Chicago Journal of International Law

Volume 19 | Number 1 Article 2

8-16-2018

"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law

Michael N. Schmitt

"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law

Michael N. Schmitt*

Abstract

This Article examines remotely conducted election meddling by cyber means in the context of international law and asks whether such cyber operations qualify as "internationally wrongful acts." An internationally wrongful act requires both a breach of a legal obligation owed by one State to another under international law and attribution of the act to the former. The Article considers three possible breaches related to such meddling—violation of the requirement to respect sovereignty, intervention into the internal affairs of another State, and, when the cyber operations are not attributable to the State from which they were launched, breach of the due diligence obligation that requires States to ensure cyber operations with serious adverse consequences are not mounted from their territory. The Article then examines the various modalities for attributing a cyber operation to a State under international law. Whether cyber meddling in another State's election is unlawful, as well as the severity thereof, determines the range of responses available to the victim State. The Article concludes that the law applicable to remotely conducted meddling in another State's election is unsettled, thereby comprising a normative grey zone ripe for exploitation by States and non-State actors.

Table of Contents

---

* Professor of International Law, University of Exeter; Charles H. Stockton Professor, Stockton Center, U.S. Naval War College; Francis Lieber Distinguished Scholar, Lieber Institute, U.S. Military Academy at West Point; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence; Director, Tallinn Manuals Project, 2009–2017. The views expressed in this article are those of the author in his personal capacity. The author thanks Mr. John Hursh, Editor-in-Chief of *International Law Studies* and Associate Director for Research at the Stockton Center, for his invaluable comments.

I. INTRODUCTION

In the aftermath of the 2016 presidential election, outgoing administration officials, including President Barack Obama and senior leaders of the intelligence community, accused the Russian government of meddling in U.S. elections.[1] European leaders raised similar concerns regarding Russian interference in European elections.[2] In contrast, President Donald Trump labeled the claims a hoax, announced that he believed Russian President Vladimir Putin's denials of meddling, and called the intelligence agency directors "political hacks."[3] Now, more than a year after his inauguration, President Trump continues to claim that "the Russians had no impact on our votes whatsoever."[4]

The possibility that one State might interfere in the political processes of another is hardly shocking. Indeed, the U.S. has a long history of involving itself covertly and overtly in foreign elections.[5] But targeting a "super power" with an influence campaign that exploited social media and remotely conducting active intrusions into its cyber infrastructure marked a significant escalation in election meddling.[6] Various aspects of the Russian campaign almost certainly violated U.S. law, as suggested by the U.S. Department of Justice's February 2018 indictment under U.S. law of numerous Russians and Russian entities with close ties to the government.[7] Far less certain is the character of the operations under international law.

This Article addresses the legality of both the Russian influence campaign and, since it is a growing phenomenon, cyber meddling in general. It attempts to

---

1 Press Release, White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://perma.cc/3XXD-8K5C [hereinafter Obama Press Release]; OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ICA 2017-01D, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (Jan. 6, 2017) [hereinafter ODNI REPORT].

2 Rick Noack, *Everything We Know so Far about Russian Election Meddling in Europe*, WASH. POST (Jan. 10, 2018), https://perma.cc/4XLC-G4JG.

3 Mark Landler & Michael D. Shear, *Indictment Makes Trump's Hoax Claim Harder to Sell*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/us/politics/a-hoax-indictments-make-trumps-claim-even-harder-to-maintain.html.

4 Linda Qui, *How Trump Has Split with His Administration on Russian Meddling,* N.Y. TIMES (Mar. 16, 2018), https://www.nytimes.com/2018/03/16/us/politics/trump-russia-administration-fact-check.html.

5 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.

6 Andy Greenberg, *Everything We Know About Russia's Election-Hacking Playbook*, WIRED (June 9, 2017), perma.cc/UU3W-NUGV.

7 Indictment, United States v. Internet Research Agency, No. 1:18-cr-00032, 2018 WL 914777, (D.D.C. Feb. 16, 2018).

pinpoint when cyber election meddling amounts to one or more "internationally wrongful acts," that is, when it is unlawful under international law and identifies responses available to the target State under international law.

Such "internationally wrongful acts" consist of two elements.[8] First, there must be a breach of a State's legal obligation through either commission or omission. Second, the act in question must be attributable to the State concerned pursuant to the law of State responsibility. Following the examination of these two issues as applied to cyber operations, the Article turns to possible responses under international law by a State that is the target of cyber election meddling. Determining that many cyber operations lie within a "grey zone" of legal uncertainty, particularly with respect to the applicable legal thresholds for unlawfulness,[9] it concludes with the author's reflections on the consequences of this uncertainty vis-à-vis cyber election meddling.

II. THE CONTEXT

The most professional and thorough open-source analysis of the Russian influence campaign is the summary of a classified report on the matter prepared by the U.S. Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) under the auspices of the Office of the Director of National Intelligence (ODNI).[10] Released less than two weeks before President Trump's inauguration, the report's key findings, offered with a "high degree of confidence,"[11] were straightforward:

> Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.[12]

---

8 Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, Draft Articles on Responsibility of States for Internationally Wrongful Acts, pt. 1, art. 2, U.N. Doc. A/56/10, at 26 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2).

9 On grey zones in international cyber law generally, see Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE, no. 2, 2017, at 1–21.

10 ODNI REPORT, *supra* note 1. See also the chronology of matter at 2016 Presidential Campaign Hacking Fast Facts, CNN LIBRARY (Feb. 21, 2018), https://perma.cc/BYR2-WFVR. On the use of cyberspace as a tool of influence, see PIRET PERNIK, INT'L CTR. FOR DEF. AND SECURITY, HACKING FOR INFLUENCE: FOREIGN INFLUENCE ACTIVITIES AND CYBER-ATTACKS (2018), https://perma.cc/VZP4-4L9G.

11 High confidence "generally indicates that judgments are based on high-quality information from multiple sources. High confidence does not imply that the assessment is a fact or a certainty; such judgments may be wrong." ODNI REPORT, *supra* note 1, at 13.

12 *Id.* at ii.

The CIA and FBI concurred, also with a high degree of confidence, that "Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him."[13] The NSA agreed, but only with a "moderate" degree of confidence.[14] Interestingly, once it appeared that Clinton would prevail, the goal of the Russian operations shifted from supporting Trump to undermining the coming Clinton presidency.[15]

According to the report, the Russian cyber influence campaign, which was approved at the "highest levels of the Russian government," was multifaceted.[16] In terms of Russian legal responsibility, the most significant operations were mounted by Russian military intelligence, the General Staff Main Intelligence Directorate or "GRU." The GRU hacked into personal email accounts of Democratic Party officials and other political figures and exfiltrated a great deal of data from the Democratic National Committee (DNC) in March 2016.[17] It then utilized the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to distribute the material, including through various exclusive releases to the media.[18] Additionally, the Russian efforts included hacking into state and local boards of election to acquire a capability to exploit them, although apparently no votes were affected.[19]

During this period, an active Russian propaganda campaign involving numerous media outlets, including RT and Sputnik, was also underway.[20] More legally significant than this classic form of political propaganda were the social media activities of "quasi-government trolls" who "amplified stories of scandals about Secretary Clinton and the role of WikiLeaks in the election campaign."[21] The "troll farm," known as the Internet Research Agency, was financed by "a close Putin ally with ties to Russian intelligence."[22] Although the organization's

---

13 *Id.*

14 Moderate confidence "generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence." *Id.* at 13.

15 *Id.* at ii.

16 *Id.* at 1.

17 *Id.*

18 *Id.* at 2–3. On tying Guccifer 2.0 to the Russian government, see Kevin Poulsen and Spencer Ackerman, *'Lone DNC Hacker' Guccifer 2.0 Slipped up and Revealed He Was a Russian Intelligence Officer*, DAILY BEAST (Mar. 22, 2018), https://perma.cc/V6W9-TG6N.

19 ODNI REPORT, *supra* note 1, at 3; Joseph Tanfani, *Russians Targeted Election Systems in 21 States, but Didn't Change Any Results, Officials Say,* L.A. TIMES (June 21, 2017), http://perma.cc/R7WJ-H3N7.

20 ODNI REPORT, *supra* note 1, at 3–4.

21 *Id.* at 4.

22 *Id.* That ally was Yevgeny Prigozhin, a Russian "oligarch" who both financed and controlled the Internet Research Agency. Neil MacFarquhar, *Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is*

mission was to support the Russian domestic and international political agenda, the extent of control the government exercised over the Internet Research Agency remains unclear; a fact that, as will be explained, hinders legal attribution of its operations to the State.[23]

Consisting of over ninety trolls, the Internet Research Agency spent in excess of two million dollars to purchase anti-Clinton and pro-Trump advertising on social media platforms such as Twitter, Facebook, and Instagram.[24] Using more than 120 groups and social media accounts, the objective was not only to convince individuals how to vote, but also to keep certain voters from the polls. For example, some messaging claimed that "Hillary Clinton doesn't deserve the black vote!"[25] Trolls also leveraged social media to encourage nearly forty anti-Clinton protests and pro-Trump rallies in swing states.[26]

The following year, ODNI released its annual *Worldwide Threat Assessment*, which warned that "[f]oreign elections are critical inflection points that offer opportunities for Russia to advance its interests both overtly and covertly," and that "[t]he 2018 US mid-term elections are a potential target for Russian influence operations."[27] Three days later, the grand jury in Special Counsel Robert Mueller's

---

Known as 'Putin's Cook', N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html. Trolls are individuals who post offensive, inflammatory, derogatory, false, or controversial comments online, often in the hope of inciting a reaction. The name of the activity, "trolling," is derived from the fishing term that referring to drawing a baited line through the water. On trolls, see Zoe Williams, *What is an Internet Troll?,* THE GUARDIAN (June 12, 2012), https://perma.cc/7G2M-B7JC.

23 Adrian Chen, *The Agency*, N.Y. TIMES MAG. (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html; Adrian Chen, *What Mueller's Indictment Reveals about Russia's Internet Research Agency,* NEW YORKER (Feb. 16, 2018), https://perma.cc/DCF4-LY7L; Krishnadev Calamur, *What is the Internet Research Agency?*, ATLANTIC (Feb. 16, 2018), https://perma.cc/WW4E-DJ9W.

