INTERNATIONAL LAW STUDIES
Published Since 1895

Foreign Cyber Interference in Elections

Michael N. Schmitt

97 INT'L L. STUD. 739 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Foreign Cyber Interference in Elections

Michael N. Schmitt[*]

CONTENTS

* Professor of International Law, University of Reading; Stockton Distinguished Scholar-in-Residence, U.S. Naval War College; Francis Lieber Distinguished Scholar, West Point; Strauss Center Distinguished Scholar, University of Texas; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence. An early version of this article appeared in a series of three *EJIL:Talk!* posts in October 2020. The author is grateful for the invaluable assistance and insights of Professor Marko Milanovic (Nottingham University) and Liis Vihul (Cyber Law International).

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

With the contentious U.S. 2020 elections having concluded, it is a propitious moment to examine the international law rules bearing on foreign interference by cyber means in this fundamental expression of democracy. As in 2016, "President Putin and the Russian state authorized and conducted influence operations against the 2020 U.S. presidential election aimed at denigrating President Biden and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US."[1]

Russia did not, however, attempt to "alter[ ] any technical aspect of the voting process, including voter registration, ballot casting, vote tabulation, or reporting results."[2] Instead, its "online influence actors sought to affect US public perceptions of the candidates, as well as advance Moscow's longstanding goals of undermining confidence in US election processes and increasing sociopolitical divisions among the American people."[3]

But Russia was not alone. According to the U.S. intelligence community, "Iran carried out a multi-pronged covert influence campaign intended to undercut former President Trump's reelection prospects," while "a range of additional foreign actors—including Lebanese Hizballah, Cuba, and Venezuela—took some steps to influence the election."[4] Interestingly, China did not conduct operations designed to alter the outcome, although it did consider doing so.[5] Despite counterfactual claims to the contrary by Trump, however, the United States successfully conducted the 2020 election.[6]

---

1. NATIONAL INTELLIGENCE COUNCIL, FOREIGN THREATS TO THE 2020 US FEDERAL ELECTIONS 2 (Mar. 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

2. *Id.* at 1.

3. *Id.* at 3.

4. *Id.* at i.

5. *Id.*

6. Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Nov. 12, 2020), https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election. The President fired Christopher Krebs, the Director of the Cybersecurity and Infrastructure Security Agency, the agency that released the statement. David E. Sanger & Nicole Perlroth, *Trump Fires Christopher Krebs, Official Who Disputed Election Fraud Claims*, NEW YORK TIMES (Nov. 17, 2020), https://www.nytimes.com/2020/11/17/us/politics/trump-fires-christopher-krebs.html.

While actual and potential interference in American elections has captured the most attention, the phenomenon is global. For instance, in an amicus brief filed in federal court, former U.S. national security officials have asserted,

> Over the last several years, evidence has emerged that Moscow has launched an aggressive series of active measure campaigns to interfere in elections and destabilize politics in Montenegro, Ukraine, Moldova, France, Germany, the Netherlands, Estonia, Sweden, Austria, Italy, Poland and Hungary, to name just a few. They sought to inflame the issues of Catalonian independence and the Brexit vote in the United Kingdom.[7]

Even Russia has been victimized. In 2018, for example, a distributed denial of service attack was conducted against Russia's Central Election Commission, allegedly from locations in fifteen countries.[8]

Such election-related cyber operations have captured the international law community's attention, as evidenced by the recent *The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means*, which 171 experts in the field signed.[9] This article examines how international law applies to election interference from three angles. Part II as-

---

7. Brief for Former National Security Officials as Amici Curiae Supporting Neither Party at 8, Roy Cockum et al. v. Donald J. Trump for President, Inc. et al., No. 1:17-cv-1370-ESH (Dist. Ct. D.C. Dec. 8, 2017). Interestingly, the U.S. Justice Department has indicted six Russian GRU intelligence officers for, *inter alia*, attempted interference in the 2017 French elections. Press Release, U.S. Dep't of Justice, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

8. *Russian Central Election Commission Comes Under Cyberattack*, RT (Mar. 18, 2018), https://www.rt.com/news/421622-russian-election-under-cyber-attack/.

9. The Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means, https://elac.web.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through (last visited Mar. 29, 2021). *See also The 9 Principles*, PARIS CALL (Dec. 11, 2018), https://pariscall.international/en/principles (Principle 3 provides that States and others must "Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities."); *Advancing Cyberstability: Final Report*, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE (Nov. 2019), https://cyberstability.org/report/ (Proposed Norm 2 provides, "State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.").

sesses if, and if so when, such interference by cyber means violates international law, particularly the rules prohibiting violation of a State's sovereignty or intervention in its internal affairs, or those requiring respect for international human rights. In Part III, the discussion turns to the duties States shoulder to put an end to hostile cyber election interference pursuant to the principle of due diligence and the requirement to protect international human rights. The article concludes in Part IV with a brief survey of the response options available under international law to States facing election meddling by cyber means.

II. INTERFERENCE AS A VIOLATION OF INTERNATIONAL LAW

Election interference by foreign States rises to the level of an "internationally wrongful act" when two elements are present.[10] First, the action or omission in question must be *legally attributable* to a State. Second, that act must *breach* an obligation owed in international law to the target State. I will first briefly examine the attribution element and then move on to the various substantive obligations that election interference is most likely to breach—the prohibition of intervention, the duty to respect the sovereignty of other States, and the obligation to respect human rights.

A. Attribution

Attribution in the legal sense must be distinguished from attribution in the technical sense of the word, although the latter forms the factual predicate for the former. Legally, the concept of attribution denotes a situation in which an individual or group's conduct is regarded as that of a State. The challenge is that there are many forms of relationship to a State. For instance, in 2020, "Russia's intelligence services, Ukraine-linked individuals with ties to Russian intelligence and their networks, and Russian state media, trolls, and online proxies engaged in activities" targeting the U.S. elections.[11]

---

10. Int'l Law Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries*, 56 U.N. GAOR Supp. No. 10, art. 2, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf [hereinafter Articles on State Responsibility]. The Articles on State Responsibility are a restatement of the customary law of State responsibility that is considered generally, albeit not entirely, accurate by most States.

