www.refworld.org/cases,ICJ,4b2913d62.html [accessed 16 June 2017]

[124] LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 29-38 (1995).

sovereignty. The Manual is heavily relied-upon as a treatise by scholars and practitioners; the longer its definition, which embraces a broad and non-territorial concept of sovereignty,[125] is permitted to proliferate, the more weight is accorded to the understanding it expresses.

Fifth, even if none of the former suggestions are put into practice, scholars should vociferously contest the *Tallinn* Manual's understanding of sovereignty and the norm of non-intervention. Because scholarly commentary can form international law and shape state practice, scholars should call into question the interpretations offered by the scholars who formulated *Tallinn* and push states and international organizations to adopt a narrower understanding of sovereignty and non-intervention.

2. Time for a New Treaty

The solutions proposed above seek a means of *curing* the current international community's understanding of the norm of non-intervention and violations of sovereignty, such that the proposed use of countermeasures doctrine remains practicable and precise.

Yet this Note has illustrated that international law does not neatly cover the topic of cyber election interference. Though countermeasures doctrine *can* be stretched to encompass the topic, it requires (i) serious modification of the concepts of non-intervention and sovereignty, and (ii) continued monitoring, such that states do not impermissibly extend and expand the scope of their violence against other states.

What may be better than modifying existing law is creating new law: an arms control agreement for information warfare. This would allow states to narrowly tailor their obligations towards one another in the context of cyber election interference. States would be able to tailor their obligations from the outset, craft obligations to which they agree to bind themselves, and make clear how and when violence could ever be used to redress a breach of the agreement. Most critically—and unlike countermeasures doctrine—states could contract such that the ability to resort to violence must be sanctioned by other members of the group, as it is in most other contexts (countermeasures, by contrast, would allow one state to be its own judge and jury as to the question of whether or not the state would be permitted to use force).

One reason that states might consider forming a new treaty rather than modifying old law is that a large and growing number of states have been affected by information campaigns in the context of elections. With an increasing proportion of states affected, the number of states who have found themselves interested stakeholders in the question is increasing. And because information warfare has reportedly largely been perpetrated by one state against many others, it is likely that many stakeholders will find themselves with unified interests in the content and the outcomes of such a negotiation.

[125] 2 The Tallinn Manual on the International Law Applicable to Cyber Warfare 92 (Michael N. Schmitt, ed., 2017)

VI. CONCLUSION

This Note argues that States and scholars alike have focused myopically on the use of countermeasures as a means by which to "hack back." Hamstrung by high bars for the use of force, jurists have sought alternative means by which states can assert their sovereignty and defend their elections from foreign interference.

International and domestic law give states a number of tools by which to defend themselves. In the case of physical damage to infrastructure, such as voting equipment, states have the opportunity to invoke the UN Charter and attack the hacking state. And in the case of "stealing" information, states can go to domestic court to fight espionage. But the rub comes, however, in the proliferation of information: true, false, and normative. Neither international law nor domestic law clearly speaks to the issue, but—desperate for answers—scholars have proven all-too-willing to argue for the use of customary international law, and the application of countermeasures doctrine, as a way to remedy states' harms.

International law is unique, in that it can be constructed through state practice.[126] But the risk of this reality is that states can act in their short-term interests, without giving careful thought to the long-term consequences of their choices. For states to embrace countermeasures doctrine as a means of addressing cyber interference in elections would be myopic. And given that *Tallinn 2.0* is a representation of at least 19 states' and some international experts' perspectives, it is *particularly* important that states not actively embrace this troubled understanding of the development of international law.

And, in addition, because customary international law can be constructed through the writings of the most highly qualified publicists of various nations,[127] international legal scholars should be writing like madmen, offering their take on why *Tallinn 2.0* is poorly reasoned: before states, beset with the serious issue of cyber election interference, start taking the Manual's suggestions seriously.

Because countermeasures doctrine expands the lawful use of violence in the international system, because current precedent allows a greater number of acts to be classified as violations of international law, and because expansion of the norm of non-intervention can be used to silence a variety of necessary actors in the international system, I cannot support its expansion.

But nor does this Note argue that international law should tie States' hands. Rather, it argues that States and jurists have not adequately examined alternative avenues by which to seek a remedy.

Though U.N. Charter Articles 2(4) and 51 have a high threshold, it is not an insurmountable one. And it is possible that a cyber attack could give rise to the level of property damage regarding voting equipment that it *could* be perceived as a use of force or an armed attack under the language of the Charter.

Outside of treaty law, customary international law also offers a solution. Scholars have long argued that there is some affirmative obligation for states to keep their own territory free of hackers: that is, to build virtual barricades that keep hacking from

[126] I.C.J. Statute, art. 38(b).

[127] I.C.J. Statute, art. 38(d).

entering their territory. This argument might properly be based on states' obligations to ensure a genuine election under the ICCPR.

States can counter cyber election interference in several ways. They can protect voting infrastructure. They can also enlist the private sector to help counter the dissemination of information emanating from foreign adversaries.

But each of these solutions is, admittedly, incomplete. And that is, in part, due to the framework of international law in which states can operate in order to redress wrongdoing surrounding election interference. States' most critical prerogative, then, should be recognition of limitations of what an international legal structure built for kinetic attacks can do. Because of the limitations of the present system, states should be incentivized to contribute to the development of new law addressing cyber interference in elections. And, importantly, states should start by reexamining the test for violations for the norm of non-intervention and for violations of sovereignty.

Cyber election interference has begun, but it's nowhere close to ending. With bodies of international law developed in an age of kinetic warfare, existing law does not have a tailor-made solution for states as a means of addressing such interference. But resorting to countermeasures as a lawful excuse to resort to violence is not the answer. Such a decision will cast far too broad a net, sweeping up critical actors in the international system—like NGOs, that *are* involved in activities interfering in the "internal affairs of the state," in the language of *Nicaragua*—that could result in formal crackdowns on civil society organizations. And too, giving states another recourse to violence will lower the barriers to warfare: precisely the opposite result of what international order was constructed to do. By creating a new understanding of what constitutes a violation of sovereignty or a violation of the norm of non-intervention, states will appropriately cabin countermeasures doctrine, preserving a useful tool in international legal order, and protecting civil society from an expansion of violence that could be used against human rights actors in international society.