24 Oliver Carroll, *St. Petersburg 'Troll Farm' Had 90 Dedicated Staff Working to Influence US Election Campaign*, INDEPENDENT (Oct. 17, 2017), https://perma.cc/BL34-WK9F.

25 Dave Lee, *The Tactics of a Russian Troll Farm*, BBC (Feb. 16, 2018), https://perma.cc/T3L5-KA4J.

26 *See id.* As an example of encouraging rallies, one troll using a false U.S. persona Facebook account sent a message to the "Florida for Trump" account stating:

> Hi there! I'm a member of Being Patriotic online community. Listen, we've got an idea. Florida is still a purple state and we need to paint it red. If we lose Florida, we lose America. We can't let it happen, right? What about organizing a YUGE pro-Trump flash mob in every Florida town? We are currently reaching out to local activists and we've got the folks who are okay to be in charge of organizing their events almost everywhere in FL. However, we still need your support. What do you think about that? Are you in?

Indictment, *supra* note 7, at 26.

27 *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 11 (2018) (Statement of Daniel R. Coats, Dir. of Nat'l Intelligence), https://perma.cc/2J27-8AE5. At a hearing before the Senate Intelligence Committee on February

investigation indicted thirteen individuals and three companies associated with the trolling operations.[28]

Those indicted worked for the Internet Research Agency and were accused of conspiring "with each other and with persons known and unknown to defraud the U.S. by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016."[29] In line with the 2017 intelligence community's assessment, the indictment alleged that "by early to mid-2016, Defendants' operations included supporting the presidential campaign of the candidate Donald J. Trump [ ] and disparaging Hillary Clinton."[30] They also involved the use of social media to criticize Republican candidates Ted Cruz and Marco Rubio, as well as to support the Bernie Sanders campaign.[31]

Of particular importance with regard to international law and the issue of legal attribution that is discussed below is the allegation that the defendants posed as Americans, created false American personas, and stole the identities of real Americans in the effort to leverage social media.[32] At times, some of the defendants even traveled to the U.S. and used U.S.-based cyber infrastructure to mask the Russian origin of their activities.

The week after the indictments were issued, President Trump took to Twitter to claim that "[t]he results of the 2016 election were not impacted or changed" and to allege "[c]ollusion between Russia and Crooked H, the DNC and the Dems."[33] He also chastised then-National Security Adviser H.R. McMaster for failing to make the same claim during his address to the Munich Security Conference.[34]

The U.S. is not alone in falling victim to election cyber meddling. A sampling of such cyber operations signals their growing appeal to States wishing to manipulate foreign elections. Most well-known are the 2014 CyberBerkut (a group

---

13, the leaders of the intelligence community made the same assertions. All of them also reaffirmed the conclusions contained in the 2017 ODNI REPORT, *supra* note 1. *See* Miles Parks, *Russian Threat to Elections to Persist through 2018, Spy Bosses Warn Congress*, NAT'L PUB. RADIO (Feb. 13, 2018), https://perma.cc/W7U9-3KSE.

28 Indictment, *supra* note 7.

29 *Id.* at 2–3.

30 *Id.* at 4.

31 *Id.* at 17.

32 *See also* Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

33 Donald J. Trump (@realDonaldTrump), TWITTER (Feb. 17, 2018, 8:22 PM), https://perma.cc/M4HG-UJR6.

34 *Id.*

of Russian hacktivists) operations targeting the Ukrainian Central Election Commission. Elements of the Commission's network were down for nearly twenty hours and on election day; a false winner was announced.[35] Two years later, the GRU, specifically its APT-28 or "Fancy Bear" hacking unit, targeted the German Bundestag, Germany's Foreign and Finance Ministries, and the Christian Democratic Union's (the party of Chancellor Angela Merkel) systems.[36] Likewise, in 2017, Emmanuel Macron's campaign for the French Presidency was the object of cyber operations that some experts attribute to the GRU.[37] The operations involved phishing attacks meant to implant malware on the campaign's website. Reportedly, the operations' digital fingerprints resembled those of the operations against the U.S. Democratic National Committee and Angela Merkel's campaign the previous year.[38]

In November 2017, such activities led U.K. Prime Minister Theresa May—just a week after Trump stated that he believed Putin's denial of meddling—to announce, "We know what you are doing and you will not succeed because you underestimate the resilience of our democracies, the enduring attraction of free and open societies and the commitment of Western nations to the alliances that bind us."[39] At the same time, the U.K. Electoral Commission opened an investigation into whether the Brexit vote had been targeted.[40]

Even Russia purportedly was victimized by cyber meddling during its presidential election. In 2018, RT News reported a distributed denial of service attack on the Russian Central Election Commission that originated from locations in fifteen countries.[41] The Commission Chairperson stated that the attack had no effect, as its automated election system is "not connected to the global network."[42]

---

35 Nikolay Koval, *Revolution Hacking, in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE 55, 56–58 (Kenneth Geers ed., 2015); *see also* Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR (June 17, 2014), https://perma.cc/N9UE-TVE6.

36 Sumi Somaskanda, *The Cyber Threat to Germany's Elections Is Very Real*, ATLANTIC (Sept. 20, 2017), https://perma.cc/5KA4-MJCR.

37 Eric Auchard, *Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group*, REUTERS (Apr. 24, 2017), https://perma.cc/6FJH-L9LL.

38 *Id.*; *see also* Laura Daniels, *How Russia Hacked the French Election*, POLITICO (Apr. 23, 2017), https://perma.cc/F3X6-DZVG.

39 *Theresa May Accuses Vladimir Putin of Election Meddling*, BBC (Nov. 14, 2017), https://perma.cc/HJ5P-5NAF.

40 *Id.*

41 *Russian Central Election Commission Comes under Cyberattack*, RT NEWS (Mar. 18, 2018), https://perma.cc/D634-SBWL.

42 *Id.*

The U.S. does not come to the table with clean hands, having aggressively engaged in covert operations to influence elections from the 1950s through the 1980s, including such notable examples as Guatemala, Iran, Chile, and Nicaragua. More recently, the U.S. offered economic aid to Russia in an attempt to bolster support for Boris Yeltsin during his 1996 reelection campaign.[43] The U.S. employed the same technique in support of Fatah in the 2006 Palestinian elections, and during the 2005 Iraqi elections Congress blocked a plan to covertly fund certain candidates.[44]

Four years later, the U.S. unsuccessfully tried to prevent the reelection of Afghan President Hamid Karzai.[45] An Afghan Supreme Court justice, who was one of the two Afghans on the five member Electoral Complaints Commission, resigned his post in protest over "foreign interference."[46] Indeed, there is a long-standing U.S. practice of supporting both opposition and civic groups active in mobilizing voters, as in the 2000 reelection campaign of Slobodan Milosevic and on a recurring basis in Belarus in an effort to weaken President Alexander Lukashenko.[47] As Loch Johnson, has observed:

> We've been doing this kind of thing since the C.I.A. was created in 1947. . . . We've used posters, pamphlets, mailers, banners—you name it. We've planted false information in foreign newspapers. We've used what the British call "King George's cavalry": suitcases of cash.[48]

And, as in Russia, the effort extends beyond *de jure* organs of government. In 2016, for instance, the National Endowment for Democracy, a private non-profit organization based in Washington, D.C., awarded nearly $7,000,000 to Russian activists and civic organizations.[49]

Still, some scholars maintain that there is a notable difference between the American and Russian approaches to electoral interference. For example, Thomas Carothers argues that post-Cold War U.S. influence activities are distinguishable from Russia's interference in Western elections, stating:

---

43 *See generally* Thomas Carothers, *Is the U.S. Hypocritical to Criticize Russian Election Meddling?*, FOREIGN AFFAIRS (Mar. 12, 2018), https://perma.cc/WU6L-4XJ5.

44 *Id.*; *see also* Scott Shane, *Russia Isn't the Only One Meddling in Elections. We Do It, Too*, N.Y. TIMES (Feb. 17, 2018), https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html.

45 Sabrina Tavernise et al., *With New Afghan Vote, Path to Stability Is Unclear*, N.Y. TIMES (Oct. 20, 2009), https://www.nytimes.com/2009/10/21/world/asia/21afghan.html.

46 *Afghan Quits Election Complaints Commission*, CNN (Oct. 13, 2009), https://perma.cc/3AUV-J7V3.

47 Carothers, *supra* note 43.

48 Shane, *Russia Isn't the Only One*, *supra* note 44.

49 *Russia 2016*, NAT'L ENDOWMENT FOR DEMOCRACY (Aug. 16, 2017), https://perma.cc/N4RW-PFEN. The endowment no longer reports its recipients in light of new laws making the receipt of foreign funding unlawful.

> [U]nlike Russian electoral meddling, U.S. democracy promotion does not seek to exacerbate sociopolitical divisions, systematically spread lies, favor particular candidates, or undercut the technical integrity of elections. On the whole, it seeks to help citizens exercise their basic political and civil rights in electoral processes, enhance the technical integrity of such processes, and increase electoral transparency.[50]

Regardless of whether this argument is convincing, the question remains as to whether attempts to influence elections, especially in light of current and emerging cyber technologies, comport with international law in general.

III. BREACH OF LEGAL OBLIGATION

The Obama Administration, despite publicly pointing the finger at Russia for engaging in election meddling, never asserted that the actions violated any primary rule of international law.[51] Instead, when imposing sanctions, President Obama merely cited "Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance."[52] Similarly, the report issued by his intelligence agencies failed to allege that the Russian efforts were unlawful under international law. Unsurprisingly, given President Trump's skepticism about the Russian operations, the current administration has remained silent as to whether Russian actions violated internationally binding norms.

This reticence begs the question of the legal character of cyber election meddling. A number of possibilities, examined below, dominate discussion. The two most prominent are violation of the target State's sovereignty and intervention into the internal affairs of the State holding the elections. A third possibility that is often ignored is breach of the obligation to exercise due diligence that the State's territory is not used as the location from which non-State actors or other States launch the cyber meddling operations.