11. NATIONAL INTELLIGENCE COUNCIL, *supra* note 1, at 2.

The clearest basis for attributing a cyber operation that interferes with an election is when an *organ* of the State conducts it,[12] as was the case with Russian intelligence agencies and their 2016 and 2020 U.S. election interference and influence campaigns.[13] An entity may qualify as an organ of the State either by being designated as such in the State's law or operating in "complete dependence" on the State.[14] The latter basis precludes the possibility of a State escaping responsibility for election interference by using an organization that lacks de jure organ status under its domestic law, but that nevertheless engages in cyber activities for and at the State's direction; in other words, acts as its de facto organ.[15]

When non-State actors conduct cyber operations, the most likely basis for attribution is that they acted "*on the instructions of, or under the direction or control of*" of the State.[16] This would appear to be the legal basis for attributing the Internet Research Agency's 2016 operations to Russia.[17] And, as noted, Russia turned to various forms of proxy actors in 2020.

The terms instruction, direction, and control are somewhat ambiguous. Some cases are self-evident, as when there is a contractual relationship between the State and a private company, like a marketing agency or social media consultancy, that is conducting the election interference, on the one hand (attribution), or when "patriotic hackers" carry out the operations without any State involvement, on the other (no attribution). Yet, in many cases, assessing whether the relationship between the non-State actor and the State amounts to instructions, direction, or control is not straightforward. This is not necessarily because of a lack of clarity in the attribution rules, but instead because of a dearth of evidence as to the nature of the relationship between the State and the non-State actor.

---

12. Articles on State Responsibility *supra* note 10, art. 4; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 15 (Michael N. Schmitt gen. ed., 2017).

13. Guy Faulconbridge, *What is Russia's GRU Military Intelligence Agency?*, REUTERS, Oct. 5, 2018, https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-idUSKCN1MF1VK.

14. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 392 (Feb. 26); Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 109–10 (June 27).

15. Articles on State Responsibility, *supra* note 10, cmt. ¶ 11 to art. 4.

16. *Id.* art. 8 (emphasis added); *see also* TALLINN MANUAL 2.0, *supra* note 12, r. 17.

17. Permanent Select Committee on Intelligence, U.S. House of Representatives, *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*, https://intelligence.house.gov/social-media-content/ (last visited Mar. 30, 2021).

Without attribution to a State, cyber election interference by non-State actors does not violate international law, although it may trigger positive obligations of prevention that are discussed below. But even when a cyber operation is attributable to a State, the interference must breach *an obligation* owed to the State conducting the election before it qualifies as an internationally wrongful act. In that regard, the discussion first turns to the prohibition of intervention.

B. Prohibition of Intervention

The international law rule that has drawn the most attention with respect to foreign cyber election interference is the prohibition of intervention into the internal or external affairs of other States. Appearing in such instruments as the 1970 Friendly Relations Declaration,[18] it is a well-accepted rule of customary international law.[19] Variants also appear in treaties such as the Charter of the Organization of American States.[20] However, caution is merited in applying the treaty rules because their parameters may differ from their customary counterpart, which is the focus of the discussion below. The applicability of the customary prohibition in the cyber context was confirmed in the 2015 UN Group of Governmental Experts (GGE) report that the General Assembly subsequently endorsed.[21] No State opposed this position.[22]

---

18. 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 (Oct. 24, 1970).

19. Philip Kunig, *Intervention, Prohibition of*, MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW (updated Apr. 2008), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=sOnqwN&result=1&prd=OPIL.

20. Charter of the Organization of American States art. 2(b), Apr. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3.

21. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter dated 26 June 2015 from the Chair of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Established Pursuant to Resolution 68/243 (2014), ¶ 24, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter 2015 Rep. of the Group of Governmental Experts]; G.A. Res. 70/237 (Dec. 30, 2015) (endorsement). For an analysis of the rule in the cyber context, see TALLINN MANUAL 2.0, *supra* note 12, cmt. to r. 66.

22. See, e.g., statements by State officials on election interference by cyber means and intervention. Ministry of Foreign Affairs, Government of Finland, International Law and Cyberspace: Finland's National Positions 3, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 (last visited Mar. 30, 2021) [hereinafter Finland's National Positions]; Roy Schöndorf (Deputy

As understood in customary law, intervention consists of two elements famously set forth by the International Court of Justice in its *Paramilitary Activities* judgment.[23] Both must be satisfied before a breach exists. First, the cyber operation in question has to affect another State's internal or external affairs, that is, its *domaine réservé*. Second, it must be coercive. States that have spoken to the issue are in accord with these constitutive elements. For instance, the 2019 "International Law Supplement" to Australia's *International Cyber Engagement Strategy* explains, paraphrasing the International Court of Justice in *Paramilitary Activities*, that a "prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that the principle of state sovereignty permits a state to decide freely."[24]

Within the *domaine réservé*, the area of activity international law leaves to regulation by States, States enjoy discretion to make their own choices. Elec-

---

Attorney General of Israel), *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395, 403 (2021); Government of the Netherlands, Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, app. at 3 (July 5, 2019), https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter Netherlands, International Legal Order in Cyberspace]; Jeremy Wright, UK Attorney General, Address at Chatham House: Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Brian J. Egan, (Legal Adviser, U.S. Dep't of State), *International Law and Stability in Cyberspace*, 35 BERKELEY JOURNAL OF INTERNATIONAL LAW 169, 175 (2017); Paul C. Ney, Jr., General Counsel, U.S. Dep't of Defense, Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-generalcounsel-remarks-at-us-cyber-command-legal-conference/.

23. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

24. DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY: 2019 INTERNATIONAL LAW SUPPLEMENT annex A (2019), https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html [hereinafter SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE]. *See also* Ministry of the Armies, International Law Applied to Cyberspace § 1.1.1. (2019) (France), https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [hereinafter France, International Law Applied to Cyberspace].

tions represent a paradigmatic example of a matter encompassed in the *domaine réservé*. Indeed, the International Court of Justice cited "choice of political system" to illustrate the concept in its *Paramilitary Activities* judgment.[25]

The increasing regulatory reach of international law is causing a growing number of State activities to fall outside the *domaine réservé*, as exemplified by the expansion of international human rights law. Today, certain election-related activities implicate rights like the freedom of expression, the right to privacy, and the right to vote (discussed below). Thus, for example, a foreign State providing secure online communications access to individuals whose right to political expression is impeded by their State during an election would not intrude into the latter's *domaine réservé*. The operation might violate other obligations owed to the latter, but not the prohibition of intervention.