A. Violation of Sovereignty

In the case of election meddling, the likeliest breach by a State of its international law obligations is violation of the target State's sovereignty. Before turning to the merits of that possibility, it is first necessary to address a recent dispute over whether sovereignty is a primary rule of international law or merely a foundational principle from which primary rules such as the prohibitions on

---

50 Carothers, *supra* note 43.

51 Primary rules of international law impose obligations on States, whereas secondary rules set forth "the general conditions under international law for the State to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom." Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8.

52 Obama Press Release, *supra* note 1.

intervention and the use of force emanate.[53] This is a key point because if sovereignty is not a primary rule of international law, then election meddling cannot qualify as an internationally wrongful act in that context.

Until very recently, and as illustrated below, there appeared to be broad consensus that sovereignty is both a principle and a primary rule of international law. As a principle, the concept denotes international law's acknowledgment that States are primarily responsible for what happens on their territory and that other States should respect said competence. On this basis, sovereignty is the fount from which various primary rules, like the prohibition on intervention into the internal affairs of other States, emerged. At the same time, sovereignty was also understood to be a primary rule of international law that is itself susceptible to violation. For instance, States have often accused other States of violating their sovereignty. The classic examples are non-consensual penetration of national airspace or territorial waters by government aircraft or vessels, respectively. In fact, at times, a single act might breach both the obligation to respect another State's sovereignty and a different primary rule derived from the principle of sovereignty, as when a State violates another State's sovereignty by unlawfully employing force within the latter's territory.

This approach had apparently been embraced by the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications, a body consisting of State representatives tasked to assess norms in cyberspace. In its 2015 consensus report, it concluded: "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[54]

Sovereignty as both a principle and rule position was unanimously adopted by the International Group of Experts (IGE) that prepared the *Tallinn Manual 2.0*

---

53 On intervention, see Section III.B, *infra*, and accompanying notes. The prohibition on the use of force is set forth in U.N. Charter article 2(4) and reflects customary international law. The *Tallinn Manual 2.0* experts concurred that cyber operations are capable of violating the prohibition, even when not accompanied by kinetic operations. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]. However, because of the relatively high consequential threshold for violation, it is unlikely, although not inconceivable, that cyber election meddling would qualify as an unlawful use of force. On the subject of cyber uses of force, see Michael N. Schmitt, *The Use of Cyber Force and International Law*, *in* OXFORD HANDBOOK ON THE USE OF FORCE IN INTERNATIONAL LAW 1110 (Marc Weller ed. 2015).

54 Rep. of the Group of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security, ¶ 15, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. GGE 2015 Report]. *See also* Rep. of the Group of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter U.N. GGE 2013 Report].

on the International Law Applicable to Cyber Operations, the product of a seven-year project to determine how international law applies in the cyber context.[55] The IGE consisted of two groups of twenty international experts, and its conclusions were vetted by scores of peer reviewers. Nor did the premise of sovereignty as a primary rule encounter serious pushback from States during the "Hague Process," which brought together fifty delegations, along with representatives from a number of international organizations, to consider drafts of the manual prior to publication.

Finally, adherence to the premise that sovereignty may be violated appeared to be the established U.S. position, as indicated in remarks by Department of State Legal Adviser Harold Koh at a 2012 interagency legal conference held at U.S. Cyber Command:

> States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State.[56]

The position of most other countries is in accord. For instance, at the European launch of *Tallinn Manual 2.0*, Dutch Foreign Minister Bert Koenders noted that "we mustn't be naive. Cyber operations against institutions, political parties, and individuals underline why we need the international legal principles of sovereignty and nonintervention in the affairs of other states."[57]

Indications began to surface in 2016 that certain U.S. officials tasked with rendering legal advice concerning cyber operations had adopted a different view. This view was set forth most fully in an *American Journal of International Law Unbound* article by Colonel Gary Corn, the Staff Judge Advocate of U.S. Cyber Command, and Robert Taylor, a recently retired senior attorney from the Department of Defense's Office of General Counsel. According to Corn and Taylor:

> Some argue that limitations imposed by the concept of sovereignty fill this normative space—that sovereignty is itself a binding rule of international law that precludes virtually any action by one state in the territory of another that violates the domestic law of that other state, absent consent. However, law

---

55 There have been two editions of the book, each prepared by different IGEs. Both treat sovereignty as a primary rule. *Compare* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 1 (Michael N. Schmitt gen. ed., 2013) *with* TALLINN MANUAL 2.0, *supra* note 53, rr. 1–4.

56 Harold Hongju Koh, Legal Adviser, U.S. State Dep't, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012). On the Koh statement, see Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. J. INT'L L. ONLINE 13 (2012). *See also* Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, § A(3)(b), at 737.

57 Bert Koenders, Foreign Minister, Neth., Remarks at The Hague Regarding Tallinn Manual 2.0 (Feb. 13, 2017) (on file with author).

> and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention.[58]

Corn and Taylor's assertions are both counter-factual and counter-normative. First, those taking the opposing view do not argue that any non-consensual cyber operation contravening the target State's domestic law also amounts to a violation of sovereignty. For instance, they are of the view that remote cyber activities that violate domestic law on espionage would not, in themselves, violate international law.[59] Indeed, violation of a State's domestic legal regime seldom bears on the breach of a primary rule of international law. Nor do those viewing sovereignty as a primary rule of law suggest that sovereignty constitutes an absolute bar to cyber operations conducted by other States. Instead, as will be explained, proponents assert that the nature of the cyber activity and its attendant consequences determine whether a violation of sovereignty has occurred. Despite such inaccuracies, it is essential to understand that by adopting the Corn-Taylor approach, election meddling by cyber-means would never amount to a violation of the target State's sovereignty, for only the breach of an obligation contained in a primary rule of international law qualifies as an internationally wrongful act.

The opposing approach was set forth in a *Texas Law Review* article in which the author and a colleague surveyed treatment of the matter by international tribunals, States, international organizations, and academics.[60] We concluded that sovereignty has been treated for decades as a primary rule of international law, and we could identify no basis for treating the concept differently in the context of cyberspace.[61] For us, and for the majority of States and international law experts, the question that presents itself is whether a remote cyber operation such as election meddling rises to the level of a violation of sovereignty.[62] As Brian Eagan, then the Department of State's Legal Adviser, noted during a 2017 Berkeley Law School address:

---

58 Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 208–09 (2017). For a reply explaining the opposing position, see Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AM. J. INT'L L. UNBOUND 213 (2017).

59 *See, for example*, Schmitt & Vihul, *Sovereignty in Cyberspace*, *supra* note 58, at 217–18; TALLINN MANUAL 2.0, *supra* note 53, at r. 32.

60 Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017).

61 *Id.* at 1650–68.

62 *Id.* at 1647; TALLINN MANUAL 2.0, *supra* note 53, at 18–27.

> The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a nonconsensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.[63]

The 1928 *Island of Palmas* arbitration sets forth the classic definition of sovereignty: "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[64] This definition signals the two critical aspects of sovereignty: territoriality and State functions. It also confirms that only States violate sovereignty, either directly, such as by virtue of cyber operations conducted by its organs, or by attribution of a non-State actor's cyber operation pursuant to the law of State responsibility, an issue examined in further detail below.

As noted, it is well-accepted that a State's non-consensual, physical penetration of another State's territory, or even unconsented to and adverse presence thereon, amounts to a violation of sovereignty. The question is when should a remotely conducted cyber operation by, or attributable to, one State that manifests on cyber infrastructure in another's territory be treated as analogously running afoul of the obligation to respect the sovereignty of other States.

The *Tallinn Manual 2.0* experts struggled mightily with this issue. They built rough consensus around two situations. First, the experts agreed, based on the right of a State to control access to its territory, that a violation of sovereignty may result from an infringement on a State's territorial integrity. In this regard, they generally agreed that a remotely conducted cyber operation causing physical damage either to the targeted cyber infrastructure (as was the case with the Stuxnet operation) or objects reliant thereon, or injury to persons, violates sovereignty.[65] It makes no difference whether the damaged cyber infrastructure is private or governmental, for the crux of the violation is the causation of consequences upon the State's territory.

It is unlikely that a State would engage in election meddling by causing physical damage to cyber infrastructure, if only because lesser means would usually suffice to achieve its objective. The more likely scenario is a cyber operation designed to induce a loss of functionality of either election systems or cyber infrastructure with a nexus to the election, such as the servers of a political party. The *Tallinn Manual 2.0* experts extended the notion of damage to loss of

---

63 Brian J. Egan, Legal Adviser, U.S. Dep't of State, Remarks at Berkeley Law School on International Law and Stability in Cyberspace (Nov. 10, 2016), https://perma.cc/B6TH-232L.

64 Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

65 TALLINN MANUAL 2.0, *supra* note 53, at 20.

functionality on the basis that it should not matter whether targeted systems are physically damaged or simply rendered inoperative, for the effect is usually the same—the system no longer works.[66] As an example, the 2012 cyber operations against Saudi Aramco necessitated the replacement of affected computers and therefore, if conducted by another State as is suspected, amounted to a violation of sovereignty even though the systems suffered no physical damage.[67] Treating the loss of functionality as the equivalent of physical damage comports with the object and purpose of the rule of sovereignty: to afford the territorial State control over consequential activities on its territory.

By this teleological approach, a malicious cyber operation that causes any election-related cyber infrastructure on a State's territory to cease to operate would qualify as a sovereignty violation. As an example, a foreign State's operation that disabled the computer systems of a political action committee or media organization that favored one candidate would breach sovereignty. The critical point is not that there was a nexus between the targeted system and the election, but instead simply that the operation resulted in the requisite harm—a loss of functionality.

It must be cautioned that the *Tallinn Manual 2.0* experts could not achieve consensus as to the precise meaning of "loss of functionality." For some, the notion implies an irreversible loss of function. For others, it extends to situations in which physical repair, as in replacement of a hard drive, is necessary. A number of *Tallinn Manual 2.0* experts would treat the need to replace the operating system or bespoke data upon which the functioning of the system relies as a loss of functionality.[68] The author sympathizes with the latter position because the essence of sovereignty is control by the State over activities on its territory; remote cyber operations that necessitate reloading or replacement represent a significant intrusion on that legal prerogative.

The most legally unsettled situations with respect to sovereignty, however, are those cyber operations that manifest on another State's territory without causing physical damage or serious loss of functionality. It was difficult to identify majority and minority views amongst the *Tallinn Manual 2.0* experts on the subject. Even those experts willing to consider the possibility that a violation of sovereignty is possible in such scenarios took contrasting positions. Among the activities proffered by one or more of them as sovereignty violations were:

---

66 *Id.* at 20–21.

67 Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

68 TALLINN MANUAL 2.0, *supra* note 53, at 21.

> a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation.[69]

In the author's view, an operation rendering cyber infrastructure incapable of performing its functions in the manner intended qualifies as a sovereignty violation. One that causes election machinery to misreport results, for example, would fall into this category, as would one that renders machinery incapable of transmitting valid elections results.

Interestingly, and despite disagreement over these diverse examples, each expert tended to justify his or her position by reference to "the object and purpose of the principle of sovereignty that affords States the full control over access to and activities on their territory."[70] In light of this confusing mélange of views, it is impossible to draw definitive red lines regarding cyber election meddling in the context of the territorial aspect of sovereignty, except with respect to situations causing physical damage or at least a significant impact on functionality. Since most operations are unlikely to reach this threshold, a grey zone of normative uncertainty looms when assessing such interference in a foreign State's elections. It accordingly would be difficult to make the case that the Russian cyber operations constituted a violation of U.S. sovereignty solely on the basis that they manifested on U.S. territory.

A more fertile ground for finding a violation of sovereignty vis-à-vis remote cyber operations affecting another State's elections is interference with, or usurpation of, inherently governmental functions.[71] Such activities, which need not cause damage or loss of functionality, violate sovereignty because States enjoy the exclusive right to perform inherently governmental activities on their territory. The "inherently governmental function" concept lacks granularity, although some cases are clear. On the one hand, purely commercial activities, even if engaged in by State-owned enterprises, do not qualify, for they obviously are not within the exclusive purview of a State. On the other hand, law enforcement and defense of the State from external attack are inherently governmental in character.

Between these extremes lies a great deal of uncertainty. Fortunately, for our purposes, a paradigmatic example of an inherently governmental function is the holding of elections. This being so, the issue is whether cyber activities qualify as interference or usurpation by virtue of their effect on an election. "Interference" denotes activities that disturb the territorial State's ability to perform the functions as it wishes. By contrast, "usurpation" involves performing an inherently

---

69 *Id.*

70 *Id.*

71 *Id.* at 21–22.

governmental function on another State's territory without its consent. In both examples, an external actor is disrupting the ability of the target State to perform its governmental functions.

While the usurpation criterion has little relevance in the election meddling context, cyber operations may well be employed to interfere with another State's elections. Certain operations would plainly qualify, as in the case of a cyber operation that altered election data or a temporary distributed denial of service attack against election machinery that rendered it impossible for voters in a particular district to cast their votes. In States with online voting, the implantation of malware in private computers that blocks voting likewise would constitute interference, as would using cyber operations to alter voter registration numbers.

It is equally clear that merely engaging in election propaganda does not amount to interference, at least as a matter of law. This conclusion is supported by the extensive State practice of engaging in both truthful and untruthful propaganda during foreign elections. Of course, such activities may be condemned, as the efforts of RT and Sputnik and the purchase of advertising on social media were in the ODNI Report,[72] but such condemnation is seldom based on assertions of a breach of international law, specifically the obligation to respect sovereignty. This paucity of *opinio juris* and surfeit of contrary practice corroborates the conclusion that election propaganda by cyber-means does not violate a target State's sovereignty.[73]

Other Russian activities likewise failed to reach the level of interference. Although the financial sums spent by Russia and its supporters in attempting to influence the U.S. elections were large, international law imposes no monetary threshold at which the financing of election activities in another State constitutes interference, even though as a practical matter foreign financing can determine the outcome of an election. The penetration by Russian hackers of local boards of election similarly failed to qualify as interference, for there was no subsequent activity that exploited the access to affect the elections. As such, interference did not occur. Moreover, even though Russian operations encouraged protests and rallies, these acts do not qualify as interference because, so long as they are peaceful, they are a regular feature in many democratic elections.

Russian operators succeeded by avoiding both ends of this legal spectrum and instead operated adroitly in the legal grey zone lying between them. Consider the messaging conducted by Russian trolls. The difference between their activities and those of a State or State-supportive media outlet that conducts an open propaganda campaign, even one involving disinformation, is the ability of the electorate to consider the source of the information. Indeed, recall that in order to enhance their efforts, the trolls created fake identities in which they

---

72 ODNI REPORT, *supra* note 1, at 3.

73 On propaganda and sovereignty, see TALLINN MANUAL 2.0, *supra* note 53, at 26.

masqueraded as Americans, sometimes even impersonating actual Americans. Thus, in addition to conveying a message to the electorate, the trolls sought to bolster that message by feigning the source thereof. Arguably, this manipulation of voters' ability to assess the messages in coming to their own decision tipped the scales and therefore constituted unlawful interference.

Another Russian activity within this grey zone was the hacking into various servers containing, *inter alia*, email traffic. As noted, the mere fact that the systems were penetrated does not suffice to qualify the hacking as interference with the election any more than espionage involving government systems is unlawful. In certain cases, however, the operations involved exfiltration of data and its "weaponization" through release at critical points in the election.[74] An assertion that the exfiltration and subsequent release were materially more aggravated than mere propaganda or disinformation, such that the operations qualified as interference, is at least somewhat supportable.

Note, in this regard, that whether the operations successfully swayed the election has no bearing on their lawfulness, as the essence of a sovereignty violation is the fact of interference. That said, there must be a degree of interference even if it does not achieve its desired objective. For example, a cyber operation that attempts to alter election returns, but which is foiled by effective point defenses in the targeted system, lacks the element of interference.[75]

Taken together, the most legally sustainable and persuasive position is that aspects of the Russian influence campaign violated U.S. sovereignty.[76] Yet, this conclusion is far from unassailable. As noted above, an argument, albeit not widely held, holds that sovereignty may never be violated because it is not a primary rule of international law. Moreover, even if sovereignty serves as a primary rule, there was no damage or substantial loss of functionality to any cyber infrastructure related to the U.S. election. Likewise, the Russian operations cleverly avoided actions, such as creating flawed returns, that would unmistakably amount to interference by taking on an inherently governmental function. Although the influence campaign was condemnable, it must be acknowledged that Russia conducted its operations in the grey zone of the law of sovereignty, thereby

---

74 ODNI REPORT, *supra* note 1, at 2–3.

75 *Id.* at 24.

76 Interestingly, the Russian operations would appear to violate a 2015 revision to the Shanghai Cooperation Organization's (of which Russia is a key member together with China) own Code of Conduct, which prohibits using "information and communications technology to . . . interfere in the internal affairs of other States" or "[u]ndermine . . . political, economic, and social stability." Permanent Reps. of China, Kaz., Kyrg., Russ., Taj., and Uzb. to the U.N., Letter dated Jan. 9, 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, arts. 2(3), 2(5), U.N. Doc. A/69/723 (Jan. 13, 2015).

complicating potential U.S. responses and avoiding the international community's opprobrium for violating international law.

B. Intervention

The other breach of an international law obligation most likely to be committed through election meddling is unlawful intervention into the internal affairs of another State.[77] Sovereignty is the foundational principle from which this primary rule of customary law derives.[78] As noted by Lassa Oppenheim, the obligation not to intervene is "the corollary of every State's right to sovereignty, territorial integrity and political independence."[79] Accordingly, States must respect the right of other States to exercise control over certain activities occurring on their territory. Note that like the violation of sovereignty, only States can engage in unlawful intervention, either directly through the actions of their organs or indirectly through instructions to, or control over, non-State actors such as IT companies, hacker groups, or terrorist organizations. And, as with sovereignty violations, cyber operations targeting both private and government infrastructure can qualify as intervention.[80]

Two elements must be satisfied before a cyber operation qualifies as wrongful intervention. The operation must affect a State's *domaine réservé* and it must be coercive.[81] Absent one of these elements, the operation may constitute interference, but it will not rise to the level of unlawful intervention.

With respect to the first element, the difference between an inherently governmental function in the context of sovereignty and the *domaine réservé* is

---

77 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 35 (Apr. 9); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 202, 205, 251 (June 27); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. Rep. 168, ¶¶ 161–65 (Dec. 19); G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, ¶ 3, (Oct. 24, 1970); TALLINN MANUAL 2.0, *supra* note 53, at r. 66. For an extensive list of examples of States styling activities as intervention, and thereby supporting the premise that the prohibition enjoys customary law status, see TALLINN MANUAL 2.0, *supra* note 53, fn. 761. On intervention in the cyber context, see Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249 (Jens David Ohlin, Kevin Govern, & Claire Finklestein eds., 2015); Terry D. Gill, *Non-Intervention in the Cyber Context*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 217 (Katharina Ziolkowski ed., 2013). On intervention generally, see OPPENHEIM'S INTERNATIONAL LAW 428–51 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

78 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 202.

79 OPPENHEIM, *supra* note 77, at 428.

80 TALLINN MANUAL 2.0, *supra* note 53, at 315.

81 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 205; *see also* TALLINN MANUAL 2.0, *supra* note 53, at 314–17.

subtle; the two categories often overlap. The former denotes an activity reserved for the government alone, while the latter refers to one that has not been committed to international law by either treaty or customary law. In its *Nicaragua* judgment, the International Court of Justice (ICJ) explained that "a prohibited intervention must . . . be one bearing on matters in which each State is permitted by the principle of sovereignty, to decide freely."[82] The Court went on to highlight the "choice of a political . . . system" as a clear-cut example of a *domaine réservé*.[83]

The conduct of elections is both an inherently governmental act and within the State's *domaine réservé*. Some limited carve-outs of this *domaine réservé* exist, principally with respect to human rights norms such as self-determination, a topic briefly mentioned below. But, as a general matter, the process by which a State selects its officials is left to the determination of that State and is broadly unregulated by international law. Accordingly, cyber activities by foreign States that affect either the process by which elections are conducted or their outcome qualify as prohibited intervention, so long as the second prong of the intervention test, coercion, is satisfied.[84]

In the election context, the determinative factor distinguishing external influence on an election (which may be unlawful in the context of a sovereignty violation involving an inherently governmental function) from prohibited intervention is the element of coercion. Referring to the right of a State to choose its own political system, the ICJ observed in *Nicaragua*, "Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[85] According to the Court, "the element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention."[86]

The question is therefore what type of election meddling can be said to be coercive. Although international law provides no conclusive definition of the

---

82 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 205; *see also* Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 24 (Feb. 7) (referring to matters "not, in principle, regulated by international law").