While foreign election interference will usually manifestly transgress the victim State's *domaine réservé*, application of the second element of prohibited intervention—*coercion*—is more complicated. It occupies center stage with respect to intervention, for, as the International Court of Justice explained in *Paramilitary Activities*, "the element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention."[26]

As Finland has astutely cautioned, "while the conduct of elections belongs undisputedly to the internal affairs of each State, all methods of electoral interference do not display the element of coercion."[27] Coercive cyber operations have to be distinguished from those that are merely influential or persuasive. Noting the "precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law," the Netherlands Ministry of Foreign Affairs has observed, "in essence it means compelling a State to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state."[28] The challenge is to identify the point at which permitted influence becomes prohibited coercion.

A helpful way to approach the issue is to distinguish election-related cyber activities that affect the State's *ability* to conduct an election from those that target voter *attitudes*. Foreign cyber activities that deprive a State of its ability to act vis-à-vis the *domaine réservé* are almost always coercive. They make it objectively impossible or substantially more difficult for the State to

25. *Military and Paramilitary Activities*, 1986 I.C.J. 14, ¶ 205.
26. *Id.*
27. Finland's National Positions, *supra* note 22, at 3.
28. Netherlands, International Legal Order in Cyberspace, *supra* note 22, at 3.

pursue a particular policy or activity, as when a cyber operation interferes with either a State's administration of an election or with the election infrastructure itself. The obvious example would be using cyber means to cause a miscount, which would be coercive because the State's actual choice, as reflected in the vote, is being repressed. Another State could do so by directly tampering with the vote count, disabling election machinery or causing it to malfunction, blocking e-voting, and the like.

Foreign States can also *indirectly* disrupt a State's ability to conduct an election by engaging in activities directed at voters, for example, by engineering voter suppression. Consider the use of social media to falsely report that a dangerous incident, like an active shooter situation, is ongoing near a voting location and warn people to stay out of the area. Reasonable individuals would follow those instructions and thus not cast their vote. Or a State could use social media to give improper instructions about voting in another State, such as the wrong location, or block or alter correct information as to where to vote. An example was the use of Twitter in English and Spanish during the 2016 elections to claim voters could cast their vote for Hillary Clinton through text messaging.[29] Those who followed the instructions did not actually vote, for there is no voting via text message in the United States.

Another example would be the circulation of false information online regarding how and when to request, complete, and mail-in, absentee ballots. Election returns even could be falsely reported before the polls closed, causing voters to conclude that because their preferred candidate has already effectively lost, there is no point in voting. In all of these cases, the target State's ability to make free choices through its election has been coerced, regardless of whether it can conclusively be shown that the election's outcome was altered.

Of course, a rule of reason must apply. Operations that result in only a minimal disruption of voting would not qualify as coercive. Other issues, like the timing of an operation or whether the State had an opportunity to thwart it, might also weigh in the assessment. But by and large, cyber operations intended to directly or indirectly affect a State's ability to conduct an election by targeting either its administration of the election or the voters' ability to cast a ballot are coercive.

The more complex case is that of cyber activities intended to influence the electorate's *attitudes* towards a particular candidate or issue on the ballot.

---

29. Jeff John Roberts, *Sneaky Ads on Twitter Tell Voters to Text Votes for Hillary Clinton*, FORTUNE (Nov. 3, 2016), https://fortune.com/2016/11/03/text-vote-hillary-clinton/.

Although directed at voters, these information operations are being used to influence the State. While no definitive standard exists for assessing them against the requirement of coercion, the assessment is necessarily one of degree.

Arguably, it is reasonable to characterize as coercive those cyber operations that deprive the electorate, or a substantial number of individual voters, of information bearing on the election. After all, having access to reliable information about candidates or issues would seem essential to ensuring an election is meaningful. Examples might include denial of service attacks against a campaign's social media presence or the targeting of media outlets that support a particular candidate.

A more complicated situation arises when information regarding candidates or issues is pushed to the electorate by a foreign State. Such operations raise critical questions of international law, for the greatest success in affecting elections has been achieved "by influencing the way voters think, rather than tampering with actual vote tallies."[30]

Traditional messaging setting forth a State's position on a foreign election is not coercive. This conclusion is supported by widespread State practice. Such messaging influences and persuades, not coerces. The unsettled question is whether there is some point at which a foreign State's information campaign becomes coercive. Imagine, for instance, a foreign State investing sufficient resources in support of a candidate to overwhelm the opponent's online advertising, thereby allowing the former to dominate the traditional and social media information space. As it stands, the law is not sufficiently clear about whether, and if so when, information operations can qualify as coercive.

Nevertheless, it might be possible to agree on certain non-exhaustive factors that would likely influence a foreign information operation's characterization during an election as coercive or not. The operation's "scale and effects" would appear to be highly relevant. There is precedent for looking to these factors in interpreting ill-defined thresholds. For example, the International Court of Justice has pointed to scale and effects when assessing

30. Luke Harding, *Rigged: America, Russia and 100 Years of Covert Electoral Interference by David Shimer – Review*, GUARDIAN (June 29, 2020), https://www.theguardian.com/books/2020/jun/29/rigged-america-russia-and-100-years-of-covert-electoral-interference-by-david-shimer-review.

whether a "use of force" rises to the level of an "armed attack,"[31] and States are increasingly using the same approach with regard to the threshold for a cyber use of force.[32] Scale and effects would consider factors such as how widespread the impact of the election interference is, how seriously it affects the election, and perhaps even the nature and significance of the election in question (e.g., municipal versus national).

Another factor that might bear on determining whether an information campaign is coercive is the veracity of the information in question. At first glance, it would seem challenging to make the case that the release of truthful information can ever be coercive. After all, at least in theory, the better informed the electorate, the more it can participate meaningfully.