83 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 205.

84 The Declaration on the Inadmissibility of Intervention, albeit not necessarily declaratory of customary international law, sets out certain parameters with respect to permissible State actions. It notes that States must "refrain from any action or attempt to destabilize the political system" and "refrain from the promotion, encouragement or support, direct or indirect, of any action which seeks to disrupt the unity or undermine or subvert the political order of other States." G.A. Res. 36/103, annex, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, at ¶ II(e)–(f) (Dec. 9, 1981).

85 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 205.

86 *Id. See also* Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 348 (2009) ("Thus the essence of intervention is coercion. . . . Only acts of a certain magnitude are likely to qualify as 'coercive,' and only those that are intended to force a policy change in the target state will contravene the principle.").

term, the Declaration on Friendly Relations provides that "[n]o State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind."[87] Drawing on this text, the *Tallinn Manual 2.0* experts agreed that coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[88]

Some election meddling certainly would reach this threshold. As Brian Egan noted while serving as Department of State Legal Adviser, "a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."[89] Blocking voting by cyber means, such as by disabling election machinery or by conducting a distributed denial of service attack, would likewise be coercive. In both of these situations, the result of the election, which is the expression of the freedom of choice of the electorate, is being manipulated against the will of the electorate.

At the other end of the spectrum are cyber operations designed to influence decisions in the target State without reaching the threshold of coercion. As explained in the *Tallinn Manual 2.0*:

> [C]oercion must be distinguished from persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State or seek no action on the part of the target State at all.[90]

Therefore, those actions described as lawful in the context of sovereignty violations, like espionage, slanted media reporting by Russian controlled media, and the purchase of advertising to sway the electorate in favor of a particular candidate, are similarly not coercive and do not qualify as a prohibited intervention.

As with sovereignty violations, a significant grey zone of normative uncertainty exists between the two ends of the influence-intervention continuum. Again, the Russian cyber meddling exploited this grey zone, thereby frustrating the ability of U.S. officials to characterize it as unlawful and thereby have the grounds for fashioning a robust response. The two best prospects for qualifying

---

87 G.A. Res. 2625 (XXV), *supra* note 77, at ¶ 3.

88 TALLINN MANUAL 2.0, *supra* note 53, at 317.

89 Egan, *supra* note 63.

90 TALLINN MANUAL 2.0, *supra* note 53, at 318–19.

Russian operations as intervention were the cyber activities that feigned American citizenship and the hacking and subsequent release of private data.

At its core, a coercive action is intended to cause the State to do something, such as take a decision that it would otherwise not take, or not to engage in an activity in which it would otherwise engage. Thus, coercion can be said to "subordinate the sovereign will" of the target State.[91] In the case of elections, this might manifest in the election of a candidate who otherwise would not win, the weakening of a successful candidate's political base, or the strengthening of an unsuccessful candidate's base in anticipation of future elections.

Arguably, the covert nature of the troll operation deprived the American electorate of its freedom of choice by creating a situation in which it could not fairly evaluate the information it was being provided. As the voters were unaware that they were being manipulated by a foreign power, their decision making, and thus their ability to control their governance, was weakened and distorted. The deceptive nature of the trolling is what distinguishes it from a mere influence operation. And it can be argued that the hacking and release tainted the electoral process by introducing information that, albeit genuine, was acquired by means that are expressly prohibited under U.S. domestic law, as well as the law of most other States—namely, the unlawful penetration and exfiltration of private data.[92] In this sense, the electorate's freedom of choice was being thwarted.

These conclusions are by no means unassailable. In particular, it remains unresolved whether coercion requires a direct causal nexus between the act in question and the coercive effect, as in the case of changing election results.[93] A number of *Tallinn Manual 2.0* experts took this position.[94] However, a majority of them, including the author, was of the view that indirect causation of coercive effect suffices.[95] This is an essential distinction because both of the aforementioned Russian activities were indirect in the sense that, while they may have affected the voters' choice of candidates, or even their decision to vote at all, the operations did not in themselves alter the result. Because indirect causation moves the activity along the continuum in the direction of interference and away from intervention, to survive as intervention it is critical to highlight the centrality

---

91 Jamnejad & Wood, *supra* note 86, at 381.

92 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2016).

93 In this regard, it must be cautioned that intervention may be direct or indirect, as in the case of financing insurgents. Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶¶ 205, 228; G.A. Res. 2625 (XXV), *supra* note 77, at ¶ 3; G.A. Res. 36/103, annex, *supra* note 84, at pmbl. The issue being examined here, however, is whether the effect that qualifies as coercive (for example, a change in election results) must be directly caused by the cyber meddling.

94 TALLINN MANUAL 2.0, *supra* note 53, at 320.

95 *Id.*

of the covert nature of the Russian operations and the extent to which they distorted the accepted U.S. electoral dynamic.

If indirect causation satisfies the causal facet of coercion, the fact that intervention need not be directed against governmental election infrastructure is of particular importance, for it means that cyber operations directed against a political party could qualify. An example would be a denial of service attack against the party's website, blog, email or other forms of online campaigning at a critical juncture in the election.[96] A cyber operation that generated false messages purportedly from the party and attempted to sway votes or alter the party's actual messaging in a significant way also would qualify.

President Trump has repeatedly suggested that any election meddling that might have occurred did not affect the outcome. However, whether this is true as a matter of fact is irrelevant as a matter of law. The internationally wrongful act of prohibited intervention does not require that the cyber operations in question be successful. It only requires that they be intended to have a coercive effect with respect to a *domaine réservé*, in this case elections.

As should be apparent, the prohibition of intervention in the context of election meddling, like the violation of sovereignty, is characterized by substantial uncertainty.[97] Fortunately, there is no disagreement over whether the prohibition comprises a primary rule of international law. But, while there are clear-cut cases that either do or do not breach the meddling State's obligations vis-à-vis

---

96 For an innovative, albeit somewhat overbroad, call for application of the principle of non-intervention to DDoS attacks, see William Mattessich, Note, *Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage,* 54 COLUM. J. TRANSNAT'L L. 873 (2016).

97 This uncertainty was acknowledged during a 2017 workshop of the European Leadership Network tasked with assessing "key concepts and norms in Russia-West relations":

> A destabilising factor affecting relations between Russia and the West have been the accusations over suspected interference in elections, both the US elections last year and the Russian elections in 2011. While the text of the non-intervention principle makes no explicit reference to elections, its remit covers direct and indirect activities that breach national and political independence, challenge political stability or change political systems.
>
> Events of the past year and a half highlight the incomplete nature of these prohibitions. The conduct of political campaigns, their direct and indirect support by foreign nationals, external governments, and the funding of parties and lobby groups by foreign states highlight the weakness of the Helsinki sixth principle. In addition, the marketisation of politics including through sponsored political advertisements and private fundraising enterprises has circumvented the non-intervention restrictions. The outcome of an electoral process directly affects a state's political independence and stability, yet the modern-day conduct of elections is not adequately safeguarded against the involvement of foreign actors, and the international normative framework remains incomplete.

DENITSA RAYNOVA, TOWARDS A COMMON UNDERSTANDING OF THE NON-INTERVENTION PRINCIPLE: EUROPEAN LEADERSHIP NETWORK POST-WORKSHOP REPORT 1, 6 (Oct. 2017).

intervention, a significant grey zone lies between the easy cases, particularly with respect to indirect coercion.[98] This grey zone creates legal uncertainly and affords States fertile ground in which to meddle in each other's political activities.

C. Due Diligence

In some cases, a lack of sufficient evidence will preclude officials from concluding that another State conducted cyber election meddling, or that the operations were otherwise attributable to it, as discussed below. However, if it can be established that they were mounted from the territory of a particular State, the possibility that the territorial State may be in breach of its due diligence obligation arises.[99]

The principle of due diligence obligates States to ensure that their territory is not used as a location from which cyber operations having serious adverse consequences for the target State are launched.[100] The ICJ acknowledged the principle of due diligence and the legal obligation it creates in its first case, *Corfu Channel*.[101] In the judgment, the court observed that it is "every State's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states."[102] Judge John Basset Moore of the Permanent Court of Justice had earlier recognized the duty in the celebrated *Lotus* case, where, writing in dissent, he stated, "It is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."[103]

During consultations regarding drafts of the *Tallinn Manual 2.0*, some States expressed a tentative view that despite the notable lineage of the rule, it was of a *lex ferenda* character.[104] Indeed, when the issue of due diligence arose during U.N. GGE deliberations regarding its 2013 and 2015 reports, all that could be agreed

---

98 For an argument that the Russian operations qualify as coercive intervention on the basis of "the nature of state interests," see Steven J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, JUST SECURITY (Mar. 29, 2018), https://perma.cc/85QN-UUQC. The author finds Barela's suggestion interesting, but unreflective of *lex lata*.

99 *See generally* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace,* 125 YALE L.J.F. 68 (2015).

100 TALLINN MANUAL 2.0, *supra* note 53, at r. 6. For an excellent survey of the obligation of due diligence, see INT'L L. ASS'N, STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW: FIRST REPORT (Mar. 7, 2014).

101 U.K. v. Alb., 1949 I.C.J., *supra* note 77.

102 *Id.* at 22; *see also* Neth. V. U.S., 2 R.I.A.A., *supra* note 64, at 839 ("Territorial sovereignty . . . involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States.").

103 S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7) (separate opinion by Moore, J.).

104 The author served as Director of the project and was present at all meetings.

upon was a hortatory statement to the effect that States "should" take actions that are necessary to put an end to harmful cyber operations occurring from their territory.[105]

The *Tallinn Manual 2.0* experts carefully considered this matter, particularly since the principle had been applied principally in the context of transboundary environmental harm.[106] Although they agreed that the principle was a primary rule of international law applicable in cyberspace, they framed a number of strict limitations on its application. First, the due diligence obligation is one of conduct, not result. Thus, so long as a State is taking all feasible measures to put an end to the harmful cyber operations, it is in compliance with the obligation.[107] Second, a majority of the experts took the position that the obligation only requires a State to take action in the face of ongoing harmful cyber activities, or ones in which a material step has been taken towards execution.[108] It imposes no preventative duty to take measures to preclude future deleterious cyber activities from its territory or to monitor its cyberspace for ongoing ones.[109] Third, borrowing from international environmental law, the experts agreed that the obligation only attaches when the consequences for the victim State are "serious."[110] Relatedly, they concluded the cyber activity in question must be "contrary to the rights" of the target State in the sense that if it had been conducted by, or was attributable to, another State, the operation would have qualified as an internationally wrongful act.[111]

Despite these limitations, the principle of due diligence nevertheless acts to relieve a target State of having to attribute election meddling to another State in order to claim that it is the victim of an internationally wrongful act. So long as the former can establish that the cyber operations would breach a legal obligation had they been attributable to a State, for instance by violating sovereignty or qualifying as a prohibited intervention, the State from whose territory the

---

105 U.N. GGE 2013 Report, *supra* note 54, ¶ 23; U.N. GGE 2015 Report, *supra* note 54, ¶ 13(c).

106 *See, for example*, Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941); U.N. Conference on the Human Environment, *Declaration of the United Nations Conference on the Human Environment*, prin. 21, U.N. Doc. A/CONF.48/14/Rev.1 (June 16, 1972); U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, prin. 2, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I), annex I (Aug. 12, 1992).

107 TALLINN MANUAL 2.0, *supra* note 53, at 47.

108 *Id.* at 43–44.

109 *Id.*

110 *Id.* at 34 (drawing from the Trail Smelter Case, *supra* note 106, at 1965); *see also* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, art. 2, ¶¶ 4, 6 of commentary, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) (using the terms "significant" and "substantial").

111 TALLINN MANUAL 2.0, *supra* note 53, at 34.

operations are being launched shoulders a legal duty to take feasible measures to put an end to the operation. The cyber operations must have serious adverse consequences, but interfering with another State's national elections will usually reach that threshold.

In the Russian meddling situation, it may be, as explained below, difficult to attribute the action of non-State actors, especially the Internet Research Agency, to Russia, a necessary step in finding Russia legally responsible for their actions. However, so long as Russia was aware of the troll farm's operations, it is responsible for failing to put an end to these operations, at least to the extent they would have violated international law had they been committed by organs of the Russian State, such as its intelligence agencies. While it is hard to imagine that the Russian authorities were unaware of the trolling, it is difficult to say with great confidence that the operations were unlawful. Again, Russia identified and exploited a grey zone of legal uncertainty.

D. Other Breaches of International Law

Some scholars have raised other possibilities for how Russian election meddling may have breached international law. Particularly creative is Professor Jens Ohlin's assertion that it may have implicated self-determination, which grants a "people" the right to determine "their political arrangements (at a systemic level) and their future destiny (at a more granular level of policy)."[112] Recognized in the first article of both the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights, the right of self-determination is generally recognized as customary international law.[113] The identical articles provide that "by virtue of that right they freely determine their political status."

However, as Ohlin himself notes, there are numerous reasons why international lawyers might hesitate to take this position. They include the fact that arguments based on self-determination typically appear when groups are trying to create a State, perhaps through succession, and that the will of the "people" cannot be determined with any degree of certainty before an election.[114] But the best response against application is that self-determination is simply not

---

112 Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law*?, 95 TEX. L. REV. 1579, 1580 (2017).

113 International Covenant on Civil and Political Rights art. 1(1), Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; International Covenant on Economic, Social and Cultural Rights art. 1(1), Dec. 16, 1966, 993 U.N.T.S. 3; *see also* G.A. Res. 2625 (XXV), *supra* note 77, at ¶ 5; East Timor (Port. v. Austl.), 1995 I.C.J. Rep. 90, ¶ 28 (June 30) (finding self-determination to have an *erga omnes* character).

114 Ohlin, *supra* note 112, at 1596–97.

meant to apply to a situation where the "people" are all citizens of a State rather than a distinct group therein that is denied the right to govern itself, as in the case of colonialism, apartheid, alien subjugation, and perhaps occupation.

Somewhat more promising is Ohlin's examination of the possibility that the Russian operations may have violated the right to privacy under international human rights law. The right to privacy is secured by Article 17 of the ICCPR, which provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation."[115] Russia is also a party to the European Convention on Human Rights, Article 8(1) of which states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[116] The right is generally considered to be customary in nature and applicable to cyber correspondence, such as e-mail.[117]

Ohlin highlights a series of obstacles to a finding that the Russian operations violated the human rights of affected individuals. He notes, for instance, that human rights were originally conceived as applicable to a State's own citizens and points to the extensive practice of espionage that States have not characterized as a violation of the right to privacy.[118] The most significant obstacle, however, is the open question of whether international human rights obligations are extraterritorial in nature, an issue directly on point with respect to cyber operations mounted remotely from outside a State's territory. As Ohlin observes,[119] there has been significant disagreement within the U.S. government over the extraterritorial applicability of the ICCPR.[120]

The broader question is the extraterritorial applicability of human rights obligations generally, including customary law rights such as that requiring respect

---

115 ICCPR, *supra* note 113, at art. 17.

116 Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221.

117 TALLINN MANUAL 2.0, *supra* note 53, at 189. This conclusion is based in part on the fact that the right is found in Universal Declaration of Human Rights art. 12. G.A. Res. 217 (III) A, (Dec. 10, 1948).

118 Ohlin, *supra* note 112, at 1584–85.

119 *Id.* at 1585–87.

120 In particular, the U.S. has long taken the position that the ICCPR obligations do not apply extraterritorially. *See, for example*, U.N. Hum. Rts. Comm'n, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, ¶ 469, U.N. Doc. CCPR/C/USA/3 (Nov. 28, 2005). Interestingly, the State Department's Legal Adviser issued a 2010 memo to the effect this position was incorrect as a matter of law. U.S. Dep't of State, Office of the Legal Adviser, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, at 4 (Oct. 19, 2010). That memo did not mature into the U.S. position.

for the right of privacy.[121] Although the prevailing view is that treaty law (absent a provision to the contrary) and customary human rights law apply extraterritorially, such obligations attach only when the State exercises "power or effective control" either over the foreign territory on which the individual owed the obligation is located or over the individual concerned.[122] Occupation of enemy territory exemplifies the former, whereas detention of the individual abroad illustrates the latter.

In the case of remote cyber operations, the State enjoys neither. An argument nevertheless can be made that a State conducting a remote cyber operation can sometimes control the exercise or enjoyment of a human right.[123] In the Russian cyber operations, for instance, remote non-consensual intrusion into databases containing personal data and the subsequent release of that data arguably deprived the individuals affected of the enjoyment of their right to privacy. Although this is an appealing argument, it is thus far unsupported by either State practice or expressions of *opinio juris*. The approach might amount to laudable *lex ferenda*, but it is not *lex lata*.

Finally, any assertion that the activities underlying the election meddling were unlawful under international law because they constituted espionage can be quickly discarded. Cyber espionage is an act "undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information," whether that information be private or governmental in nature.[124] The GRU's cyber activities in the Russian case, such as the exfiltration of email traffic, clearly constituted espionage. Similarly, collection operations targeting "U.S. primary campaigns, think tanks, and lobbying groups [that were] viewed as likely to shape future U.S. policies" qualify as espionage.[125]

Espionage, *per se*, does not violate of international law.[126] Thus, the mere fact that Russian intelligence agencies were conducting cyber espionage involving the U.S. elections did not render them unlawful. That is not to say that an espionage operation never violates international law, as the means by which the information

---

121 For comprehensive treatment of the subject, see MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY ch. IV (2011).

122 TALLINN MANUAL 2.0, *supra* note 53, at 183–84. The *Tallinn Manual 2.0* experts drew the term "power or effective control" from Hum. Rts. Comm., General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (Mar. 29, 2004). With regard to European Court of Human Rights jurisprudence in this context, see Al-Skeini v. United Kingdom, 2011-IV Eur. Ct. H.R. 99, ¶¶ 130–39; Catan v. Moldova & Russia, 2012-V Eur. Ct. H.R. 309, ¶ 105.

123 TALLINN MANUAL 2.0, *supra* note 53, at 185.

124 *Id.* at 168.

125 ODNI REPORT, *supra* note 1, at 2.

126 TALLINN MANUAL 2.0, *supra* note 53, at r. 32.

is gathered may amount to an internationally wrongful act. For instance, if a government aircraft flying in the national airspace of the target country conducts cyber operations designed to access election-related cyber infrastructure, doing so arguably violates the State's sovereignty by virtue of the unconsented-to presence of the aircraft.

IV. ATTRIBUTION

In a press statement made in the twilight of his presidency, President Obama suggested that Russia's data theft and subsequent disclosure were of a nature that the highest levels of the Russian government must have ordered them.[127] The intelligence community likewise concluded that Putin "ordered an influence campaign in 2016 aimed at the US presidential election."[128] Specifically, it found that the effort consisted of covert and overt activities by "Russian government agencies, State-funded media, third-party intermediaries, and paid social media users or 'trolls.'"[129]

Predictably, Russia demanded that the U.S. provide the evidence to support these allegations.[130] Although the indictment brought by Special Counsel Robert Mueller does contain an account of some alleged Russian activities, a granular U.S. reply is unlikely, in great part because providing this evidence would reveal sensitive cyber capabilities.[131] Moreover, there is no obligation under international law for one State accusing another State of unfriendly—or even unlawful—conduct to reveal the information on which it bases these accusations.[132]

Still, the U.S. government's naming of Russia as the actor behind the influence campaign does raise the issue of the attribution. Recall that an act or omission only qualifies as an internationally wrongful act if it both breaches an obligation under international law and is attributable to a State. In this regard, factual attribution must be distinguished from legal attribution. The former refers to the level of certainty that a cyber operation was conducted by a particular individual, group, organization, or State. As a general matter, factual attribution

---

127 Obama Press Release, *supra* note 1.

128 ODNI REPORT, *supra* note 1, at ii.

129 *Id.* at 2.