But consider the scenario offered above where a foreign State dominates the information space. Or recall the 2016 Russian meddling, in which genuine but purloined material was released at a point in the election that did not allow the Clinton campaign time to react and recover effectively, thereby skewing voting. In that case, the fact that the truthful information was packaged in a layer of deception about the identity of those who acquired it and their affiliation with Russia complicated matters. Had American voters known that the information, even if truthful, was being disseminated by Russia as part of an influence campaign, they might have weighed it differently. Perhaps there should be a presumption that the dissemination of truthful and complete information does not violate international law, but that presumption should be rebuttable in extreme cases.

It would seem easier to describe *dis*information campaigns as coercive.[33] The range of possible scenarios is limited only by one's imagination. For instance, artificial intelligence could create fake user profiles (profile pics,

31. Interpreting "use of force" under Article 2(4) of the U.N. Charter and "armed attack" under Article 51, see Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

32. *See, e.g.,* DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY, ANNEX A, AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE 90, (2017), https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html.

33. While misinformation is false information, disinformation is false information spread with the intent to deceive. Meira Gebel, *Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online*, BUSINESS INSIDER (Jan. 15, 2021), https://www.businessinsider.in/tech/how-to/misinformation-vs-disinformation-what-to-know-about-each-form-of-false-information-and-how-to-spot-them-online/articleshow/80295200.cms.

names, etc.) in considerable numbers to create negative "buzz" about a candidate on social media. Or consider a deep fake in which a candidate purportedly admits to egregious criminal behavior. Released just before election day, when there is no time to counteract its effect, it successfully sways the election result. Similarly, take a cyber operation involving a fake website masquerading as an influential media outlet that puts out a story as the polls open claiming the candidate has admitted to criminal activity. The story goes viral, and the candidate loses.

Many other factors could play into determining whether a foreign information campaign (including disinformation) during an election is fairly considered coercive. For instance, an operation designed to achieve a specific result, such as the election of a particular candidate favored by the foreign State, is probably more likely to be characterized as coercive than one intended merely to cause general electoral disruption, for instance by using social media to disseminate disinformation about all the key candidates. Similarly, an operation that exploits specific vulnerabilities in the target State, such as ethnic or religious division, presumably would be more prone to being seen as coercive than one that is merely negative.

C. Obligation to Respect Sovereignty

Foreign activities in cyberspace can also violate the rule of sovereignty. Before discussing how, it must be cautioned that one State, the United Kingdom, has rejected the proposition that cyber operations can amount to a violation of sovereignty, relying instead on the rule of intervention to serve as the bulwark against, *inter alia*, foreign election interference.[34] However, the stance, which has been discussed in depth elsewhere,[35] has not been adopted by any other State. On the contrary, a growing number, including Finland,[36]

34. Wright, *supra* note 22.

35. *Compare* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 207 (2017) (suggesting that sovereignty is not a primary rule of international law), *with* Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace:* Lex Lata Vel Non?, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 213 (2017) (arguing that actions reaching a threshold degree of infringement on the territorial integrity of another State, as well as those which constitute an interference with or usurpation of inherently governmental functions, violate the rule of sovereignty). *See also* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEXAS LAW REVIEW 1639 (2017).

36. Finland's National Positions, *supra* note 22, at 1–3.

France,[37] the Netherlands,[38] Germany,[39] Iran,[40] the Czech Republic, Austria, and Switzerland,[41] have taken the opposite position. Seemingly, so has NATO (with the UK reserving).[42] It is the better view, for as Finland has warned,

> The argument has been raised recently that no legal consequences could be attached to sovereignty as a general principle, at least for the purposes of cyber activities. It is not only difficult to reconcile such an idea with the established status of the rule prohibiting violations of sovereignty in international law, but it also gives rise to policy concerns. Agreeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights.[43]

The analysis that follows proceeds on the basis that the requirement to respect the sovereignty of other States is a primary rule of international law.[44]

Max Huber famously set forth the classic definition of sovereignty in the 1928 *Island of Palmas* arbitration: "Sovereignty 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

---

37. France, International Law Applied to Cyberspace, Ministry of the Armies, *supra* note 24, § 1.1.1.

38. Netherlands, International Legal Order in Cyberspace, *supra* note 22, at 1–3.

39. Norbert Riedel, Commissioner for International Cyber Policy, Germany, Address at Chatham House: Cyber Security as a Dimension of Security Policy (May 18, 2015), https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

40. General Staff of the Armed Forces of the Islamic Republic of Iran, Declaration Regarding International Law Applicable to the Cyberspace (July 2020), *reprinted in* NOURNEWS (Aug. 18, 2020), https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

41. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security - Second Substantive Session, UN WEB TV (Feb. 10–14, 2020), videos of sessions available at http://webtv.un.org/.

42. UNITED KINGDOM MINISTRY OF DEFENCE, ALLIED JOINT PUBLICATION-3.20: ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS, at v (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

43. Finland's National Positions, *supra* note 22, at 3.

44. TALLINN MANUAL 2.0, *supra* note 12, rr. 1–5.

of a State."[45] This formulation contains within it both instances of how sovereignty can be violated.

First, sovereignty can be violated based on an *infringement of territorial integrity and inviolability*.[46] There is general agreement that a cyber operation causing physical damage or injury in another State qualifies as a violation of its sovereignty. Consensus also appears to have coalesced around treating a relatively permanent loss of cyberinfrastructure functionality as the requisite damage.[47] While physical damage is unlikely in the election interference context, prior to the 2020 federal election, the U.S. government warned that foreign governments might try to compromise election infrastructure (functionality) in the 2020 elections.[48] This raises the question of whether such operations would have violated U.S. sovereignty.

Unfortunately, there is no such consensus as to a loss of functionality that is temporary or that causes the affected cyberinfrastructure to operate in a manner other than intended, as in making it run slowly or generate spurious results. This is problematic because such consequences can be expected of election-related cyber operations; a real-world example is the denial of service attacks targeting Ukraine in 2014.[49] France, which has been targeted during elections,[50] has addressed hostile cyber operations generating consequences of this nature in its legal doctrine. In 2018, the Ministry of the Armies noted that it would treat "any cyberattack against French digital sys-

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

46. TALLINN MANUAL 2.0, *supra* note 12, cmt. ¶¶ 11–14 to r. 4.

47. *See, e.g.,* Open-Ended Working Group, *supra* note 41 (Czech Republic); France, International Law Applied to Cyberspace, *supra* note 24, § 1.1.1.

48. Press Release, Office of the Director of National Intelligence, Statement by NCSC Director William Evanina: Election Threat Update for the American Public (Aug. 7, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

49. In 2014, CyberBerkut, a group of Russian hacktivists, targeted the Ukrainian Central Election Commission, bringing its network down for twenty hours and nearly leading to the announcement of a false winner. Mark Clayton, *Ukraine Election Narrowly Avoided "Wanton Destruction" from Hackers*, CHRISTIAN SCIENCE MONITOR (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

50. In 2017, the GRU (Russian military intelligence) purportedly conducted operations directed at Emmanuel Macron's campaign for the French presidency. Eric Auchard, *Macron Campaign was Target of Cyber Attacks by Spy-linked Group*, REUTERS, Apr. 24, 2017, https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200.

tems or any effects produced on French territory by digital means" attributable to a State as a breach of France's sovereignty.[51] While the precise parameters of the functionality standard are indistinct, France presumably would treat a cyber operation targeting its government election hardware/software or that causes "effects" on other systems, such as a denial of service operation directed at a campaign's website, as a breach of French sovereignty. It remains to be seen whether other States will be willing to go as far in interpreting the territorial aspect of the sovereignty rule.

Second, cyber activities that *interfere with, or usurp, an "inherently governmental function"* of the target State can violate its sovereignty.[52] The issue in the election context is interference. An inherently governmental function is one that only States may perform (or authorize non-State entities to carry out); plainly, conducting elections qualifies. There is no requirement that the interference be coercive, as is the case with intervention—any interference with the State's ability to perform the function in question suffices. And unlike the violation of sovereignty based on territoriality, there is no requirement of any particular physical or functional effects. The only necessary consequence is interference itself.

It is not clear whether the rule encompasses all interference with an election. Of course, a foreign State's cyber activity that directly diminishes the government's ability to conduct the election violates that State's sovereignty on this basis.[53] Examples include temporarily disrupting election hardware and software's proper functioning, blocking access to online government information about the election, and altering that information.

It is somewhat unsettled whether cyber activities that are not directed against the government's election systems can violate sovereignty. It would seem reasonable that those that indirectly disrupt the election's smooth execution, such as voter suppression activities, would qualify.[54] For example, posting incorrect information about how, where, or when to vote reasonably could be characterized as interfering with the State's ability to conduct the election.

---

51. France, International Law Applied to Cyberspace, *supra* note 24, § 1.1.1.

52. TALLINN MANUAL 2.0, *supra* note 12, cmt. ¶¶ 15–20 to r. 4.

53. See, e.g., the Oxford Statement's reference to "Interfering, by digital or other means, with electoral processes with respect to balloting or verifying the results of an election." Oxford Statement on International Law Protections, *supra* note 9, r. 2a.

54. See, e.g., the Oxford Statement's reference to "Conducting cyber operations that adversely impact the electorate's ability to participate in electoral processes, to obtain public, accurate and timely information thereon, or that undermine public confidence in the integrity of electoral processes." *Id.* r. 2b.

The open question is whether cyber activities involving information or disinformation that does not affect how the election is carried out ever violate sovereignty. Consider, for instance, operations designed to foster societal division, as in using "dog whistles" to exploit racial fault lines.[55] If such operations are causally related to the requisite consequences (e.g., by inciting riots that cause damage or injury), a violation of the rule might be made out, but even this remains uncertain.

D. Obligation to Respect Human Rights

There is widespread consensus that human rights must be respected and protected online as they are offline.[56] Several specific rights loom large in the online election interference context—the freedom of expression; the right to privacy; the right to participate in public affairs, vote, and stand for election; and the right of all peoples to self-determination. However, the applicability of human rights to cyber election interference operations may be questioned on the ground of extraterritoriality, a much-contested issue in various other contexts. Each of these points will be addressed in turn.

Both treaty and customary international law guarantee *freedom of expression*. It is enshrined in such instruments as the International Covenant for Civil and Political Rights (ICCPR),[57] the Universal Declaration of Human Rights,[58] and regional treaties like the European Convention on Human Rights (ECHR).[59] As described in Article 19(2) of the ICCPR, it encompasses the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." States that interfere with

55. Ian Olasov, *Offensive Political Dog Whistles*, VOX (Nov. 7, 2016), https://www.vox.com/the-big-idea/2016/11/7/13549154/dog-whistles-campaign-racism.

56. *See, e.g.,* 2015 Rep. of the Group of Governmental Experts, *supra* note 21, ¶ 28; Human Rights Council Res. 20/8, U.N. Doc. A/HRC/RES/20/8 (July 16, 2012); Human Rights Council Res. 26/13, U.N. Doc. A/HRC/RES/26/13 (June 26, 2014); Human Rights Council Res. A/HRC/RES/32/13 (July 18, 2016); Human Rights Council Res. A/HRC/RES/38/7 (July 17, 2018); TALLINN MANUAL 2.0, *supra* note 12, rr. 34–38; Oxford Statement on International Law Protections, *supra* note 9, r. 2c.

57. International Covenant on Civil and Political Rights art. 19, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

58. G.A. Res. 217 (III) A, art. 19, Universal Declaration of Human Rights (Dec. 12, 1948) [hereinafter UDHR].

59. Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].

elections abroad implicate the freedom of expression when they, for instance, obstruct candidates' online campaigns (impart) or alter or erase online information about candidates that voters wish to access (seek).

Like the right to freedom of expression, the *right to privacy* is a customary right that also finds expression in treaty law.[60] It, too, can be implicated by election interference, as was well illustrated by the exfiltration and public dissemination of private email during the 2016 U.S. presidential elections.[61]

Both treaties and customary law also guarantee all citizens the right to *participate in public affairs, vote in elections, and stand for election*.[62] While international case law has historically focused on internal interference with these rights, there is no reason in principle to exclude interference by third States from their scope (on the extraterritoriality point, see below). Thus, for example, cyber operations resulting in voter suppression would directly impede enjoyment of the right to vote. As for influence operations, the UN Human Rights Committee has noted that "voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind."[63]

None of the aforementioned individual rights are absolute. States may limit their exercise or enjoyment by measures that pursue a legitimate aim, are necessary to achieve that aim, are prescribed by law, and are proportionate.[64] However, it is improbable that a foreign State's electoral interference could satisfy these requirements, if only because it would not be pursuing an aim regarded as legitimate under human rights law. It is much more likely that the victim State would act to counter foreign online election interference. If it does, any activity that impedes access to online expression, such as requiring internet service providers or social media companies to filter,

---

60. *See, e.g.,* ICCPR, *supra* note 57, art. 17; UDHR, *supra* note 58, art. 12; ECHR, *supra* note 59, art. 8.