130 *Putin Tells U.S. to Send Evidence of Vote Meddling*, REUTERS (Mar. 3, 2018), https://perma.cc/N2AY-G56Y.

131 *See, for example*, David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), https://perma.cc/WY9C-J45T (explaining U.S. unwillingness to reveal the way it was able to attribute the 2014 Sony hack to North Korea).

132 This was the conclusion of the *Tallinn Manual 2.0* IGE. TALLINN MANUAL 2.0, *supra* note 53, at 83. Although there is no legal obligation to do so, the U.N. GGE has encouraged States to provide such evidence when cyber operations are at issue. U.N. GGE 2015 Report, *supra* note 54, at ¶ 15.

under international law is subject to a reasonableness standard.[133] With the notable exception of attribution for the purpose of taking countermeasures,[134] international law generally does not require States to be correct in their determinations; rather, they must be reasonable when making them.

Legal attribution, by contrast, deals with the conditions precedent to a finding that a State is responsible for a cyber operation pursuant to the secondary rules of international law set forth in the law of State responsibility. The International Law Commission has authoritatively restated this body of law in its Articles on State Responsibility.[135] Legal attribution plays an essential role in ascertaining the lawfulness of cyber meddling because a finding that cyber election meddling constituted an internationally wrongful act requires both that the cyber operations involved have breached an obligation owed by the meddling State (the "responsible State" in the law of State responsibility) to the target State (the "injured State") and that the operations were attributable to the former as a legal matter.

The most straightforward form of attribution is on the basis that an organ of the State, like the GRU or other intelligence agency, conducted the cyber operation in question.[136] Such operations are attributable to the State even when they are *ultra vires*, that is, beyond the assigned responsibility of the organ.[137] As an example, if the activities of the Russian intelligence agencies with respect to the U.S. elections were unauthorized, Russia would nevertheless bear responsibility under international law. The key is whether the organ is acting in an apparently official capacity or a purely private one.[138] Engaging in private criminal activity for personal gain would be an example of the latter.

To qualify as an organ of the State, the entity must either enjoy that status under the State's domestic laws or factually act as an instrument of, and in

---

133 TALLINN MANUAL 2.0, *supra* note 53, at 81–82. Fact-finding bodies like tribunals, arbitral panels, domestic courts and the like must abide by the standards and burdens of proof applicable in proceedings before them. These may differ, as in the case of criminal trials imposing a higher standard of proof than applicable in civil proceedings.

134 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, ¶ 3 of commentary to art. 49; TALLINN MANUAL 2.0, *supra* note 53, at 116. A State that misattributes a cyber operation upon which a countermeasure is based commits an internationally wrongful act.

135 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8.

136 *Id.*, art. 4(1); TALLINN MANUAL 2.0, *supra* note 53, at r. 15.

137 And even in the face of contrary direction from superiors. *See* Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at ¶ 13 of commentary to art. 4.

138 *Id.*

complete dependence on, the State.[139] The inclusion of *de facto* organs precludes a State from escaping responsibility for a breach of its international obligations by simply failing to designate as such an entity that is acting as an organ of the State. For instance, by setting up an extra-legal cyber intelligence organization that operates entirely for State purposes and at its direction, a State does not evade legal responsibility for its operations.[140]

By these standards, Russia is responsible for any aspect of the cyber election meddling conducted by its intelligence agencies that amounted to a violation of an international law prohibition, as arguably was the case vis-à-vis the hacking and release operation. However, the activities of State-owned entities present a more complicated situation. The fact that an entity is State-owned does not suffice in itself for attribution of its activities to the State.[141] Rather, it must be determined whether the entity, despite being owned by the State, engages in undertakings that are solely private in nature, such as commerce. If so, its actions are not attributable to the State simply on the basis that it is an organ of the State.

Particularly problematic is the case of State-owned media, for the media sometimes serve governmental purposes like conveying government information to the public or serving as a surrogate of the State internationally in public diplomacy, propaganda, or disinformation activities. Yet, State-owned media may also, despite government ownership, act independently, much like a private media company. In terms of attribution, the key is whether "the State was using its ownership interest in or control of a corporation specifically in order to achieve a particular result."[142] According to the ODNI Report, this was the case with respect to RT and Sputnik because they contributed to the digital part of the influence campaign.[143] However, even if the actions of these and other Russian media might

---

139 *Id.* at ¶ 11 of commentary to art. 4; *see also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶¶ 392–93 (Feb. 26).

140 Person or entities that do not qualify as *de jure* or *de facto* State organs may nevertheless be empowered under domestic law to exercise "elements of governmental authority." If so, their activities, including those that are *ultra vires*, are attributable to the State. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, art. 5; TALLINN MANUAL 2.0, *supra* note 53, at r. 15. Because of the requirement for authorization under law and the limitation to activities that are by nature elements of government authority, attribution on this basis is unlikely in the case of cyber election meddling. A possible exception would be a secret contract to engage in offensive cyber operations during foreign elections.

141 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at ¶ 6 of commentary to art. 8.

142 *Id.* at ¶ 6 of commentary to art. 8 (*citing* Foremost Tehran, Inc. v. Islamic Republic of Iran, 10 Iran-U.S. Cl. Trib. Rep. 228 (1986); American Bell International Inc. v. Islamic Republic of Iran, 12 Iran-U.S. Cl. Trib. Rep. 170 (1986)).

143 ODNI REPORT, *supra* note 1, at 3.

be attributable to the State, it is difficult to style their activities as a breach of any obligation Russia owed the U.S.

As illustrated in the case of U.S. election meddling, the relevant cyber operations may be conducted by actors other than organs of the State, as with the Internet Research Agency's troll farm. Because the nexus to the State is more attenuated in these situations, the threshold for attribution is more demanding than that applicable to organs of the State. For instance, the State is not responsible for *ultra vires* activities of the non-State actors like private companies, patriotic hacker groups, or hacktivists.[144]

The key normative hurdle to attribution, however, is that the State is only responsible for the cyber operations of a non-State actor when the actions taken are pursuant to the "instructions of, or under the direction or control of" the State,[145] or when the State acknowledges and adopts the operations as its own *post factum*.[146] The likelihood that a State might acknowledge and adopt a non-State actor's cyber meddling in another State's elections is slim. Therefore, the crux of the matter is the meaning of the terms instructions, direction, and control.

Both the International Law Commission and legal scholars have struggled to describe the difference between the three terms with meaningful granularity.[147] Their failure has signaled a definitional grey zone no less dense than those described earlier in the context of breaches of obligations, and no less susceptible to leveraging by a State wishing to meddle in foreign elections.

The International Law Commission's commentary to the Articles on State Responsibility suggests that "instruction" denotes a situation in which the non-State actor functions as the State's auxiliary.[148] Restated, a State instructs a non-State actor when it directs the non-State actor to perform a particular cyber operation, including election meddling, on its behalf. There is no requirement that

---

144 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at ¶¶ 7–8 of commentary to art. 8.

145 *Id.* at art. 8; TALLINN MANUAL 2.0, *supra* note 53, at r. 17(a).

146 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, art. 11; TALLINN MANUAL 2.0, *supra* note 53, r. 17(b). Acknowledgment and adoption were illustrated in the actions of the Iranian government following the 1979 occupation of the US Embassy and consulates in Iran and the decision of the Ayatollah Khomeini to perpetuate those activities, including keeping US personnel hostage therein. The International Court of Justice later found Iran responsible on this basis. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. Rep. 3, ¶ 74 (May 24).

147 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, ¶¶ 2–5 of commentary to art. 8; *see also* Kubo Mačák, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors,* 21 J. CONFLICT & SECURITY L. 405 (2016).

148 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at ¶ 2 of commentary to art. 8.

the non-State actor be compensated for the activity involved, although the possibility is not excluded. For instance, a hacker group could execute a cyber operation on the instructions of a State intelligence agency solely out of patriotism. Likewise, a criminal organization could carry out the same operation solely for financial gain. So long as the State told the group to conduct it, motivation is irrelevant.

Although the International Law Commission's commentary suggests that the terms "direction" and "control" are to be understood in the disjunctive,[149] it goes on to treat them ensemble as "effective control,"[150] a standard articulated by the ICJ in *Nicaragua*[151] and subsequently confirmed in its *Genocide* judgment.[152] In the latter case, the Court explained:

> [I]t is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of "complete dependence" on the respondent State; it has to be proved that they acted in accordance with that State's instructions or under its "effective control". It must however be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[153]

Perhaps the best way to think of effective control in the context of attribution for cyber election meddling is a *de facto* ability on the part of the State to cause the non-State group in question to launch a cyber operation that it would otherwise not launch or to refrain from one in which it desires to engage. It need not instruct the group to engage in a particular operation, but the relationship between the State and the group must be such that the State can, if it wishes, compel the non-State group to desist in the operation or alter the conduct thereof.

Unfortunately, the effective control test raises as many questions as it answers. For instance, with what degree of granularity must the State be aware of the operation in question to exercise effective control over it? And by what means may effective control be established? If a State provides all of the funding that makes the group's cyber operations possible, but the group develops its own operational design, is sufficient control in place to attribute the group's cyber activities to the State?

By outsourcing aspects of its interference campaign to private entities and individuals, Russia again found a grey zone of international law that allowed it safe haven to carry out its activities, for it is much more difficult to ascertain legal

---

149 *Id.* at ¶ 7 of commentary to art. 8.

150 *Id.* at ¶¶ 4–5 of commentary to art. 8.

151 Nicar. v. U.S., 1986 I.C.J., *supra* note 77, at ¶ 115.

152 Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J., *supra* note 139, at ¶ 400.