61. *2016 Presidential Campaign Hacking Fast Facts*, CNN (Oct. 28, 2020), https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

62. *See, e.g.,* ICCPR, *supra* note 57, art. 25; UDHR, *supra* note 58, art. 21; Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms art. 3, Mar. 20, 1952, C.E.T.S. 009; American Convention on Human Rights art. 23, Nov. 22, 1969, 1144 U.N.T.S. 123.

63. Human Rights Committee, General Comment No. 25: The Right to Participate in Public Affairs, Voting and the Right of Equal Access to Public Service, ¶ 19, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (July 12, 1996).

64. Human Rights Committee, General Comment No. 34: Article 19: Freedom of Opinion and Expression, ¶ 22, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011); TALLINN MANUAL 2.0, *supra* note 12, r. 37.

delete, or label data posted or transmitted by the interfering State, must itself be justifiable under the criteria mentioned above.

It has been suggested that the human right to *self-determination*, which again is protected by both customary and treaty law,[65] might be implicated by foreign election interference.[66] Self-determination includes the right of a people to determine their own political arrangements. Those taking the position that the issue of self-determination surfaces in the context of foreign election interference do so on the basis that elections represent the sovereign will of a people concerning the nature of their governing political system and, therefore, disrupting them interferes with their exercise of self-determination.

The argument is facially plausible, but this interpretation of the right presents numerous challenges. Self-determination is a collective, not individual, right, which raises issues as to its enforcement; the right typically applies in the context of a State's emergence; there are practical difficulties in determining that the interference blocked the will of the people; and it is unclear whether the concept of a "people" in international law, which is already unsettled, can refer to the entire population of an established State or only to a sub-group. Nevertheless, this is an interesting proposition that could gain traction in the face of chronic foreign election interference by cyber means, especially when such interference is systematic and large-scale.

Whether any of these human rights apply to foreign cyber election interference depends on the contentious issue of *extraterritoriality*, that is, whether States owe human rights obligations to those in the territory of another State.[67] After all, a foreign State's election interference operations are extraterritorial by definition. Of course, in the case of specific treaty obligations, the answer is found by interpreting the instrument's jurisdictional provisions. The discussion that follows, however, takes on the issue in a general sense.

Restrictive views on the matter hold that human rights do not apply extraterritorially. The United States, for example, has long taken this position vis-à-vis the ICCPR[68] (but see a 2010 U.S. State Department Legal Adviser

65. *See, e.g.,* ICCPR, *supra* note 57, art 1; International Covenant on Economic, Social and Cultural Rights art. 1, Dec. 16, 1966, 993 U.N.T.S. 3; U.N. Charter arts. 1, 55.

66. Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEXAS LAW REVIEW 1579, 1595–98 (2017).

67. *See generally* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES (2011).

68. Human Rights Committee, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Third Periodic Report annex I, U.N. Doc. CCPR/C/USA/3 (Nov. 28, 2005).

memorandum[69]). The European Court of Human Rights adopted a somewhat less restrictive (but still restrictive) position regarding the European Convention on Human Rights in the *Bankovic* case, which involved the right to life.[70] By such restrictive approaches, even if cyber election interference theoretically implicates human rights such as the freedom of expression or the right to privacy, it would not violate the human rights of those affected because the relevant human rights rule would not apply in the first place.

The various opposing views argue that human rights law governs extraterritorial cyber operations. Under one, the negative obligation to respect human rights (i.e., to refrain from conduct) simply should be understood to apply extraterritorially. By a second, termed the "functional approach," control over the *exercise or enjoyment* of rights provides a basis for their application.[71] For instance, concerning the right to life, the Human Rights Committee has interpreted State jurisdiction under the ICCPR as reaching "all persons over whose enjoyment of the right to life [the State] exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner."[72]

The same logic could be applied to rights such as the freedom of expression or privacy that are implicated by foreign election interference, as the remotely conducted election interference may impact them as described above. Indeed, three distinguished officials have recently asserted, "the right to freedom of expression, which includes the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any

69. Legal Adviser (Harold Koh), U.S. Department of State, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010), https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf.

70. Bankovic v. Belgium, 2001-XII Eur. Ct. H.R. 333, ¶¶ 74–82. The Court held that even bombing individuals in areas outside a State's control is insufficient to create a jurisdictional link with respect to the right to life.

71. For a discussion of both views, see Marko Milanovic, *Surveillance and Cyber Operations*, *in* RESEARCH HANDBOOK ON EXTRATERRITORIAL HUMAN RIGHTS OBLIGATIONS (Mark Gibney et al. eds, forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3708440.

72. Human Rights Committee, General Comment No. 36, Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, ¶ 63, U.N. Doc. CCPR/C/GC/36 (Oct. 30, 2018).

media, applies to everyone, everywhere."[73] In this regard, as the Human Rights Committee has opined, it would seem "unconscionable" to interpret human rights law to permit a State to violate human rights on the territory of another State in a manner that it "could not perpetrate on its own territory."[74]

III. POSITIVE OBLIGATIONS

As should be clear, certain election-related cyber operations by foreign States will directly violate primary rules of international law, like sovereignty, intervention, and human rights obligations. These are *negative* obligations. That is, they prohibit States from engaging in particular conduct. However, States sometimes shoulder *positive* obligations to act in the face of hostile cyber operations. Two loom large, the obligation of due diligence under general international law and the duty to protect human rights.

A. Obligation of Due Diligence

The International Court of Justice acknowledged a so-called "due diligence" obligation of States to control activities occurring on their territories in its first case, *Corfu Channel*.[75] In its 1949 judgment, the Court observed that a State must not "allow knowingly its territory to be used for acts contrary to the rights of other states." The *Tallinn Manual 2.0* experts concluded that there was no reason to exclude the rule's application in the cyber context;[76]

---

73. David Kaye, Harlem Désir & Edison Lanza, *COVID-19: Governments Must Promote and Protect Access to and Free Flow of Information During Pandemic – International Experts*, UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (Mar. 19, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E.

74. Lopez Burgos v. Uruguay, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176, ¶ 12.3 (1981). *See also* the German Federal Constitutional Court's judgment on the extraterritoriality of the Basic Law where the Court held that fundamental rights protections apply to overseas surveillance operations, thereby making any subsequent legal policy not to extend protections to other types of transnational cyber operations difficult to reconcile with the judgment. BVerfG, 1 BvR 2835/17, ¶¶ 231–42 (May 19, 2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html;jsessionid=F1565975A319E56AE395F4B175E4F225.2_cid377.

75. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

76. TALLINN MANUAL, *supra* note 12, rr. 6–7.

a number of States have come to the same conclusion.[77] However, unable to achieve unanimity on its status as a binding rule of international law in the cyber context, the UN Group of Governmental Experts treated due diligence as (at the least) a so-called "voluntary, non-binding norm of responsible State behaviour" in its 2013 and 2015 reports.[78]

Accordingly, whether a State must, as a matter of international law, take action to stop election interference by third States or non-State actors conducted from, or by otherwise using (as in the case of hosting leaked data on a server in a third State or taking remote control of cyberinfrastructure from which to mount hostile operations), its territory remains unsettled. Even if so, the *Tallinn Manual 2.0* experts cautioned that the due diligence obligation is quite limited in reach.[79] Although the rule applies to both State and non-State actors' hostile cyber operations, the obligation only attaches when the operations are ongoing or imminent (in the sense of a material step having been taken). Additionally, they must affect an international legal right of the State concerned, cause "serious adverse consequences," and the territorial State has to know of the operations in question. In these circumstances, the territorial State will still only be in breach of the obligation if it was feasible to end the operations and it did not do so.[80] Importantly, there is no obligation to look to other States, including the victim State, for assistance, although the territorial State is free to do so.

---

77. *See, e.g.,* Kersti Kaljulaid, President of Estonia, Opening Address at CyCon 2019 (May 29, 2019), https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html; Finland's National Positions, *supra* note 22, at 4–5; France, International Law Applied to Cyberspace, *supra* note 24, § 1.1.1.; Netherlands, International Legal Order in Cyberspace, *supra* note 22, at 4–5; Open-ended Working Group, *supra* note 41 (Brazil, Korea). The Oxford Statement treats due diligence as a binding rule of international law. Oxford Statement on International Law Protections, *supra* note 9, r. 4a. *But see* Open-ended Working Group, *supra* note 41 (Argentina); Schöndorf, *supra* note 22, at 404 (Israel).

78. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013), transmitted by Letter dated 7 June 2013 from the Chair of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Established Pursuant to Resolution 66/24 (2012), ¶ 23, U.N. Doc. A/68/98 (June 24, 2013); 2015 Rep. of the Group of Governmental Experts, *supra* note 21, ¶ 13(c).

79. TALLINN MANUAL 2.0, *supra* note 12, cmt. at 30–50 to rr. 6–7.

80. The Oxford Statement appears to suggest that there is a preventive obligation. Rule 4b provides,

These limitations loom large in an election interference scenario. Most significantly, remotely conducted election interference from or through the territorial State would have to implicate a legal right of the victim State. The myriad fault lines outlined above in the relevant negative obligations would directly affect whether the due diligence rule applies in a particular situation. For instance, a State claiming a due diligence breach on the basis that the election interference implicates the rule of non-intervention would face the uncertainty surrounding the threshold for coercion.

However, there is one significant benefit of looking to the rule of due diligence in cases of election interference. In a situation in which a State cannot adequately attribute remote election interference in fact or law to the State from whose territory it is being conducted, the former may nevertheless be able to claim a breach of due diligence on the part of the latter. The territorial State's failure to stop the election interference would open the door to countermeasures (see below) that could take the form of cyber operations directed against the source of the interference.[81]

B. Obligation to Protect Human Rights

In addition to the duty to *respect* human rights, States shoulder an obligation to *protect* (secure, ensure) the human rights of individuals on their territory, a principle captured in the ICCPR[82] and other human rights instruments, like the ECHR.[83] As explained by the Human Rights Committee,

> the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts

---

> To discharge [the obligation of due diligence], states may, to the extent feasible, be required to, inter alia, investigate, prosecute or sanction those responsible, take measures to prevent or thwart operations spreading misleading or inaccurate information, and/or assist and cooperate with other states in preventing, ending, or mitigating the adverse consequences of foreign cyber operations affecting electoral processes.

Oxford Statement on International Law Protections, *supra* note 9. Although this is a worthy aspirational norm, international law has not developed to the point of requiring preventive obligations of due diligence in the cyber context.

81. For an explanation of this dynamic, see Michael N. Schmitt, *In Defense of Due Diligence*, 124 YALE LAW JOURNAL FORUM 68, 79–80 (2015).

82. ICCPR, *supra* note 57, art. 2(1).

83. ECHR, *supra* note 59, art. 1.

> committed by private persons or entities that would impair the enjoyment of Covenant rights.[84]

Thus, if harmful cyber interference by another State or a non-State actor is likely to impede, or is impeding, the exercise of protected rights related to the election, the State in which the election is taking place must take those measures at its disposal to prevent or end the interference.[85]

It must be emphasized that unlike the due diligence obligation under general international law, which only applies to ongoing or imminent activities, the human rights obligation to protect requires a State to take reasonable preventive measures in anticipation of remotely conducted election interference that would place protected rights at risk. Moreover, the protective obligation undoubtedly applies because the inability to exercise or enjoy the right in question occurs on the territory of the State conducting the election. However, it is unclear whether the protective obligation would extend to individuals located outside the State's territory, such that State A would have a *human rights* duty to protect elections in State B if A's territory was being used to mount cyber operations against B.

Like due diligence under general international law, the obligation is a duty of conduct, not of result. States need only take those actions within their capabilities in the attendant circumstances. Factors bearing on feasibility range from cost to technical wherewithal.