153 *Id.*

attribution in such cases than in those situations involving the State's organs. The U.S. intelligence community may have felt comfortable in attributing the operations of the Intelligence Research Agency and other non-State actors to Russia, but in doing so it was not applying the strict legal tests set forth in the law of State responsibility. Indeed, based on the information contained in their 2017 report and other open source material, it is difficult to conclusively attribute these actions to Russia as a matter of law, although it would seem self-evident that those actions were carried out as a matter of fact in support of Russian governmental objectives. The best that can be said is that it might be reasonable to attribute them to Russia.

V. RESPONSES

Responding to the Russian cyber operations, and as the Trump inauguration loomed, the Obama Administration imposed sanctions on the GRU and Federal Security Service (FSB), four GRU intelligence officers, and three companies that had supported the GRU's operations. The Secretary of the Treasury designated two Russians as having used "cyber-enabled means to cause misappropriation of funds and personal identifying information," while the Department of State shuttered two Russian compounds used for intelligence purposes and declared thirty-five Russian intelligence operatives "*persona non grata*."[154]

In March 2018, the Trump Administration finally announced sanctions on Russia after much foot-dragging following the passage of sanctions legislation in July 2017.[155] This was the first time that the administration had officially acknowledged Russia's involvement in the operations. Of particular note were sanctions on the Internet Research Agency, as well as Russians indicted by Special Counsel Robert Mueller. The FSB and GRU were also sanctioned.[156] Further sanctions, also tied to the legislation, were announced the following month.[157]

---

154 White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://perma.cc/C83Z-SQSL; Obama Press Release, *supra* note 1; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

155 Peter Baker, *White House Penalizes Russians over Election Meddling and Cyberattacks*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html.

156 *Id.*; Laura Smith-Spark & Radina Gigova, *Russia to Expand American 'Blacklist' after New US Sanctions*, CNN (Mar. 16, 2018), https://perma.cc/DY52-LW48. For a list of individuals and entities sanctioned, see U.S. DEP'T OF TREASURY, CAATSA—Russia-Related Designations, Cyber-Related Designations and Designations Updates, Russia/Ukraine-Related Designations Updates, Issuance of Cyber-Related General License 1A, Updated FAQs (Mar. 15, 2018), https://perma.cc/LD9M-NGJM.

157 Gardiner Harris, *Trump Administration Imposes New Sanctions on Putin Cronies*, N.Y. TIMES (Apr. 6, 2018), https://www.nytimes.com/2018/04/06/us/politics/trump-sanctions-russia-putin-oligarchs.html.

Under international law, there are four categories of responses available to States facing hostile cyber operations.[158] The measures taken by the Obama and Trump Administrations fall into the category of "retorsion." An act of retorsion is an unfriendly, but not otherwise unlawful measure,[159] with sanctions and expulsion of diplomatic personnel being the most emblematic and frequent.[160] The cyber operations to which an act of retorsion responds need not constitute an internationally wrongful act, although they may. That both administrations limited their responses to retorsion suggests that they were hesitant to characterize the Russian operations as breaches of international law attributable to Russia. If this was the case, the Russian tactic of operating within the grey zone proved partially successful.

If the cyber operation to which the target State wishes to respond qualifies as an internationally wrongful act, countermeasures may be taken. Countermeasures are measures that would be unlawful, either as a breach of treaty law or of customary international law, but for the fact that they are a response to another State's internationally wrongful act.[161] They must be proportionate to the internationally wrongful act, and, within the cyber context, be designed to cause the other State to desist in its ongoing unlawful cyber operations or to provide assurances, guarantees, or reparations.[162] The classic example is an active defense

---

158 *See generally* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum,* 8 HARV. NAT'L SECURITY J. 239 (2017); *see also* Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SECURITY (Oct. 14, 2016), https://perma.cc/Q8L5-C432.

159 TALLINN MANUAL 2.0, *supra* note 53, at 112.

160 As noted by Professor Sean Murphy in his Statement of Defense of the United States, "every state has the right to grant or deny foreign assistance, to permit or deny exports, to grant or deny loans or credits, and to grant or deny participation in national procurement or financial management, on such terms as it finds appropriate." Sean Murphy, Statement of Defense of the United States, Iran-United States Claims Tribunal, Claim No. A/30, at 57 (1996), https://perma.cc/W92E-3LLM. In support, he cites Iran v. United States, AWD No. 382-B1-FT, 62, 19 Iran-US Cl. Trib. Rep. 273, 292 (Aug. 31, 1988).

161 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at art. 22.

162 *Id.* at arts. 49–53; TALLINN MANUAL 2.0, *supra* note 53, at rr. 20–25, 27–29; *see also* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014). Assurances are a communication by the responsible State that the unlawful act will cease and not be repeated, whereas a guarantee is a measure designed to ensure non-repetition, such as removing providing information that enables the injured State to locate and remove malware. Reparations may take the form of restitution, compensation, and satisfaction (apology).

cyber operation, typically a "hack back" designed to end a malicious cyber operation launched by another State.[163]

Although there are numerous other limitations on the taking of countermeasures, the option allows for flexibility in two regards. First, countermeasures need not be directed at the entity that launched the initial unlawful cyber operation.[164] As an example, unlawful cyber election meddling could be addressed by conducting hack backs against government ministries, or even private cyber infrastructure, so long as the purpose of doing so is to apply pressure to end the meddling; retaliation or punishment are not permissible purposes. Second, countermeasures need not be in kind.[165] Thus, cyber election meddling could be addressed by engaging in non-cyber measures that would otherwise be unlawful, such as imposing trade sanctions that are contrary to a treaty between the two States.[166]

A third response is based upon the "plea of necessity." States may engage in cyber or non-cyber activities that would otherwise be unlawful when their "essential interests" face "grave and imminent peril" and taking the responsive measures is the only way to defend the interest.[167] In such cases, there is no requirement that the situation to which the response is taken either constitutes a breach of a legal obligation or be attributable to a State. This dispenses with much of the grey zone discussed earlier. In the Russian case, for example, the U.S. would not have needed to conclude that the influence campaign violated any primary rule of international law or establish that the nexus between the Russian government and those conducting the operations satisfies the attribution tests set out in the law of State responsibility.

However, those grey zone issues are replaced by others resident in the plea of necessity. The determinative issue is whether the integrity of the election system amounts to an essential interest of the State. Although it is reasonable to hold that the fair and credible election of high-level government officials, especially the President, is an essential interest of the State, whereas the election of local officials might not be, the threshold of essentiality is indistinct. Moreover, the situation must be ongoing or imminent and the threat posed must be extremely serious. Minor cyber election meddling, even in national elections, would not merit a

---

163 On active defense in the cyber context and the recently adopted U.S. policy of facilitating active defense by the private sector, see Morgan Chalfant, *DHS Giving 'Active Defense' Cyber Tools to Private Sector, Secretary Says*, THE HILL (Jan. 16, 2018), https://perma.cc/2ERH-HULF.

164 TALLINN MANUAL 2.0, *supra* note 53, at 112–13.

165 *Id.* at 128–29.

166 Unless the treaty sets forth the remedy for, or process to handle, a breach of its terms.

167 Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 8, at art. 25; TALLINN MANUAL 2.0, *supra* note 53, at r. 26.

response based on the plea, while meddling that threatened the outcome of an election might be characterized as grave. Determining when the peril posed by cyber election meddling in other cases qualifies as grave is more challenging.

The final response option is the use of cyber or non-cyber force in self-defense pursuant to Article 51 of the U.N. Charter and customary international law. The textual condition precedent for self-defense is an "armed attack."[168] Unfortunately, the threshold at which a cyber operation qualifies as an armed attack is unsettled.[169] Certainly, a cyber operation that causes significant physical damage or injury suffices, although consequences at this level are highly unlikely with respect to cyber election meddling. Whether nondestructive or injurious consequences that are severe would merit the use of force in self-defense is highly questionable. In the author's opinion, it is difficult to envision even internationally unlawful cyber election meddling that would, without more, allow the target State to resort to force in order to put an end to the operations.

VI. REFLECTIONS ON GREY AREAS

Cyber election meddling presently exists within the grey zone of international law. This zone of normative uncertainty presents a tempting environment for States that are not fully committed to the international rule of law. By operating within the grey zone, these States can avoid consensus condemnation of their cyber operations as violations of binding international legal norms. Moreover, absent a clear violation of international law attributable to the State launching the operations—and as the U.S. responses to date have demonstrated—victim State responses will generally be limited to acts of retorsion.

As the international community struggles to identify how extant norms such as respect for sovereignty, the prohibition of intervention, and due diligence obligations apply to cyber operations, some of those involved in cyber law and policy are attempting to limit the reach of international law into cyberspace. For instance, the recent failure of the U.N. GGE to agree upon text for its aborted 2017 report concerning such basic matters as applicability of the law of self-defense and international humanitarian law, topics that they had addressed in previous reports, marks a major step backwards.[170] That opposition to the text included Russia and China does not bode well for global cyber security or the rule of law more generally. Clearly, certain States are embracing legal ambiguity as a force multiplier in their cyber operations. In the realm of cyber election meddling,

---

168 U.N. Charter art. 51.

169 TALLINN MANUAL 2.0, *supra* note 53, at 340–44; Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited,* 56 VILL. L. REV. 569, 586–603 (2011).

170 Michael N. Schmitt & Liis Vihul, *International Cyber Law Politicized: The U.N. GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://perma.cc/3EXH-VYE8.

the ambiguity stretches from an existential threat to sovereignty as a primary rule of law to confusion over the application of the coercion criterion to voting behavior. This ambiguity represents a troubling threat to the democratic process.

Some States are taking the lead in attempting to shrink the grey zone. Efforts to bring like-minded States together to craft consensus are laudable. So too are cyber law capacity-building efforts such as the Netherlands' "Hague Process," in which the Netherlands sponsors regional training in collaboration with other States to construct common ground for future negotiations over the content, shape, and vector of international cyber law.[171]

Ultimately, States need to make a choice. The grey zone represents both opportunity and threat. Until States exercise their prerogative to develop new norms and interpret existing ones in the context of cyber operations, those States that are not committed to a rule-based international order will enjoy an asymmetrical advantage over those that are dedicated to compliance with the law. And foreign elections will continue to represent a lucrative target in the strategies of the former.

---

[171] Personal knowledge of the author; training conducted in collaboration with Cyber Law International.