---

84. Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 8, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004).

85. See, e.g., Finland's confirmation that "States are bound by all their human rights obligations both online and offline. Furthermore, each State has to protect individuals within its territory and subject to its jurisdiction from interference with their rights by third parties." Finland's National Positions, *supra* note 22, at 8. The Oxford Statement provides,

> States have an obligation to protect and ensure the integrity of their own electoral processes against interference by other states. To discharge this obligation, states may be required to put in place electoral security measures, such as legislation and backup systems, as well as to secure the availability of public, timely and accurate information on electoral processes. Any restrictive measures taken by states that interfere with human rights must be in accordance with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

Oxford Statement on International Law Protections, *supra* note 9, r. 4b.

IV. RESPONSE OPTIONS

States facing remotely conducted foreign cyber election interference have a number of response options at their disposal. Internally, they may take various measures under their domestic law to protect election integrity. Such actions, which may, for example, involve the regulation of social media platforms and restrictions on speech that contains electoral disinformation, have to comply with the requirements of international human rights law mentioned above. These are regulatory questions of great complexity that will not be addressed here further.

Internationally, States may bring the matter before various dispute resolution fora, such as the International Court of Justice or the European Court of Human Rights, or before political bodies like the UN Security Council. The Council could even authorize measures under Chapter VII of the UN Charter to terminate the operations should it find the election interference to constitute a "threat to the peace."[86] However, several self-help measures are also available under international law to victim States.

The option chosen by the United States when targeted by the Russian election interference in 2016 was *retorsion*.[87] Retorsion is an act that, albeit unfriendly, does not violate international law.[88] For instance, the Obama administration imposed sanctions, expelled "diplomatic" personnel, and closed Russian facilities in response to Russia's election meddling. Because retorsion involves acts that international law does not prohibit, a State may engage in it without establishing that the underlying activities violate its international legal rights. This may be why the Obama administration elected that course of action.

If the remotely conducted election interference violates international law, the "injured State" may also take *countermeasures*.[89] The difference between retorsion and a countermeasure is that the latter is an act (action or omission) that would be unlawful but for the fact that the injured State conducts it to compel the offending State ("responsible State") to desist and/or

86. U.N. Charter art. 39.

87. David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, NEW YORK TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

88. Thomas Geigrich, *Retorsion*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (updated Sept. 2020), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983?rskey=6tWaep&result=1&prd=MPIL.

89. Articles on State Responsibility, *supra* note 10, art. 22; TALLINN MANUAL 2.0, *supra* note 12, rr. 20–25.

to secure any reparations that might be due for any harm suffered.[90] For reasons such as the risk of escalation, some nervousness surrounds the political endorsement of countermeasures' applicability in the cyber context. Nevertheless, many States have explicitly confirmed their availability in response to unlawful cyber operations.[91]

In this regard, countermeasures are typically thought of as "hack backs." For instance, an injured State may conduct cyber operations to disable the responsible State's cyberinfrastructure used to perform the election interference, an act that otherwise might amount to a breach of the responsible State's sovereignty. However, the injured State may also direct countermeasures at cyberinfrastructure other than that involved in the hostile operation;[92] indeed, the countermeasure need not even be cyber in nature, so long as it is designed to put an end to the unlawful cyber activity affecting the election or to secure reparations for harm suffered.[93]

It must be emphasized that countermeasures are subject to multiple conditions and limitations, such as a requirement of proportionality.[94] Perhaps most significantly, they are only available in response to election interference that violates international law (including a failure to exercise due diligence). If either the element of attribution or breach is missing, a response cannot qualify as a countermeasure. The victim State, therefore, would be limited to responding with acts of retorsion.

Finally, a State facing a "grave and imminent peril" to one of its "essential interests," irrespective of the source and regardless of whether the peril is the result of an international law violation, may take otherwise unlawful action to put an end to the threat so long as the measures it takes are the only means of doing so and do not affect the essential interests of any other

90. Articles on State Responsibility, *supra* note 10, art. 49.

91. *See, e.g.,* SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE annex A, *supra* note 24; Kaljulaid, *supra* note 77 (Estonia); France, International Law Applied to Cyberspace, *supra* note 24, § 1.1; Schöndorf, *supra* note 22, at 405 (Israel); Netherlands, International Legal Order in Cyberspace, *supra* note 22, at 7–8; Wright, *supra* note 22 (UK); U.S. Department of State, October 2014 U.S. Submission to GGE, Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, §A(3), at 13, https://2009-2017.state.gov/documents/organization/244486.pdf.

92. TALLINN MANUAL 2.0, *supra* note 12, cmt. ¶ 6 to r. 20.

93. *Id.* cmt. ¶ 1 to r. 21.

94. *Id.* r. 23.

State.[95] This so-called "*plea of necessity*" is a measure limited to exceptional circumstances.[96]

The conduct of elections is undoubtedly an essential interest in a democracy. Therefore, the determinative question concerning a particular instance of election interference will usually be whether the consequences are severe enough to merit characterization as "grave." Unfortunately, international law provides no bright-line threshold for the requisite gravity. But if the peril is grave, an otherwise unlawful cyber response to the election interference is permissible as long as it is the only viable option to terminate the interference.

V. CONCLUDING THOUGHTS

It's complicated. Some foreign election-related activities are obviously unlawful, as when State organs conduct cyber operations that affect the target State's ability to carry out the election. Beyond the few unequivocally wrongful cases, multiple fault lines in the international law governing cyber activities could hinder definitive characterization of particular election interference as unlawful. These range from questions of fact and evidence to unsettled issues surrounding the existence and interpretation of international law's primary rules. Such problems bleed over into the availability of response options. The reality of this "fog of law" demands continued action by States to clarify the rules.[97] Until that occurs, States will struggle to determine how to characterize election interference and respond effectively to it.

95. Articles on State Responsibility, *supra* note 10, art. 25.

96. TALLINN MANUAL 2.0, *supra* note 12, r. 26.

97. *See, e.g.,* Duncan Hollis (Rapporteur), *Improving Transparency: International Law and State Cyber Operations—Fifth Report*, OEA/Ser.Q, CJI/doc. 615/20 rev.1 (Aug. 7, 2020), http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf.