Foreign Electoral Interference: Determining State Responsibility Under International Law in the Context of Emerging Modern Forms of Electoral Interference Conducted in Cyberspace

Jason L. Sy[★]

★ '20 J.D., *with honors*, Ateneo de Manila University School of Law. The Author was a member of the Board of Editors of the *Ateneo Law Journal*. He joined the Board of Editors of the *Journal* for its 61st Volume and served as an Associate Lead Editor for the third Issue of the same Volume. He also served as the Lead Editor for the *Journal*'s April 2019 Special Issue entitled *Claudio Teehankee: A Pillar of the Rule of Law*. The Author was a member of the Executive Committee of the *Journal*'s 63d Volume. He was the Lead Editor of the fourth Edition of the ATENEO LAW JOURNAL LEGAL CITATION GUIDE released in 2020. The Author's previous works include *Social Justice: Strengthening the Heart of the 1987 Constitution for Those at the Margins of Philippine Society*, 64 ATENEO L.J. 1412 (2020) with Dean Sedfrey M. Candelaria; *Achieving Climate Justice Through Tort Law: Issues and Challenges*, 63 ATENEO L.J. 1042 (2019) with Dean Antonio G.M. La Viña; *Discovery of Trade Secrets: A Procedural Quagmire*, 62 ATENEO L.J. 1218 (2018) with Jayme A. Sy, Jr.; & *Gone Without a Trace: A Re-Examination of Bank Secrecy Laws and Anti-Money Laundering Laws in Light of the 2016 Bangladesh Bank Heist*, 62 ATENEO L.J. 90 (2017) with Dean Jose Maria G. Hofileña.

This Note is a revised and abridged version of the Author's Juris Doctor thesis (on file with the Professional Schools Library, Ateneo de Manila University).

Cite as 66 ATENEO L.J. 1012 (2022).

I. INTRODUCTION

Foreign electoral interference is a "time-honored way" of a State to bend another State's domestic and foreign policy to its will and, seemingly, such interference elicits "far more condemnation than war" possibly because "the rights of democratic participation have primacy over all other rights[,] or because most often electoral subversion takes place covertly."[1]

The year 2016 saw the proliferation of emerging forms of electoral interference in cyberspace. In a declassified report published by the United States (U.S.) Office of the Director of National Intelligence, Russian

1. Cécile Fabre, *The Case for Foreign Electoral Subversion*, 32 ETHICS & INT'L AFF. 283, 283 (2018).

interference in the U.S. elections was characterized as follows — "We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election, the consistent goals of which were to undermine public faith in the U.S. democratic process, denigrate Secretary [Hillary Diane Rodham] Clinton, and harm her electability and potential presidency."[2] The assessment goes on to project that "Moscow will apply lessons learned from its Putin-ordered campaign aimed at the U.S. presidential election to future influence efforts worldwide, including against U.S. allies and their election processes."[3] As investigations unfolded, it was evident that groups with Russian ties were found to have meddled in the 2016 U.S. presidential elections with their "attempt to influence the elections [which] challenged the effectiveness of international law and norms."[4] Similarly, in the Philippine election that same year, there were reports of Russian interference, particularly in social media.[5]

Although the possibility of States interfering with democratic processes of another State is nothing new,[6] the various aspects surrounding cyber-electoral

2. United States Office of the Director of National Intelligence, National Intelligence Council, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution, at 1, *available at* https://www.dni.gov/files/documents/ICA_2017_01.pdf (last accessed Jan. 30, 2022) [https://perma.cc/QZ6R-M9TJ].

3. *Id.* at ii (emphasis omitted).

4. David P. Fidler, *The U.S. Election Hacks, Cybersecurity, and International Law*, 110 AM. J. INT'L L. UNBOUND 337, 338 (2016). *See generally New Cambridge Analytica Leak Exposes Global Election Manipulation*, RAPPLER, Jan. 5, 2020, *available at* https://www.rappler.com/technology/news/248533-new-cambridge-analytica-leak-exposes-global-election-manipulation (last accessed Jan. 30, 2022) [https://perma.cc/8GW8-QRNB]; THE GREAT HACK (The Othrs 2019); CHRISTOPHER WYLIE, MINDF*CK: CAMBRIDGE ANALYTICA AND THE PLOT TO BREAK AMERICA (2019); & BRITTANY KAISER, TARGETED: THE CAMBRIDGE ANALYTICA WHISTLEBLOWER'S INSIDE STORY OF HOW BIG DATA, TRUMP, AND FACEBOOK BROKE DEMOCRACY AND HOW IT CAN HAPPEN AGAIN (2019).

5. Natashya Gutierrez, *Bots, Assange, An Alliance: Has Russian Propaganda Infiltrated the Philippines?*, RAPPLER, Feb. 26, 2018, *available at* https://www.rappler.com/newsbreak/in-depth/196576-russia-propaganda-influence-interference-philippines (last accessed Jan. 30, 2022) [https://perma.cc/3PNK-HXFP].

6. Ann M. Simmons, *Russia's Meddling in Other Nations' Elections Is Nothing New. Just Ask the Europeans*, L.A. TIMES, Mar. 30, 2017, *available at* https://www.latimes.com/world/europe/la-fg-russia-election-meddling-

interference, including the status and character thereof, seem to be unclear with respect to their place in international law. As elections are "at the heart of democracy[,]"[7] States are certainly interested in vigorously defending and safeguarding this hallmark of democracy.

Current discussions and debates surrounding electoral interference — especially in the context of the recent rise of modern forms of electoral interference conducted via cyberspace — have been unable to clearly resolve and settle issues such as state responsibility for cyber-electoral interference. Given this lack of consensus, this Note primarily tackles the question of whether foreign cyber-electoral interference constitutes a violation of international law, particularly under the United Nations (UN) Charter and customary international law. This Note likewise seeks to determine whether the current principles and rules under international law may squarely and adequately address these modern forms of electoral interference conducted through cyberspace, and, if the answer to such query is in the negative, whether these principles and rules may be recast and reappropriated, and whether new principles and rules in international law should necessarily be adopted to address the gaps.

A. Scope and Limitations

This Note primarily focuses on pertinent legal literature and concepts that apply to cyber-electoral interference, particularly with regard to the framework for state responsibility under international law. At the outset, this Note has a specified scope and certain limitations.

The focus is on state responsibility between and among States, i.e., State-to-State violations, flowing from cyber-electoral interference.

First, this Note focuses on electoral interference conducted through the medium of cyberspace. This Note is mindful that electoral interference may be conducted through other modes; nevertheless, this study seeks to investigate electoral interference conducted in cyberspace given its emergence and proliferation in recent years as well as the novel challenges it poses.

20170330-story.html (last accessed Jan. 30, 2022) [https://perma.cc/FNK6-3MFK].

7. The Kofi Annan Commission on Elections and Democracy in the Digital Age, About the Commission, *available at* https://www.kofiannanfoundation.org/our-work/kofi-annan-commission (last accessed Jan. 30, 2022) [https://perma.cc/8PCB-KU.S.J].

Second, this Note delves into the topic of state responsibility between and among States, i.e., State-to-State violations, flowing from cyber-electoral interference viewed as an emerging phenomenon. While this Note acknowledges that cyber-electoral interference may possibly implicate and violate human rights, i.e., State-to-individual violations, such will not be discussed in this Note which rather seeks to answer the initial question as regards what the possible breaches are by States — with respect to their obligations owed to other States under international law following acts of cyber-electoral interference. Moreover, in view of practical considerations, this Note intends to conduct an in-depth study on the State-to-State level to lay the foundation and pave the way for a possible future study which may be undertaken to explore human rights violations and other concomitant legal ramifications brought about by cyber-electoral interference.

Third, in relation to the previous point, this Note tackles international law, not domestic law. The main question that this Note seeks to answer is whether cyber-electoral interference is a violation of international law and, if in the affirmative, what obligations under international law are violated by such act. Thus, the domestic legal framework as well as the measures adopted by respective States with respect to cyber-electoral interference will be beyond the scope of this Note.

Lastly, this Note mainly focuses on States and conduct attributed to States using the modes of attribution set forth in the International Law Commission's 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)[8] which reflects customary international law. Thus, it will necessarily leave out acts of private persons, groups, or corporations in themselves whose conduct cannot be attributed to the State but nevertheless conduct cyber-electoral interference. Conducts of persons or groups which are funded by private sectors, advocacy groups, or candidates to interfere in elections are likewise excluded. An entirely separate study — that will unavoidably require a different set of legal bases from what this Note utilizes — may prove to be instructive in analyzing these private entities and their potential liability under both domestic and international law.

8. Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, annex, U.N. Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter ARSIWA].

B. Significance of the Study

1. While Emerging Forms of Electoral Interference Conducted in Cyberspace Has Gained Much Attention in Recent Years, Its Status Under International Law Remains Unclear.

This Note hopefully aims to shed light on the recent proliferation of cyber-electoral interference. There is an urgent necessity to protect States from cyber-electoral interference as it undermines their electoral processes and diminishes the public's confidence in these processes. The results of this Note may prove to be helpful for leaders and policy makers in the international law plane as they shape and influence ongoing debates as to how cyber-electoral interference should be effectively understood and addressed in the age of the Internet, especially in light of the proliferation and heightened use of social media in recent years — which in no small way is true for the Philippines, dubbed as the "social media capital of the world."[9]

2. The Philippine's Domestic Legal Framework Advocates for Free and Credible Elections and Prohibits Foreign Electoral Interference.

Pursuant to the 1987 Philippine Constitution, "[t]he Philippines renounces war as an instrument of national policy, adopts the generally accepted principles of international law as part of the law of the land[,] [ ] adheres to the policy of peace, equality, justice, freedom, cooperation, and amity with all nations"[10] and "pursue[s] an independent foreign policy."[11]

Moreover, as provided under the Philippine Constitution, the State, through the Commission on Elections (COMELEC), must ensure that the elections are "free, orderly, honest, peaceful, and credible."[12] The Congress

9. Janvic Mateo, *Philippines Still World's Social Media Capital – Study*, PHIL. STAR, Feb. 3, 2018, *available at* philstar.com/headlines/2018/02/03/1784052/philippines-still-worlds-social-media-capital-study (last accessed Jan. 30, 2022) [https://perma.cc/RZE9-TB7J].

10. PHIL. CONST. art. II, § 2.

11. PHIL. CONST. art. II, § 7.

12. *See* PHIL. CONST. art. IX-C, §§ 2 (4) & 4; art. II, §§ 2, 7, 11, & 26; & art. V, § 2. For instance, Sections 2 and 4 of Article IX-C provide, to wit —

> SECTION 2. The Commission on Elections shall exercise the following powers and functions:
>
> ...
>
> (4) Deputize, with the concurrence of the President, law enforcement agencies and instrumentalities of the Government, including the Armed

of the Philippines is likewise mandated to pass legislation in the pursuit of such goal.[13] In addition, the Constitution mandates the COMELEC to refuse registration of organizations, political parties, or coalitions who are "supported by any foreign government."[14] Receiving "[f]inancial contributions from foreign governments and their agencies" is also a ground for canceling the registration of political parties, organizations, coalitions, or candidates that benefitted from those contributions.[15] The power to cancel such registration is bestowed upon the COMELEC, as provided under the Constitution.[16] Moreover, in accordance with Section 81 of the Omnibus Election Code, one of the many election-related laws in the Philippines, any intervention by foreigners in any Philippine election is illegal, as follows —

> SECTION 81. Intervention of foreigners. — It shall be unlawful for any foreigner, whether judicial or natural person, to aid any candidate or political party, directly or indirectly, or take part in or influence in any manner any election, or to contribute or make any expenditure in connection with any election campaign or partisan political activity.[17]

This aforesaid provision appears to be a catch-all provision for any and all forms of foreign intervention. Section 96 of the same Code likewise makes it "unlawful for any person, including a political party or public or private

---

> Forces of the Philippines, for the exclusive purpose of *ensuring free, orderly, honest, peaceful, and credible elections*.
>
> SECTION 4. The Commission may, during the election period, supervise or regulate the enjoyment or utilization of all franchises or permits for the operation of transportation and other public utilities, media of communication or information, all grants, special privileges, or concessions granted by the Government or any subdivision, agency, or instrumentality thereof, including any government-owned or controlled corporation or its subsidiary. Such supervision or regulation shall aim to ensure equal opportunity, time, and space, and the right to reply, including reasonable, equal rates therefor, for public information campaigns and forums among candidates in connection with the objective of *holding free, orderly, honest, peaceful, and credible elections*.

PHIL. CONST. art. IX-C, §§ 2 (4) & 4 (emphases supplied).

13. PHIL. CONST. art. V, § 2.

14. PHIL. CONST. art. IX-C, § 2 (5).

15. PHIL. CONST. art. IX-C, § 2 (5).

16. PHIL. CONST. art. IX-C, § 2 (5).

17. Omnibus Election Code of the Philippines [OMN. ELECTION CODE], Batas Pambansa Blg. 881, § 81 (1985).

entity to solicit or receive, directly or indirectly, any aid or contribution of whatever form or nature from any foreign national, government[,] or entity for the purposes of influencing the results of the election."[18] Despite this domestic legislation in place, "[n]o one in the Philippines has ever been punished for the crime of foreign intervention. It was made illegal to prevent a repeat of the 1953 election when Edward Lansdale, a [U.S. Central Intelligence Agency] operative, meddled and helped elect Ramon Magsaysay."[19]

In addition to the Philippine Constitution and the country's laws, electoral interference infringes on various rights of Filipinos as guaranteed by various international instruments the Philippines is a signatory to.[20]

Overall, the Philippine domestic legal framework evinces the existence of the state policy that intervention of foreigners — including foreign citizens, foreign corporations, and no less foreign States — runs counter to conducting "free, orderly, honest, peaceful, and credible elections"[21] and it is in the best interest of the Philippines to guard its democratic processes from foreign intervention, especially one mounted by the awesome machinery of another State.

C. Organization of the Study

This Note consists of seven Parts. This Part I presented a brief background of electoral interference and the statement of the problem in relation to the topic, along with the scope, limitations, and significance of this Note.

Part II shall provide a historical and conceptual background of foreign electoral interference. Emerging modern typologies of foreign cyber-electoral

18. *Id.* § 96.

19. Raissa Robles, *Could Cambridge Analytica Boss Alexander Nix Be Probed for Meddling in Philippine Election?*, S. CHINA MORNING POST, Apr. 7, 2018, *available at* https://www.scmp.com/news/asia/southeast-asia/article/2140702/could-cambridge-analytica-boss-alexander-nix-be-probed (last accessed Jan. 30, 2022) [https://perma.cc/Q86J-H3J9].

20. *See, e.g.*, International Covenant on Civil and Political Rights arts. 1, 17, 19, 20, & 25, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976); International Covenant on Economic, Social and Cultural Rights art. 1, *opened for signature* Dec. 19, 1966, 993 U.N.T.S. 3 (entered into force Jan. 3, 1976); Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217 (III) (Dec. 10, 1948); & PHIL. CONST. art. IX-C, §§ 2 & 4; art. II, §§ 2, 7, 11, & 26; & art. V, § 2.

21. PHIL. CONST. art. IX-C, §§ 2 (4) & 4.

interference will be introduced and tackled as there is a necessity to delineate and nuance the discussion for succeeding parts of the Note. Cyber-electoral interference will then be differentiated from cyber-attacks, in general, to highlight the distinctive effects of attacks targeting elections as opposed to conventional attacks understood in the kinetic sense. Finally, a comparison between foreign electoral interference and espionage will be made, as a matter of clarification, as this study will focus on the former, not the latter.

Part III shall examine how acts of electoral interference can meet one of the two elements of an internationally wrongful act, namely, breach. The other element is attribution which will be tackled in the following Part. Part III will also deal with what specific obligations under international law may potentially be breached by cyber-electoral interference in connection with the four typologies identified in the previous Part.

Part IV shall discuss the modes of attribution under the Articles of State Responsibility, where the discussion will be based on the type of actors involved, in addition to the conduct that a State has acknowledged and adopted. Subsequently, problems concerning the attribution of conduct in cyberspace will be scrutinized.

Part V discusses the consequences following the existence of an internationally wrongful act stemming from an act of foreign electoral interference. The remedies on the part of the victim State will likewise be discussed.

Part VI conducts a synthesis and assessment of the gaps encountered in the previous discussions, while Part VII provides for the Author's recommendations upon the setting of parameters based on the foregoing analysis. This last Part ends the study with a set of conclusions in relation to combatting the threat posed by emerging modern forms of foreign cyber-electoral interference.

II. FOREIGN ELECTORAL INTERFERENCE

A. History

Foreign electoral interference is nothing new, at least in terms of the primary goal which is to sway the outcome of elections.[22] As early as 1796, France reportedly interfered in the U.S. elections.[23] As the electoral process is part

22. Paul Baines & Nigel Jones, *Influence and Interference in Foreign Elections*, 163 RU.S.I J. 12, 13 (2018).

23. *Id.*

and parcel of how a nation governs itself, elections have been used and exploited by States as an avenue to further assert their interests in the "command-and-control system" of the target State — elections representing a significant part of such system.[24] In modern times, "the shift has moved from physical coercion to coercive influence, including through disinformation and 'hybrid' campaigns, where deniable military assets are used to achieve a political objective." [25] Recently, numerous reports of cyber-electoral interference which involve "exploit[ing] social media and remotely conducting active intrusions into [a State's] cyber infrastructure marked a significant escalation in election meddling."[26]

B. Nature & Character

There remains no universal nor established definition of "electoral interference" under international law. In the context of foreign interference, interference "denotes activities that disturb the territorial State's ability to perform the functions as it wishes."[27] As a tautological definition, electoral interference is interference in elections — with the words "interference" and "elections" being defined separately in common and widely-used lexicons.[28] Thus, electoral interference may be defined as "the act of meddling"[29] in "the formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting"[30] in order to "disturb the territorial State's ability to perform the [said formal process] as it wishes."[31] This Note seeks to assess foreign electoral interference which, in the words of former

24. *Id.*

25. *Id.*

26. Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 32 (2018) (citing Andy Greenberg, *Everything We Know About Russia's Election-Hacking Playbook*, WIRED, June 9, 2017, *available at* https://www.wired.com/story/russia-election-hacking-playbook (last accessed Jan. 30, 2022) [https://perma.cc/UU3W-NUGV]).

27. Schmitt, *supra* note 26, at 45.

28. Interference is loosely defined as "[t]he act of meddling in another's affairs[,]" while an election is "the formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting." BLACK'S LAW DICTIONARY 937 (10th ed. 2014) & Encyclopædia Britannica, Election, *available at* https://www.britannica.com/topic/election-political-science (last accessed Jan. 30, 2022) [https://perma.cc/2SQE-TWUX].

29. BLACK'S LAW DICTIONARY 937.

30. Encyclopædia Britannica, *supra* note 28.

31. *See* Schmitt, *supra* note 26, at 45.

Australian Prime Minister B. Malcolm Turnbull, is "unacceptable interference" flowing from "activities that are in any way *covert*, *coercive*[,] *or corrupt*."[32]

As currently observed, "[i]f there is a single lesson from cyber activity over the last decade, it is that [S]tates must have a common lexicon in order to respond to cyber threats. It is not enough to simply speak of 'hacking the vote.'" [33] With scholars devising an established and widely-accepted framework in the future, this emerging area of international law may hopefully be further developed.[34]

One study suggests that foreign electoral interference "represents a significant threat to democracies such as the [U.S.]" and that the electoral intervention of foreign powers "can polarize the electorate and diminish faith in democratic institutions without provoking the kind of public demand for retaliation prompted by conventional military attacks."[35]

Indeed, the body of academic literature tackling electoral interference usually tends to discuss electoral interference without giving such term any strict and technical definition. For purposes of discussion in this Note, "cyber-electoral interference" shall mean an act or a series of acts that falls under any of the four typologies described in the next Section.

C. The Emergence of Cyber-Electoral Interference

1. The Move Toward Automated Election Systems Worldwide

A study conducted in 2018 reported that 32 countries are utilizing automated election systems, including developed democratic countries such as the U.S., Switzerland, Canada, and Australia.[36] Other countries include Mexico, Peru,

32. Fergus Hanson & Elise Thomas, Cyber-Enabled Election Interference Occurs in One-Fifth of Democracies, *available at* https://www.aspistrategist.org.au/cyber-enabled-election-interference-occurs-in-one-fifth-of-democracies (last accessed Jan. 30, 2022) [https://perma.cc/MJ4L-WHFV] (citing Commonwealth, *Parliamentary Debates*, House of Representatives, Dec. 7, 2017, 13146 (Malcolm Turnbull, Prime Minister) (Austl.)) (emphasis supplied).

33. LAURA GALANTE & SHAUN EE, DEFINING RUSSIAN ELECTION INTERFERENCE: AN ANALYSIS OF SELECT 2014 TO 2018 CYBER ENABLED INCIDENTS 5 (2018).

34. *See id.*

35. Michael Tomz & Jessica L. P. Weeks, *Public Opinion and Foreign Electoral Intervention*, 114 AM. POL. SCI. REV. 856, 871-72 (2020).

36. Brazilian Superior Electoral Court, Electronic Voting Is Already a Reality in More Than 30 Countries, *available at* english.tse.jus.br/noticias-tse-

Japan, South Korea, Brazil, and India — the last being the largest democratic nation in the world by the number of voters, estimated to be more than 800 million.[37] In the Philippines, the move towards automation of election systems was initiated through the passage of Republic Act No. 9369, better known as the Automated Election Systems Law, which amended Philippine election laws to provide for an automated system to "ensure the secrecy and sanctity of the ballot and all election, consolidation[,] and transmission documents in order that the process shall be transparent and credible and that the results shall be fast, accurate[,] and reflective of the genuine will of the people."[38] Following the passage of that law, automated elections were conducted nationwide in the Philippines in 2010, 2013, 2016, and 2019.[39]

In recent years, the number of countries adopting electronic election infrastructure is evidently on the rise.[40] Research also indicated that transitioning and utilizing electronic voting systems — systems that provide for more accessibility and convenience during elections — increase voter participation.[41] Thus, given the trend toward the adoption of electronic systems in various jurisdictions, there is an urgent necessity to safeguard them.

---

en/2018/Marco/electronic-voting-is-already-a-reality-in-more-than-30-countries (last accessed Jan. 30, 2022) [https://perma.cc/H7SP-BGVK].

37. *Id.*

38. An Act Amending Republic Act No. 8436, Entitled "An Act Authorizing the Commission on Elections to Use an Automated Election System in the May 11, 1998 National or Local Elections and in Subsequent National and Local Electoral Exercises, to Encourage Transparency, Credibility, Fairness and Accuracy of Elections, Amending for the Purpose Batas Pambansa Blg. 881, as Amended, Republic Act No. 7166 and Other Related Election Laws, Providing Funds Therefor and for Other Purposes", Republic Act No. 9369, § 1 (2007) (also known as the Automated Election Systems Law).

39. Artemio V. Panganiban, *Father of Automated Elections*, PHIL. DAILY INQ., May 26, 2019, *available at* https://opinion.inquirer.net/121582/father-of-automated-elections (last accessed Jan. 30, 2022) [https://perma.cc/AZQ6-H35T].

40. High Level Conference on the Future of International Election Observation, Challenges and Opportunities of Election Observation: ICT (Background Paper), at 1, *available at* https://eeas.europa.eu/sites/eeas/files/final_en_background_paper_ict.pdf (last accessed Jan. 30, 2022) [https://perma.cc/7DVD-8668].

41. *See* Mike Burmester & Emmanouil Magkos, *Towards Secure and Practical e-Elections in the New Era*, *in* SECURE ELECTRONIC VOTING 66 (Dimitris A. Gritzalis ed., 2003); Wolfgang Drechsler & Ülle Madise, *Electronic Voting in Estonia*, *in* ELECTRONIC VOTING AND DEMOCRACY: A COMPARATIVE ANALYSIS 98-104 (Norbert Kersting & Harald Baldersheim eds., 2004); Richard T. Carback, et al.,

In one study conducted by the Australian Strategic Policy Institute based on 97 elections and 31 referendums between November 2016 to April 2019, foreign electoral interference occurred in 20 countries within that time frame: "Australia, Brazil, Colombia, the Czech Republic, Finland, France, Germany, Indonesia, Israel, Italy, Malta, Montenegro, the Netherlands, North Macedonia, Norway, Singapore, Spain, Taiwan, Ukraine and the U.S.."[42] Moreover, covert foreign cyber-electoral interference has been said to occur in about one for every five democratic nations.[43] In another report published in 2019, the proportion of nationwide elections among democracies worldwide targeted by cyber-electoral interference "has more than doubled since 2015."[44]

2. Four Proposed Typologies of Cyber-Electoral Interference

With foreign electoral interference moving from the physical space to cyberspace and increasing rampantly, scholarship squarely tackling the links between these new modes of electoral interference conducted in cyberspace and voting behavior "is in its infancy."[45] There remains no settled categorization of these modern forms of electoral interference conducted in cyberspace. Several reputable sources have proposed typologies, primarily based on how States have attempted to influence elections in recent years.[46]

The Scantegrity Voting System and Its Use in the Takoma Park Elections, *in* REAL-WORLD ELECTRONIC VOTING: DESIGN, ANALYSIS AND DEPLOYMENT 272-75 (Feng Hao & Peter Y. A. Ryan eds., 2017); & Stanford University Computer Science Department, Electronic Voting, *available at* https://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0001.html (last accessed Jan. 30, 2022) [https://perma.cc/Z2H7-TGBX].

42. FERGUS HANSON, ET AL., HACKING DEMOCRACIES: CATALOGUING CYBER-ENABLED ATTACKS ON ELECTIONS (AUSTRALIAN STRATEGIC POLICY INSTITUTE POLICY BRIEF REPORT NO. 16/2019) 8 (2019).

43. Hanson & Thomas, *supra* note 32.

44. Communications Security Establishment, 2019 Update: Cyber Threats to Canada's Democratic Process, at 16, *available at* https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf (last accessed Jan. 30, 2022) [https://perma.cc/7WCW-SU22].

45. Isabella Hansen & Darren J. Lim, *Doxing Democracy: Influencing Elections via Cyber Voter Interference*, 25 CONTEMP. POL. 150, 151 (2018).

46. CHRIS TENOVE, ET AL., DIGITAL THREATS TO DEMOCRATIC ELECTIONS: HOW FOREIGN ACTORS USE DIGITAL TECHNIQUES TO UNDERMINE DEMOCRACY 12 (2018) (proposing four kinds: "cyber[-]attacks on systems and databases, misinformation campaigns, micro-targeted manipulation, and trolling"); DANIEL

These classifications are what scholars proposed to provide a better understanding of emerging forms of electoral interference in cyberspace. Drawing from these various typologies, the Author has analyzed these scholarly works, noting overlaps between the different proposed typologies, and has deemed the following four typologies discussed in the next Section — with the nomenclature based on the various academic works analyzed — as an optimal categorization of electoral interference conducted in cyberspace, with the purpose of this Note as the paramount consideration, i.e., to primarily

---

FRIED & ALINA POLYAKOVA, DEMOCRATIC DEFENSE AGAINST DISINFORMATION 3–4 (2018) (proposing three kinds: overt foreign propaganda, social media infiltration, cyber hacking); Luke McNamara, Framing the Problem: Cyber Threats and Elections, *available at* https://www.fireeye.com/blog/threat-research/2019/05/framing-the-problem-cyber-threats-and-elections.html (last accessed Jan. 30, 2022) [https://perma.cc/F4F8-4AUK] (proposing four kinds: social-media enabled disinformation, cyber espionage, "hack and leak" campaigns, and attacks on critical election infrastructure); EUvsDisinfo, Methods of Foreign Electoral Interference, *available at* https://euvsdisinfo.eu/methods-of-foreign-electoral-interference (last accessed Jan. 30, 2022) [https://perma.cc/YQ4W-8JBZ] (proposing four kinds: information manipulation, cyber disruption, political grooming, and extreme intervention); Barrie Sander, *Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 CHINESE J. INT'L L. 1, 4 (2019) (proposing two kinds: cyber tampering operations and cyber influence operations); ERIK BRATTBERG & TIM MAURER, RUSSIAN ELECTION INTERFERENCE: EUROPE'S COUNTER TO FAKE NEWS AND CYBER ATTACKS 27 (2018) (proposing three kinds: information operations, cyber operations, and mixed operations); Jacqueline Van De Velde, The Law of Cyber Interference in Elections, at 17–21, *available* at https://law.yale.edu/sites/default/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf (last accessed Jan. 30, 2022) [https://perma.cc/F4DU-SPZT] (proposing four kinds: physical destruction of voting equipment, meddling with a vote count, theft of information, and information campaigns); GALANTE & EE, *supra* note 33, at 5 (proposing six kinds: infrastructure exploitation, vote manipulation, strategic publication, false-front engagement, sentiment amplification, and fabricated content); CLAIRE WARDLE & HOSSEIN DERAKHSHAN, INFORMATION DISORDER: TOWARD AN INTERDISCIPLINARY FRAMEWORK FOR RESEARCH AND POLICY MAKING 5 & 20–22 (2017) (proposing three kinds: misinformation, disinformation, and malinformation); Hansen & Lim, *supra* note 45, at 151 (proposing three kinds: doxing, disinformation, and trolling); HANSON, ET AL., *supra* note 42, at 10–16 (proposing three kinds: targeting of voting infrastructure and voter turnout, interference in the information environment around elections, and long-term erosion of public trust in public institutions). *See also* Sander, *supra* note 46, at 5 n. 12.

analyze state responsibility stemming from such acts. The analysis in subsequent Parts will be based on these four identified typologies. The examples illustrated in each typology may be based on either theoretical situations or real events, as reported in the media, including those which were discovered and thwarted before posing extensive consequences. The first two typologies relate to election infrastructure, while the last two typologies relate to the voting public or a segment thereof.[47]

a. Typology 1: Attacking Election Infrastructure[48]

Typology 1, adopted based on a mode of cyber-electoral interference proposed by Jacqueline Van De Velde and another mode advanced by Luke McNamara,[49] involves the "physical destruction of ... voter equipment" through cyberspace.[50] This typology includes remote cyber operations conducted with the principal goal of physically destroying election infrastructure, including "election management systems, voting systems, [and] election pollbooks," among others, in order to interfere in the conduct of a State's elections.[51] A hypothetical example that will squarely fall under Typology 1 is an operation conducted through cyberspace that unleashes a virus in election infrastructure systems causing the cooling mechanisms of such systems to overheat and eventually result to the system's physical components melting down — where there certainly is a manifestation of physical damage, necessitating repair or replacement of machines or their component parts.[52] While there has not been any real-world example of Typology 1 to date, this typology is nevertheless being introduced for the purpose of aiding in the analysis later on — as it will be shown that States have less intrusive means to interfere in one State's elections, as seen in the next typologies, without the

47. *See id.* at 5-14.

48. This coined terminology and definition are adopted and based on a combination of Van De Velde's proposed first mode of cyber-electoral interference (i.e., physical destruction of voting equipment) with McNamara's fourth mode (i.e., attacks on critical election infrastructure). *See* Van De Velde, *supra* note 46 & McNamara, *supra* note 46.

49. *Id.*

50. Van De Velde, *supra* note 46, at 17.

51. McNamara, *supra* note 46.

52. *See* INTERNATIONAL GROUPS OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 20 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

need for physical destruction but yielding equally damaging effects or posing even far greater consequences in a State's elections.

b. Typology 2: Manipulating Voting and Transmission Systems[53]

Typology 2, which is based on the intersection between a form of electoral interference observed by a set of authors led by Chris Tenove and another form proposed by Laura Galante and Shaun Ee,[54] involves the exploitation of electorate systems and software — without physical damage — in order to "alter[ ] vote tallies, vote input, vote transmission, or other modes of counting and transmitting the voters' true choices."[55] To emphasize the delineation of this typology from Typology 1, if an act results in the exploitation of electoral systems while, at the same time, causing physical damage to election infrastructure, then such act will fall under Typology 1, not Typology 2. In other words, Typology 2 entails an act which results in interference with the voting or transmission systems that does not result in physical damage. This typology does not include acts merely intended to convey and announce a false result or intended to question the credibility of a State's election, as distinguished from the next two typologies discussed below.[56]

An example of Typology 2 is a situation where the systems of electronic voting machines are hijacked by malicious code, thereby programming these systems to automatically record a vote in favor of a particular candidate, even if the voter actually voted for a different candidate.[57] This was speculated to have occurred during the 2016 and 2019 Philippine elections wherein Vote Counting Machines (VCMs) allegedly printed receipts not reflecting the candidates chosen by a voter, e.g., reflecting a different candidate than the one actually chosen by a voter — though there remains not much evidence pointing to malicious code or a perpetrator behind such irregularities, inasmuch that it may be due to a systemic glitch.[58]

53. This coined terminology and definition are drawn from Tenove, et al.'s first kind of cyber-electoral interference (i.e., cyber-attacks on systems and databases) and Galante & Ee's second kind of cyber-electoral interference (i.e., vote manipulation). *See* TENOVE, ET AL., *supra* note 46 & GALANTE & EE, *supra* note 33.

54. *Id.*

55. GALANTE & EE, *supra* note 33, at 5.

56. *Id.*

57. HANSON, ET AL., *supra* note 42, at 10.

58. *Comelec Slams Reports on VCM Irregularities*, SUNSTAR, May 7, 2016, *available at* https://www.sunstar.com.ph/article/73122 (last accessed Jan. 30, 2022)

Another example, albeit thwarted in its tracks, was during the 2014 Ukrainian elections, when CyberBerkut — a hacker group reportedly serving as a front for Russia's intelligence agency[59] — declared, four days before the election, that they had "destroyed the computer network [election] infrastructure" after the deletion of crucial files in Ukraine's election computers, rendering the vote-counting system inoperable but which Ukraine was able to fix in time for the elections.[60] The hacker group also covertly installed a virus on the Ukrainian election commission server which was intended to publish erroneous results showing that the presidential candidate Dmytro Yarosh won when he, in reality, garnered less than one percent of the total votes.[61] The virus was fortunately detected and neutralized about 40 minutes prior to a news broadcast going live; however, the broadcast still announced the "fake" news because such development was not relayed to it in time.[62]

[https://perma.cc/DQ96-4QDE] & Vito Barcelo, et al., *Many Machines Malfunction*, MANILA STAND., May 14, 2019, *available at* https://www.manilastandard.net/news/2019-polls-the-final-push/294699/many-machines-malfunction.html (last accessed Jan. 30, 2022) [https://perma.cc/MLN8-7BCF]. *See also* Motion to Strike Out or Expunge Protestee's Verified Answer Dated 12 August 2016 with Manifestation and Answer Ad Cautelam to the Counter-Protest, Sept. 9, 2016, at 17-37 (on file with the Presidential Electoral Tribunal), *in* Ferdinand "Bongbong" R. Marcos, Jr. v. Maria Leonor "Leni Daang Matuwid" G. Robredo, P.E.T. Case No. 005, Feb. 16, 2021, *available at* https://sc.judiciary.gov.ph/18172 (last accessed Jan. 30, 2022).

59. Scott Jasper, Russia's Ultimate Weapon Might Be Cyber, *available at* https://nationalinterest.org/blog/the-buzz/russias-ultimate-weapon-might-be-cyber-24255 (last accessed Jan. 30, 2022) [https://perma.cc/FK6J-UVKL].

60. Mark Clayton, Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers, *available at* https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers (last accessed Jan. 30, 2022) [https://perma.cc/2MZ3-NLMD].

61. Andrew E. Kramer & Andrew Higgins, *In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking*, N.Y. TIMES, Aug. 16, 2017, *available at* https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html (last accessed Jan. 30, 2022) [https://perma.cc/5Q9Z-3XGV].

62. Anna Mostovych, Russian Hacking Attempt Fails, but Fake Election News Airs, *available at* euromaidanpress.com/2014/05/26/russian-hacking-attempt-fails-but-fake-election-news-airs (last accessed Jan. 30, 2022) [https://perma.cc/38M6-ADVW].

A denial-of-service (DoS) attack[63] will fall under Typology 2. This attack occurs as a result of malicious acts, including acts that inundate a network system with traffic, performed by a person or group with the goal of preventing legitimate users from "access[ing] information systems, devices, or other network resources."[64] For instance, one week before the April 2019 Finnish election, there was a DoS attack against a web service which publishes election tallies.[65] While investigation remains ongoing, the attack was suspectedly conducted by "hackers backed by Russian intelligence."[66]

c. Typology 3: Publicizing Illicitly-Obtained Information[67]

Typology 3, a consolidation of one suggested form of cyber-electoral interference by Luke McNamara and another form advanced by Laura Galante and Shaun Ee,[68] involves the so-called "hack and release" phenomenon in which cyber operations target and exploit private or governmental systems to illicitly obtain private or classified information and thereafter disseminate such stolen information to the public or to a segment thereof with intent to "embarrass, expose, or otherwise cast the subject in a negative light."[69]

During the 2016 U.S. presidential elections, a prime illustration of this typology was the leak of the Democratic National Committee's documents, through the websites of DCLeaks.com and WikiLeaks, reportedly orchestrated by the Russian military intelligence agency Glavnoye Razvedyvatelnoye Upravlenie (GRU) operating under the guise of "Guccifer 2.0" with the goal of maligning Hillary Diane Rodham Clinton's presidential campaign.[70] This

63. *See* United States Cybersecurity & Infrastructure Security Agency, Security Tip (ST04-015): Understanding Denial-of-Service Attacks, *available at* https://www.us-cert.gov/ncas/tips/ST04-015 (last accessed Jan. 30, 2022) [https://perma.cc/W8U5-4SU8].

64. *Id.*

65. HANSON, ET AL., *supra* note 42, at 19 tbl. 5.

66. *Id.*

67. This coined terminology and definition are drawn from the name of McNamara's third kind of cyber-electoral interference (i.e., "hack and leak" campaigns) and Galante & Ee's third kind of cyber-electoral interference (i.e., strategic publication). *See* GALANTE & EE, *supra* note 33 & McNamara, *supra* note 46.

68. *Id.*

69. GALANTE & EE, *supra* note 33, at 5.

70. *Id.* at 10 (citing Eric Lipton, et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES, Dec. 13, 2016, *available at* https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-

typology was also apparent in the 2017 French elections, when nine gigabytes worth of data relating to presidential candidate Emmanuel Jean-Michel Frédéric Macron were leaked.[71] The data were obtained around October 2016 through "a 'massive, coordinated act of hacking'" using various techniques including spear-phishing emails and were released on the eve of 5 May 2017, right before the elections were to take place.[72] Security experts then pointed to Fancy Bear, a hacker group affiliated with the Russian intelligence agency GRU,[73] as the culprit behind the "hack and release" operation.[74]

d. Typology 4: Mounting Information Campaigns[75]

Typology 4, derived from the forms of electoral interference proposed by Jacqueline Van De Velde; Erik Brattberg and Tim Maurer; and, Isabella Hansen and Darren J. Lim,[76] involves the strategic use of the Internet to inject information — whether true, partly true, or false — through various websites including, most especially, social media platforms where "fake news," bots, and trolls are deployed to impersonate other voters, change narratives, form echo chambers, and develop hatred and fear among the voting citizenry of a

---

dnc.html (last accessed Jan. 30, 2022) [https://perma.cc/JB24-62TZ]; Sean Gallagher, *DNC "Lone Hacker" Guccifer 2.0 Pegged as Russian Spy After Opsec Fail*, ARS TECHNICA, Mar. 24, 2018, *available at* https://arstechnica.com/tech-policy/2018/03/dnc-lone-hacker-guccifer-2-0-pegged-as-russian-spy-after-opsec-fail (last accessed Jan. 30, 2022) [https://perma.cc/3JQJ-VZH7]; & Lily Hay Newman, *Yes, Even Elite Hackers Make Dumb Mistakes*, WIRED, Mar. 25, 2018, *available at* https://www.wired.com/story/guccifer-elite-hackers-mistakes (last accessed Jan. 30, 2022) [https://perma.cc/BAB7-H9Y6]).

71. HANSON, ET AL., *supra* note 42, at 21 tbl. 6.

72. *Id.* (citing En Marche!, Communiqué de Presse - En Marche a été Victime d'une Action de Piratage Massive et Coordonnée, *available at* https://en-marche.fr/articles/communiques/communique-presse-piratage (last accessed Jan. 30, 2022) [https://perma.cc/N2Y2-Y73G]).

73. CrowdStrike, Who Is Fancy Bear (APT28)?, *available at* https://www.crowdstrike.com/blog/who-is-fancy-bear (last accessed Jan. 30, 2022) [https://perma.cc/Q5YF-RGMA].

74. HANSON, ET AL., *supra* note 42, at 21 tbl. 6.

75. This coined terminology and definition are drawn from Van De Velde's fourth kind of cyber-electoral interference (i.e., information campaigns), Brattberg and Maurer's first kind (i.e., information operations), and Hansen and Lim's second and third kinds (i.e., disinformation and trolling). *See* Van De Velde, *supra* note 46; BRATTBERG & MAURER, *supra* note 46; & Hansen & Lim, *supra* note 45.

76. *Id.*

particular State with the goal of, generally, eroding the public's trust in a State's electoral processes or, at times, specifically, to influence voters to choose a particular candidate in that State's elections or vote in a desired manner.[77] This typology includes the creation of misleading or fraudulent content based on disputed issues and its subsequent promotion through the Internet, especially through social media platforms.[78] Trolling, which is subsumed under this typology, involves the flooding of online websites, including social media platforms, with "provocative and/or lurid posts."[79]

Rampant disinformation campaigns in cyberspace were employed in the 2016 U.S. presidential elections, allegedly by Russia — using sophisticated hacking and social media manipulation techniques, among others.[80] For instance, the Internet Research Agency (IRA), another Russian company reportedly under the direction of the Russian government,[81] created social media accounts in order to impersonate Americans, spread extreme political beliefs, and even organize rallies through such accounts.[82] IRA likewise managed social medial accounts to make factually dubious claims that Hillary

77. *See* BRATTBERG & MAURER, *supra* note 46, at 26–29.

78. McNamara, *supra* note 46.

79. Hansen & Lim, *supra* note 45, at 151.

80. Timothy Summers, *How the Russian Government Used Disinformation and Cyber Warfare in 2016 Election – an Ethical Hacker Explains*, CONVERSATION, July 27, 2018, *available at* https://theconversation.com/how-the-russian-government-used-disinformation-and-cyber-warfare-in-2016-election-an-ethical-hacker-explains-99989 (last accessed Jan. 30, 2022) [https://perma.cc/2YS9-SRB6].

81. Kris Holt, *Cyber Command Put the Kibosh on Russian Trolls During the Midterms*, ENGADGET, Feb. 26, 2019, *available at* https://www.engadget.com/2019/02/26/cyber-command-russia-internet-research-agency-military-attack (last accessed Jan. 30, 2022) [https://perma.cc/ZQ4Z-JXF3].

82. GALANTE & EE, *supra* note 33, at 10 (citing Alicia Parlapiano & Jasmine C. Lee, *The Propaganda Tools Used by Russians to Influence the 2016 Election*, N.Y. TIMES, Feb. 16, 2018, *available at* https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html (last accessed Jan. 30, 2022) [https://perma.cc/FCT5-96GP]; Indictment, July 13, 2018 (on file with the United States District Court, District of Columbia), *in* United States of America v. Viktor Borisovich Netyksho, et al., No. 1:18CR00215 (D.D.C., filed July 13, 2018) (U.S.) (pending); FireEye, Complimentary Intel Report: Russia's APT28 Strategically Evolves Its Cyber Operations, *available at* https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html (last accessed Jan. 30, 2022) [https://perma.cc/J9JB-XMMH]; & CrowdStrike, *supra* note 73)).

Clinton's adviser blamed her for the Benghazi incident which claimed the lives of several Americans.[83]

Meanwhile, in 2018, China was purportedly engaged in a disinformation campaign that targeted social media platforms and chat groups with zombie accounts that the country set-up in order to undermine the Democratic Progressive Party of Taiwan headed by President Tsai Ing-Wen.[84]

D. Cyber-Electoral Interference Compared to Cyber-Attacks and Espionage

In contrast to electoral interference through physical penetration of the territory of a State or adverse presence therein which is certainly deemed an unlawful intrusion of a State's territory, it remains to be seen whether these emerging forms of electoral interference conducted in cyberspace can be treated analogously with those cases of interference conducted through physical means.[85]

As Van De Velde observes, cyber-electoral interference is different from cyber-attacks in general given: (1) the nature of the target which need not even be computers, (2) the nature of the attack which need not be always hacking as in cyber-attacks — as cyber-electoral interference may involve persuasive information campaigns, and (3) the nature of the damage which may, at times, be unquantifiable as it may go into the erosion of the public's confidence in the electoral system.[86] Moreover, "[t]he single greatest difference between cyber election interference and other cyber-attacks is the propensity of [S]tates to target civilians alongside systems. In doing so, the attack becomes difficult to identify, quantify, control, and remedy."[87]

It bears stressing that espionage is not the same as electoral interference. Electoral interference may occur with or without espionage. In any case, while the rules of espionage in times of war have been the subject of several

83. GALANTE & EE, *supra* note 33, at 10 (citing Ben Nimmo, @DFRLab, *#ElectionWatch: Beyond Russian Impact*, MEDIUM, Feb. 27, 2018, *available at* https://medium.com/dfrlab/electionwatch-beyond-russian-impact-2f5777677cc0 (last accessed Jan. 30, 2022) [https://perma.cc/VSQ7-LKC6]).

84. HANSON, ET AL., *supra* note 42, at 23 tbl. 6.

85. Schmitt, *supra* note 26, at 32.

86. Van De Velde, *supra* note 46, at 8-10.

87. *Id.* at 10. *See generally* SAMULI HAATAJA, CYBER ATTACKS AND INTERNATIONAL LAW ON THE USE OF FORCE: THE TURN TO INFORMATION ETHICS (1st ed. 2018) & Kenneth J. Biskner, *Russian Exploitation of the Cyber Gap in International Law*, ARMY WAR C. REV., Volume No. 4, Issue Nos. 1 & 2.

international agreements,[88] the academic literature surrounding espionage during peace time, i.e., "outside the laws of war[,] is much less developed."[89] Espionage, however, is beyond the scope of this Note which will focus on electoral interference.

As it stands, the permissibility of electoral interference under international law remains unsettled. Moreover, state practice and *opinio juris* as to which kinds of activities conducted in cyberspace possibly constitute violations of the norm of respecting sovereignty and the principle of non-intervention remain likewise unclear.[90] There is currently no specific set of rules under international law that directly addresses either "cyberspace in general or [ ] electoral interference[ ] in particular."[91] Thus, there is a need to review existing pertinent concepts and mechanisms which may possibly be applied or be reinterpreted to assess and analyze these emerging acts of electoral interference. The next Part will tackle the legal ramifications of cyber-electoral interference in the international plane under the auspices of the framework for state responsibility.

III. FIRST STEP IN LOCATING THE NEXUS OF STATE RESPONSIBILITY FOR CYBER-ELECTORAL INTERFERENCE: POSSIBLE BREACHES

A. ILC's Articles on Responsibility of States for Internationally Wrongful Acts of 2001: An Overview

The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts of 2001 (ARSIWA) is the principal source referred to in relation to the present-day conception of State responsibility under international law.[92] The ARSIWA was adopted by the International

88. These include the Hague Conventions of 1907, the Geneva Conventions, and the Additional Protocols to the Geneva Conventions.

89. Afsheen John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 601-07 (2007).

90. Fidler, *supra* note 4, at 341-42.

91. Anat Eisenstein Bar-on, The (il)Legality of Interference in Elections Under International Law, *available at* https://csrcl.huji.ac.il/people/illegality-interference-elections-under-international-law (last accessed Jan. 30, 2022) [https://perma.cc/FF88-VCJ7].

92. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 31 (2002) [hereinafter ARSIWA OFFICIAL COMMENTARIES] & Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in* RESEARCH HANDBOOK ON

Law Commission in 2001 and has been frequently cited by international tribunals as "it is considered to be an authoritative statement of the customary international law on state responsibility."[93]

Under the ARSIWA, a State can be held responsible if, first, such act or omission "constitute[s] a breach of an international legal obligation in force for that State at that time" and, second, such act or omission is "attributable to the State under international law."[94] The concurrence of both requisites produces what is known as an "internationally wrongful act."[95] Once an internationally wrongful act is established, state liability attaches. This Section investigates the possible breaches of cyber-electoral interference under international law.

Once the perpetrating State interferes in an election, the following, at the outset, are potential breaches stemming from a violation of rights and obligations of States under international law: (1) prohibition on the threat or use of force under the UN Charter, (2) sovereignty under customary

INTERNATIONAL LAW AND CYBERSPACE 115 (Nicholas Tsagourias & Russell Buchan eds., 2d ed. 2021).

93. Antonopoulos, *supra* note 92, at 115 (citing U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies*, 65th Session of the General Assembly, U.N. Doc. A/65/76 (Apr. 30, 2010); U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts: Comments and Information Received from Governments*, 65th Session of the General Assembly, U.N. Doc. A/65/96 (May 14, 2010); U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies*, 68th Session of the General Assembly, U.N. Doc. A/68/72 (Apr. 30, 2013); U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies*, 71st Session of the General Assembly, U.N. Doc. A/71/80 (Apr. 21, 2016); U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies*, 74th Session of the General Assembly, U.N. Doc. A/74/83 (Apr. 23, 2019); & JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 524 (9th ed. 2019)).

94. ARSIWA, *supra* note 8, art. 2 & ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 2 cmt. 1, at 81.

95. *Id.*

international law, (3) norm of non-intervention under customary international law, and (4) due diligence obligation under customary international law.[96]

B. Possible Breaches Relating to Cyber-Electoral Interference Under International Law

1. Prohibition on the Threat or Use of Force Under the UN Charter

a. Conventional Concept

The UN Charter, under Article 2, Paragraph 4, provides that "[a]ll Members shall refrain in their international relations from the *threat or use of force* against the territorial integrity or political independence of any [S]tate, or in any other manner inconsistent with the Purposes of the [UN]."[97] The prevailing view on the international plane is that force solely refers to armed force — not political or economic coercion — that may be resorted to in a direct or indirect manner, such as when a State participates in the use of force through rebels or, possibly, another State.[98] While the word "use" in the said Article is undisputedly clear, the word "threat" remains subject to some degree of uncertainty as the "threat of force" is indeed an aspect that the international community deals with daily, with state practice tolerating some of these "threats" such as weapon development — aware that these remain concomitant to self-defense, as an exception to the prohibition.[99] With regard to the phrase "against the territorial integrity or political independence of any [S]tate,"[100] some legal scholars have relied on such phraseology to introduce substantial qualifications on the use of force, nevertheless, the preparatory

96. *See* Jens David Ohlin, *Election Interference: A Unique Harm Requiring Unique Solutions*, *in* DEFENDING DEMOCRACIES: COMBATING FOREIGN ELECTION INTERFERENCE IN A DIGITAL AGE 239-62 (Duncan B. Hollis & Jens David Ohlin eds., 2021); Van De Velde, *supra* note 46; Schmitt, *supra* note 26; & Michael Schmitt & Jeffrey Biller, The NotPetya Cyber Operation as a Case Study of International Law, *available at* https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law (last accessed Jan. 30, 2022) [https://perma.cc/E7KE-LYPS].

97. U.N. CHARTER art. 2, ¶ 4 (emphasis supplied). Notably, though the word "war" was not used in the aforesaid Article, the term "force" embracing a wider conception of military action is used. Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1624 (1984).

98. CRAWFORD, *supra* note 93, at 719-20.

99. *Id.* at 720.

100. U.N. CHARTER art. 2, ¶ 4.

work leading to the adoption of the UN Charter is clear that the phrase was used specifically to protect small States and not meant to be restrictive in its effect.[101]

Article 2, Paragraph 4 is said to be "a cornerstone of the [UN] Charter" as it explicitly prohibits the "unilateral threat or use of force by [S]tates, save in certain limited circumstances."[102] This prohibition on the unilateral use of force is said to be a *jus cogens* rule — a peremptory norm from which absolutely no derogation is permitted.[103] Under the UN Charter, there are two limited circumstances which exempt a State from the ambit of Article 2, Paragraph 4, namely: (1) using force as self-defense as in Article 51 and (2) using force pursuant to a UN Security Council authorization under Article 42.[104]

Self-defense, or every State's right to defend itself, under Article 51 is the "most prominent qualification" to the use of force, viz. — "Nothing in the present [UN] Charter shall impair the inherent right of individual or collective self-defen[s]e if an armed attack occurs against a Member of the [UN], until the Security Council has taken measures necessary to maintain international peace and security."[105] Notably, this right to self-defense is not limitless as the force employed must be both necessary and proportionate — for both individual and collective self-defense.[106] In the case of *Military and Paramilitary*

---

101. CRAWFORD, *supra* note 93, at 719.

102. *Id.* (citing Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, 223 (Dec. 19)).

103. Sondre Torp Helmersen, *The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations*, 61 NETH. INT'L L. REV. 167, 173 (2014).

104. Ohlin, *supra* note 96, at 243; & U.N. CHARTER arts. 51 & 42. There are other exceptions to the prohibition on the use of force carved out by international law such as ad hoc consent and treaties including the United Nations Convention on the Law of the Sea. *See generally* Helmersen, *supra* note 103, at 176-82.

105. CRAWFORD, *supra* note 93, at 720 (citing U.N. CHARTER art. 51).

106. CRAWFORD, *supra* note 93, at 722 (citing CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 157-65 (4th ed. 2018); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14, 103 (June 27); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 245 (July 8); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, 183 (Nov. 6); & *Armed Activities on the Territory of the Congo*, 2005 I.C.J. at 223). As Crawford explains —

> necessity has generally been interpreted as meaning that the defending [S]tate must have no other option in the circumstances than to act in forceful self-defen[s]e, while proportionality requires that the size, duration, and target of the response broadly correspond to the attack in

Activities in and Against Nicaragua (Nicaragua v. United States of America),[107] the International Court of Justice (ICJ) stated that this formulation of the right of self-defense under Article 51 refers to an inherent right under existing customary international law as well as under the UN Charter itself,[108] to wit —

> Article 51 of the Charter is only meaningful on the basis that there is a 'natural' or 'inherent' right of self-defen[s]e and it is hard to see how this can be other than of a customary nature, even if its present content has been confirmed and influenced by the Charter ... It cannot, therefore, be held that [A]rticle 51 is a provision which 'subsumes and supervenes' customary international law.[109]

In that same case, however, the ICJ had ruled that the fact that the U.S. provided arms and support to irregular groups did not amount to an "armed attack by the U.S. against Nicaragua or by Nicaragua against [neighboring] [S]tates, although other illegalities (the mining of a [harbor], intervention in internal affairs) had been committed."[110] Though such assistance may be considered a threat or use of force, or unlawful intervention, such does not constitute an "armed attack" which shall trigger the application of Article 51.[111]

Article 42 of the UN Charter, alongside Articles 39 and 25, permits the UN Security Council to authorize the use of force where UN members "may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[112] The UN Security Council, under Article 39, may authorize such use of force only upon "determin[ing] the existence of any threat to the peace, breach of the peace, or act of

---

> question. Thus, self-[defense] cannot be merely punitive or retaliatory in character.
>
> CRAWFORD, *supra* note 93, at 722 (citing GRAY, *supra* note 106, at 157).

107. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14 (June 27).

108. MALCOLM N. SHAW, INTERNATIONAL LAW 1132 (6th ed. 2008) (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 176).

109. *Id.*

110. CRAWFORD, *supra* note 93, at 721 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 62 & 64).

111. CRAWFORD, *supra* note 93, at 721 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 104).

112. U.N. CHARTER art. 42 & Helmersen, *supra* note 103, at 180.

aggression[.]"[113] Where such authorization has been decided upon by the UN Security Council, such decision shall be binding to all UN members, pursuant to Article 25.[114] An enforcement action may usually involve using force against a particular State; however, the authorization can also contemplate peacekeeping operations which are conditioned upon the consent of the State where the operations will be conducted.[115]

b. Application to Cyber-Electoral Interference

As the UN Charter expressly prohibits use of force such as, indisputably, military intervention, except for the two exceptions present under the UN Charter,[116] therefore, there is a high threshold for electoral interference — much higher when conducted in cyberspace — to overcome in order for conduct to be a violation of the prohibition on the use of force.[117] Moreover, the UN Charter "conceptualizes attacks in a kinetic sense," thus, cyber-attacks resulting to physical damage can arguably reach that threshold and possible serve as an example of violating this prohibition.[118] Nevertheless, most international scholars agree that many instances of cyber-attacks do not reach such threshold.[119] Consequently, it may be said that cyber-electoral interference which do not result to physical damage may unlikely reach the high threshold as well.[120] Thus, considering the foregoing, only Typology 1 can properly be characterized as a violation of the prohibition on the use of force under the UN Charter.

2. Sovereignty Under Customary International Law

a. Conventional Concept

Sovereignty as a modern concept is said to have its origins in the Treaty of Westphalia back in 1648, though it has been suggested that modern sovereignty was established even prior to such time.[121] There are numerous

113. U.N. CHARTER art. 39 & Helmersen, *supra* note 103, at 180.

114. Helmersen, *supra* note 103, at 180 (citing U.N. CHARTER art. 25).

115. CRAWFORD, *supra* note 93, at 731.

116. Ohlin, *supra* note 96, at 243.

117. Van De Velde, *supra* note 46, at 23.

118. *Id.*

119. *Id.* at 25.

120. *Id.*

121. Samantha Besson, Sovereignty, *available at* https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-

variations of sovereignty as a concept, found in international law, such as in the UN Charter that reflects the principle of sovereign equality and the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States that details rights which flow from such principle of sovereign equality.[122] Moreover, sovereignty has likewise been said to be a *jus cogens* norm, as seemingly confirmed by the conditions set forth under Article 53 of the Vienna Convention on the Law of Treaties.[123] The concept of sovereignty was elaborated upon by the Permanent Court of Arbitration in the *Island of Palmas Case*,[124] viz. —

> 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 of a State. The development of the national organi[z]ation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations.[125]

The problem with the concept of "sovereignty" is that the term gets lost in translation and is used in various senses by lawyers, political experts, and even politicians, at times, inaccurately, so much so that the term seems "something of a cluster concept housing many different ideas within its rich but often confusing rubric."[126] In the *Military and Paramilitary Activities in and Against Nicaragua* case, the ICJ discussed the principle of sovereignty as a concept primarily linked to physical territory,[127] to wit —

9780199231690-e1472 (last accessed Jan. 30, 2022) [https://perma.cc/Y4ES-PJVF]. *See generally* Bruce P. Frohnen, *A Problem of Power: The Impact of Modern Sovereignty on the Rule of Law in Comparative and Historical Perspective*, 20 TRANSNAT'L L. & CONTEMP. PROBS. 599, 601-13 (2012).

122. Besson, *supra* note 121 (citing U.N. CHARTER art. 2, ¶ 1 & Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), annex, U.N. Doc. A/RES/2625 (XXV) (Oct. 24, 1970)).

123. Besson, *supra* note 121 (citing Vienna Convention on the Law of Treaties art. 53, *opened for signature* May 23, 1969, 1155 U.N.T.S. 331 [hereinafter VCLT] (entered into force Jan. 27, 1980)).

124. Island of Palmas Case (Neth./U.S.), Award, 2 R.I.A.A. 829 (1928).

125. *Id.* at 838.

126. Ohlin, *supra* note 96, at 251.

127. Van De Velde, *supra* note 46, at 26.

> [T]he principle of respect for State sovereignty, which in international law is of course closely linked with the principles of the prohibition of the use of force and of non-intervention. The basic legal concept of State sovereignty in customary international law, expressed in, inter alia, Article 2, [P]aragraph 1, of the [UN] Charter, extends to the internal waters and territorial sea of every State and to the air space above its territory. ... The [ICJ] has no doubt that these prescriptions of treaty-law merely respond to firmly established and longstanding tenets of customary international law.[128]

Sovereignty is directly or indirectly relied upon by "[m]ost[,] ... if not all [other] institutions and principles of international law[.]"[129] As Malcolm N. Shaw[130] observes, "[t]he principle of respect for the sovereignty of [S]tates was [a] [ ] principle closely allied to the principles of the prohibition of the use of force and of non-intervention."[131] Moreover, as another scholar explains, it appears that sovereignty is subsumed under the norm of non-intervention such that violating sovereignty amounts to violating the norm of non-intervention, though the reverse would not logically follow.[132]

b. Application to Cyber-Electoral Interference

The meaning of sovereignty is dynamic as it changes across political and historical contexts.[133] Notably, "because of its essentially contestable nature, the concept has been remarkably resilient both epistemically and normatively, and its pregnancy in contemporary legal discourse has not been undermined but rather increased by controversy."[134] Thus, it is no surprise that sovereignty can be interpreted in light of emerging phenomena such as cyber-electoral interference.

There is currently a broad consensus among international law experts that sovereignty is seen both as a principle and as a primary binding rule under

128. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 212.

129. Besson, *supra* note 121.

130. Malcolm N. Shaw, considered one of the most highly qualified publicists, has "receiv[ed] a number of citations across several cases and/or authors[.]" Michael Peil, *Scholarly Writings as a Source of Law: A Survey of the Use of Doctrine by the International Court of Justice*, 1 CAMB. J. INT'L & COMP. L. 136, 160 (2012).

131. SHAW, *supra* note 108, at 1148 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 111).

132. Van De Velde, *supra* note 46, at 32.

133. Besson, *supra* note 121.

134. *Id.*

international law.[135] This was the view "unanimously adopted by the International Group of Experts (IGE) that prepared the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" — commonly and simply called the Tallinn Manual 2.0 — which was the result of a seven-year international endeavor to assess how international law is applied in the context of cyberspace.[136] Sovereignty as a principle is an "acknowledgment that States are primarily responsible for what happens on their territory and that other States should respect said competence."[137] Thus, sovereignty as a principle serves as a basis from which different primary rules of international law have emerged, such as the rule of non-intervention of States into another State's internal affairs.[138] Meanwhile, sovereignty as a primary rule of international law means that sovereignty "is itself susceptible to violation[,]" as evident in the classic example of the territorial airspace or waters of a State being penetrated by government aircraft or ships of another State without the former State's consent.[139] Therefore, it may be possible for a single act of a State to violate the obligation to respect the sovereignty of another State and the obligation not to unlawfully use force in that latter State — as a different primary rule derived from sovereignty as a principle.[140] At present, the Tallinn Manual 2.0 supports the view that the prevailing definition of sovereignty is "qualif[ied] [to be] [ ] a norm of international law from which derogation is not permitted."[141]

Accordingly, the Tallinn Manual 2.0 provides the conditions when cyber operations conducted remotely will violate the sovereignty of a State, hinging on two different bases,[142] as follows:

> (1) the degree of infringement upon the target State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions. The first is based on the premise that a State controls access to its sovereign territory ... and the second on the sovereign right of a

135. Schmitt, *supra* note 26, at 40.

136. *Id.* at 40-41.

137. *Id.* at 40.

138. *Id.*

139. *Id.*

140. *Id.*

141. Allison Denton, *Fake News: The Legality of the Russian 2016 Facebook Influence Campaign*, 37 B.U. INT'L L.J. 183, 200 (2019). *See* Besson, *supra* note 121 (citing VCLT, *supra* note 123, art. 53).

142. Ohlin, *supra* note 96, at 243.

> State to exercise within its territory, 'to the exclusion of any other State, the functions of a State[.']143

Considering the first basis, i.e., "the degree of infringement upon the target State's territorial integrity[,]" the IGE came up with three levels to analyze whether sovereignty is violated: "(1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality."144

As for physical damage, there was a majority consensus among the drafters of the Tallinn Manual 2.0 that while physical presence on a State's territory to perform cyber operations without its consent certainly violates sovereignty, "the causation of physical consequences by remote means on that territory likewise constitutes a violation of sovereignty."145 The drafters regarded a remote cyber operation causing physical damage "either [due] to the targeted cyber infrastructure ... or objects reliant thereon, or injury to persons" as a violation of sovereignty. 146 Thus, Typology 1, i.e., attacking election infrastructure through cyberspace may fall squarely under this level. However, as Michael N. Schmitt suggests, it is highly improbable that a State will interfere in elections by inflicting physical damage to cyber-related infrastructure, "if only because lesser means would usually suffice to achieve its objective" 147 — as apparent in the next level discussed hereafter.

An illustrative example for "loss of functionality," which falls short of physical destruction under the first level, is a cyber operation infiltrating the web servers of a political party which thereafter become inoperable and necessitate a reinstallation of software, such as the operating system.148 Loss of functionality of a State's infrastructure as a result of a remotely-conducted cyber operation of another State is treated by the Tallinn Manual 2.0 as equivalent to physical damage, "consistent with the object and purpose of the principle of sovereignty, which clearly protects territorial integrity against physical violation."149 Nevertheless, analysis on this level remains ambiguous — an ominous gray area — as experts of the Tallinn Manual 2.0 could not

143. TALLINN MANUAL 2.0, *supra* note 52, at 20 (citing *Island of Palmas Case*, 2 R.I.A.A. at 838).

144. TALLINN MANUAL 2.0, *supra* note 52, at 20.

145. *Id.*

146. Schmitt, *supra* note 26, at 43 (citing TALLINN MANUAL 2.0, *supra* note 52, at 20).

147. Schmitt, *supra* note 26, at 43.

148. *Id.* & TALLINN MANUAL 2.0, *supra* note 52, at 20–21.

149. TALLINN MANUAL 2.0, *supra* note 52, at 20.

reach a consensus as to the definite meaning of "loss of functionality" because of the "the lack of expressions of *opinio juris*" in relation thereto.[150]

Even murkier waters lie ahead as one treads through the third level which encompasses cyber operations that have effects falling neither under "physical damage" nor "loss of functionality" such that there remains a looming uncertainty when assessing interference conducted through cyberspace in an election of a particular State.[151] Examples under this level include alteration or deletion of data in a cyber system with consequences that are neither physical nor functional.[152] Given the foregoing, Typology 2 involving manipulation of electoral systems conducted through cyber means may arguably fall under this third level or even in the second level in the event that it results in "loss of functionality." Meanwhile, Typologies 3 and 4 are inapplicable in this analysis under the first basis as their target and effects relate to the voting population, not to election systems and infrastructure.

With regard to the second basis, i.e., interference with or usurpation of inherently governmental functions, this relates to those functions "exclusively reserved to [a] State on [ ] [its] territory."[153] Although the experts making the Tallinn Manual 2.0 did not provide a controlling definition of "inherently governmental function," they indicated that the notion of acts *jure imperii*[154] may be helpful in assessing whether such function is inherently governmental.[155] This basis flows from the fact that each State possesses an exclusive right to perform such inherently governmental functions or to decide on matters regarding their performance.[156] The intrusions meeting the thresholds of physical damage and loss of functionality, as well as intrusions not reaching both thresholds, become immaterial as what is crucial is the functions being interfered or usurped, not the degree of destruction.[157] The Tallinn Manual 2.0 experts agreed that it is immaterial, under this basis, to ascertain whether the pertinent inherently governmental function is being

150. *Id.* at 21 & Schmitt, *supra* note 26, at 44.

151. Schmitt, *supra* note 26, at 45.

152. TALLINN MANUAL 2.0, *supra* note 52, at 21.

153. *Id.* at 22.

154. As defined by Black's Law Dictionary, *jure imperii* is a Latin word, literally meaning "by right of sovereignty[,]" which refers to "public acts that a nation undertakes as a sovereign [S]tate, for which the sovereign is usu[ally] immune from suit or liability in a foreign country." BLACK'S LAW DICTIONARY 979.

155. TALLINN MANUAL 2.0, *supra* note 52, at 22 n. 26.

156. *Id.* at 21–22.

157. *Id.* at 22.

exercised "by the State [ ] or has been privati[z]ed."[158] Examples put forth by the drafters of the Tallinn Manual 2.0 include the alteration or deletion of data in such a way that the conduct of elections is interfered with.[159] Thus, based on these observations, Typology 1 relating to physical destruction and Typology 2 relating to non-physical manipulation of voting and transmission systems both involve interference with or usurpation of conducting elections — which is an inherently governmental function.

Effectively, based on the analysis offered by the Tallinn Manual 2.0, there still remains "a suboptimal debate by quarrelling about whether, instead of when, sovereignty can be violated[,]"[160] as may be evident when juxtaposed with Typologies 3 and 4. Certainly, Typologies 3 and 4 are not applicable in the analysis of either bases set forth by the Tallinn Manual 2.0 considering that these typologies target the voting public, instead of election systems, by publishing information through cyberspace — given that publication of information cannot, by itself, be properly regarded as an infringement of a State's territorial integrity under the first basis nor be considered an inherently governmental function which is an essential element under the second basis.

3. Norm of Non-intervention Under Customary International Law

a. Conventional Concept

Under both general and customary international law, the principle of non-intervention is a well-accepted norm.[161] The norm of non-intervention, in the words of the leading case of *Military and Paramilitary Activities in and Against Nicaragua*, is a principle that "forbids all States or groups of States to intervene

158. *Id.*

159. *Id.*

160. Michael Schmitt, In Defense of Sovereignty in Cyberspace, *available at* https://www.justsecurity.org/55876/defense-sovereignty-cyberspace (last accessed Jan. 30, 2022) [https://perma.cc/9859-VAK3] (emphases omitted).

161. Ashley C. Nicolas, *Taming the Trolls: The Need for an International. Legal Framework to Regulate State Use of Disinformation on Social Media*, 107 GEO. L.J. 36, 37 (2018) (citing Conference on Security and Cooperation in Europe: Final Act, *adopted* Aug. 1, 1975, DEP'T ST. BULL., Sept. 1, 1975, at 323 & Treaty of Friendship, Co-operation and Mutual Assistance Between the People's Republic of Albania, the People's Republic of Bulgaria, the Hungarian People's Republic, the German Democratic Republic, the Polish People's Republic, the Romanian People's Republic, the Union of Soviet Socialist Republics and the Czechoslovak Republic art. 8, *signed* May 14, 1955, 219 U.N.T.S. 3 (entered into force June 6, 1955)).

directly or indirectly in internal or external affairs of other States."[162] This norm prohibits foreign state interference over other States' internal or foreign affairs.[163] Non-intervention, as a principle that surrounds sovereignty, is crucial in maintaining an established system of competing States.[164] However, not all kinds of intervention is proscribed and, currently, there is limited academic literature delineating what is lawful interference and otherwise.[165]

Non-intervention was further explained in the *Military and Paramilitary Activities in and Against Nicaragua* case, in this wise —

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a *political*, economic, social[,] and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[166]

Thus, non-intervention, from the *Military and Paramilitary Activities in and Against Nicaragua* case, has two distinct elements: (1) cases involving matters which a State can freely decide upon by virtue of sovereignty,[167] including "the choice of *political*, economic, social[,] and cultural systems and the formulation of foreign policy[,]"[168] and (2) coercion which is "particularly obvious in the case of an intervention which uses force, either in the direct

162. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 108, ¶ 205.

163. Van De Velde, *supra* note 46, at 25 (citing Philip Kunig, Intervention, Prohibition of, *available at* http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL (last accessed Jan. 30, 2022) [https://perma.cc/VLM6-BSAD]).

164. SHAW, *supra* note 108, at 213.

165. Van De Velde, *supra* note 46, at 25.

166. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 108, ¶ 205 (emphasis supplied).

167. SHAW, *supra* note 108, at 1148.

168. *Id.* (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 108) (emphasis supplied).

form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[169]

b. Application to Cyber-Electoral Interference

Before the modern age, an unlawful intervention saw one State engaging in some kind of coercion, e.g., using force, in order to force another sovereign State into one choice which it would not have made absent the coercion.[170] Notably, the ICJ only had few chances to opine on the limitations of the prohibition of intervention due to the fact that, prior to the modern age, most of the conduct which violated the norm of non-intervention also inevitably involved a physical infringement of sovereignty.[171] In other words, conduct made subject of international law cases before modern times involved physical intrusion, with international tribunals primarily anchoring their rulings based on violations of a State's sovereignty, while briefly discussing the violations of the prohibition of intervention or omitting such discussion altogether.

While the ICJ in the *Military and Paramilitary Activities in and Against Nicaragua* case laid down two elements, as enumerated above, these do not sufficiently provide for an adequate framework to cover cyber-electoral interference, such as the one conducted during the 2016 U.S. Presidential elections.[172]

With regard to the prohibition of intervention, Rule 66 of the Tallinn Manual 2.0 states that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[173] This reflects the agreement among the Tallinn Manual 2.0 experts that this prohibition is a norm of customary international law, inasmuch as the said Rule reflects the idea that coercive intervention through modes conducted in cyberspace is likewise proscribed.[174]

Thus, translated to cyberspace, for an operation to violate the prohibition of intervention, the Tallinn Manual 2.0 prescribes two elements, as follows:

169. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 108, ¶ 205.

170. Nicolas, *supra* note 161, at 37 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 108, ¶ 205).

171. Nicolas, *supra* note 161, at 37.

172. Ohlin, *supra* note 96, at 244.

173. TALLINN MANUAL 2.0, *supra* note 52, at 312, rule 66.

174. *Id.* at 312.

"[t]he operation must, [first,] affect a State's *domaine réservé*[,] and[, second,] it must be coercive."[175]

The first element relating to a State's *domaine réservé*, in the words of the *Military and Paramilitary Activities in and Against Nicaragua* case, relates to matters including the "choice of a *political*, economic, social, and cultural system, and the formulation of foreign policy."[176] With respect to cyber-electoral interference, this element is complied with as elections necessarily involve matters related to the choice of a political system.[177]

The crucial question, however, relates to complying with the second requisite, i.e., that the operation "must be coercive."[178] The experts of the Tallinn Manual 2.0 defined coercion as one "not limited to physical force, but rather refer[ing] 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."[179] There is doubt that cyber operations aimed at influencing decisions meet this "coercive" element.[180] Tallinn Manual 2.0 acknowledges such nuance, observing that

> coercion 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.[181]

175. Schmitt, *supra* note 26, at 48 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 205 & TALLINN MANUAL 2.0, *supra* note 52, at 314–17).

176. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 205 (emphasis supplied).

177. *See* TALLINN MANUAL 2.0, *supra* note 52, at 315.

178. Schmitt, *supra* note 26, at 48 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 205 & TALLINN MANUAL 2.0, *supra* note 52, at 314–17).

179. TALLINN MANUAL 2.0, *supra* note 52, at 317 (citing Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, *supra* note 122, princ. 3).

180. Schmitt, *supra* note 26, at 50.

181. TALLINN MANUAL 2.0, *supra* note 52, at 318–19 (emphases supplied). According to the Merriam-Webster Dictionary, the word "influence" is defined as "the act or power of producing an effect without apparent force or direct authority[,]" or alternatively, "the power or capacity of causing an effect in indirect or intangible ways" while "compel" means "to drive or urge with force[.]" THE MERRIAM-WEBSTER DICTIONARY 147 & 372 (2004). Likewise, "compel," as defined by

Thus, mounting information campaigns for the voting public chiefly designed to influence and persuade — Typology 4 of cyber-electoral interference — will not amount to coercion.[182] As an example, it has been suggested that the influence campaign conducted in cyberspace in the campaign period for the 2016 U.S. elections should be characterized as "deception, not coercion" as it involved impostors pretending to be U.S. citizens in social media "to amplify particular social and political positions, thereby increasing partisan rancor and the type of political anger that encourages people to vote."[183] Meanwhile, with regard to Typology 3, while the publication of such information does not arguably amount to coercion, the process of illicitly obtaining such information necessarily involves coercion given that process necessitates an unconsented cyberspace intrusion into a private or classified system or database to extract the said information.

4. Due Diligence Obligation Under Customary International Law

a. Conventional Concept

In the general legal sense, "due diligence" is broadly defined as "an obligation of conduct on the part of a subject of law" in which, "[n]ormally, the criterion applied in assessing whether a subject has met that obligation is that of the responsible citizen or responsible government[.]"[184] This principle traces its roots from the ancient Latin maxim "*sic utero tuo ut alienum non laedas*[,]" roughly translated as, "use your own property in such a manner as not to injure that of another[.]"[185]

As a concept under international law, due diligence is currently viewed as a general principle of law with state practice devising more specific rules and standards with regard to what is required by due diligence insofar as particular

Black's Law Dictionary, means "[t]o cause or bring about by force, threats, or overwhelming pressure[.]" BLACK'S LAW DICTIONARY 342.

182. *See* TALLINN MANUAL 2.0, *supra* note 52, at 319.

183. Ohlin, *supra* note 96, at 244.

184. Timo Koivurova, Due Diligence (Max Planck Encyclopedia of Public International Law Entry), *available at* https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034 (last accessed Jan. 30, 2022) [https://perma.cc/XAK5-2KLL].

185. Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer*, 95 TEX. L. REV. 1555, 1565 (2017).

areas of international law are concerned.[186] Moreover, due diligence is reflective of a general principle of international law laid down in the ICJ case of *Corfu Channel*,[187] where the court explained —

> The obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them. Such obligations are based ... on certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communication; and *every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*.[188]

Due diligence was likewise emphasized in the *Trail Smelter Arbitration*[189] between the U.S. and Canada where the arbitral tribunal ratiocinated, viz. —

> under the principles of international law, ... no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.[190]

In light of its history in international law, due diligence was important particularly with regard to state responsibility for private actors which, in such case, entailed preventive measures that a State is expected to employ within "its sphere of exclusive control when international law was breached by private persons, not by the State as a legal entity."[191] As one scholar observes, the obligations relating to due diligence play a crucial role, given that its focus relates to the "responsibility of a State for violations of international law by private persons under its exclusive jurisdiction and control[,]" and, in many situations, this obligation is becoming "of increasing importance given that the globalizing world is shifting societal power to non-State actors."[192]

---

186. Koivurova, *supra* note 184.

187. Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 INT'L & COMP. L.Q. 643, 649 (2018) (citing Corfu Channel Case (U.K. v. Alb.), Merits, Judgment, 1949 I.C.J. 6, 22 (Apr. 9)).

188. *Corfu Channel Case*, 1949 I.C.J. at 22 (emphasis supplied).

189. Trail Smelter Arbitration (U.S./Can.), Award, 3 R.I.A.A. 1905 (1941).

190. *Id.* at 1965.

191. Koivurova, *supra* note 184.

192. *Id.*

b. Application to Cyber-Electoral Interference

In cyberspace, the general applicability of the obligation of due diligence is undisputed, in view of the widely-accepted rule that States must not allow their territory to be utilized for cyber operations in order to wreak havoc and cause serious consequences for other States.[193]

As regards cyberspace operations, Tallinn Manual 2.0 experts considered the current gamut of primary and secondary international law sources and while they noted that due diligence has been applied primarily in "transboundary environmental harm[,]"[194] they observed that it "has been particulari[z]ed in speciali[z]ed regimes of international law" and that, "[s]ince new technologies are subject to pre-existing international law absent a legal exclusion therefrom, they concluded that the due diligence principle applies in the cyber context."[195] This due diligence principle is brought about by omission — not only confined to absolute inaction but also including employment of measures which are either ineffective or insufficient in the face of other measures which are more feasible, i.e., "reasonably available and practicable."[196] While agreeing that the principle is a primary rule under international law applicable in the cyber context, Tallinn Manual 2.0 experts qualified the application of the principle, as follows —

> 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. 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. 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. Third, borrowing from international environmental law, the experts agreed that the obligation only attaches when the consequences for the victim State are 'serious.'

193. Chircop, *supra* note 187, at 644.

194. Schmitt, *supra* note 26, at 54 (citing *Trail Smelter Arbitration*, 3 R.I.A.A. at 1965; U.N. Conference on the Human Environment, *Declaration of the United Nations Conference on the Human Environment*, princ. 21, U.N. Doc. A/CONF.48/14/Rev.1 (June 16, 1972) (also known as the Stockholm Declaration); & U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, annex I, princ. 2, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I) (Aug. 12, 1992) (also known in short as the Rio Declaration)).

195. TALLINN MANUAL 2.0, *supra* note 52, at 31.

196. *Id.* at 43.

> 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.[197]

Thus, based on the quoted passage above, the limitations may be summarized as follows: (1) "a State is taking all feasible measures to put an end to cyber operations,"[198] (2) a State is "tak[ing] action in the face of ongoing harmful cyber activities or ones in which a material step has been taken towards execution,"[199] and (3) "consequences ... are 'serious'" and "'contrary to the rights' of the target State."[200]

Notwithstanding these limitations, this principle of due diligence is able to solve, or at the very least, mitigate the legal conundrum of attributing cyber operations in that it relieves the victimized State from having to attribute specific acts of cyber operations to the perpetrator State.[201] Otherwise stated, "[l]egal recognition of such breaches of diligence permits State victims of cyber harm to take action to induce compliance and terminate harm without necessarily tracing attribution to the original, difficult-to-identify source. Such an approach has gained momentum among both States and commentators."[202] As long as the victim State can positively establish that cyber operations breached an obligation under international law had they been attributable to a State, such as instances of violations of sovereignty or prohibited non-intervention, the State where such cyber operations are being mounted has "a legal duty to take feasible measures to put an end to the operation."[203] Furthermore, the conduct in question, i.e., the cyber operations, should pose serious adverse consequences and, consequently, conduct involving the interference with a State's elections will typically meet such threshold.[204]

197. Schmitt, *supra* note 26, at 54 (citing TALLINN MANUAL 2.0, *supra* note 52, at 34, 43-44, & 47).

198. Schmitt, *supra* note 26, at 54 (citing TALLINN MANUAL 2.0, *supra* note 52, at 47).

199. Schmitt, *supra* note 26, at 54 (citing TALLINN MANUAL 2.0, *supra* note 52, at 43-44).

200. *Id.* *See* Chircop, *supra* note 187, at 650.

201. Schmitt, *supra* note 26, at 54-55. *See* discussion *infra* Part IV (on attribution of cyber-electoral interference).

202. Jensen & Watts, *supra* note 185, at 1558.

203. Schmitt, *supra* note 26, at 54-55.

204. *Id.*

In any case, while there remain "several doctrinal ambiguities [that] surround due diligence" such as, for instance, the specific level of harm needed to trigger the application of the due diligence obligation, most proponents nevertheless agree, at the very least, that this duty of due diligence only applies where there is known harm.[205] This duty enjoins States only to "undertake reasonably feasible measures to cease offending uses of its territory" inasmuch as there is general consensus among experts that there exists "no duty to affirmatively monitor networks or to prevent offending use of cyber infrastructure."[206]

C. Summary of Potential Violations of Cyber-Electoral Interference Based on the Four Typologies

Based on the foregoing discussion in this Part, the following are the possible violations under the current framework of international law, summarized in a table detailing the applicability of each potential violation as juxtaposed with the four adopted typologies of cyber-electoral interference and explained thereafter. To reiterate, the four typologies discussed in the previous Sections, are as follows: Typology 1: Attacking election infrastructure,[207] Typology 2: Manipulating voting and transmission systems,[208] Typology 3: Publicizing illicitly-obtained information,[209] and Typology 4: Mounting information campaigns.[210]

Typology / Violation	Typology 1: Attacking election infrastructure	Typology 2: Manipulating voting and transmission systems	Typology 3: Publicizing illicitly-obtained information	Typology 4: Mounting information campaigns
Prohibition on the Use of Force	✓	✗	✗	✗

205. Jensen & Watts, *supra* note 185, at 1566 (citing TALLINN MANUAL 2.0, *supra* note 52, at 40-43).

206. Jensen & Watts, *supra* note 185, at 1566 (citing TALLINN MANUAL 2.0, *supra* note 52, at 43-50).

207. *See* Van De Velde, *supra* note 46 & McNamara, *supra* note 46.

208. *See* TENOVE, ET AL., *supra* note 46 & GALANTE & EE, *supra* note 33.

209. *See* GALANTE & EE, *supra* note 33 & McNamara, *supra* note 46.

210. *See* Van De Velde, *supra* note 46; BRATTBERG & MAURER, *supra* note 46; & Hansen & Lim, *supra* note 45.

Sovereignty	✓	✓	✗	✗
Norm of Non-Intervention	✓	✓	✓	✗
Due Diligence Obligation	✓	✓	✓	✓

1. Prohibition on the Threat or Use of Force Under the UN Charter

The prohibition on the threat or use of force is rooted in the UN Charter, an international agreement, and is a primary rule of international law. While "force" is widely perceived and accepted among legal scholars to relate to physical damage, whether "force" extends to the non-physical destruction of operating software of machines remains unsettled. Typology 1, i.e., attacking election infrastructure, alone can result to a violation on the prohibition on the threat or use of force. Typologies 2, 3, and 4 — which involve conduct not resulting to physical damage — cannot be characterized as "force" under *lex lata*.

2. Sovereignty Under Customary International Law

A violation of a State's sovereignty, according to the Tallinn Manual 2.0, may be based on either: "[Basis] (1) the degree of infringement upon the target State's territorial integrity; and [Basis] (2) whether there has been an interference with or usurpation of inherently governmental functions."[211]

For Basis (1), there are three identified thresholds of damage: "[(1a)] physical damage, [(1b)] loss of functionality, [and] [(1c)] infringement upon territorial integrity falling below the threshold of loss of functionality."[212] The standards relating to both (1b) and (1c) remain unsettled. In relation to Basis (1), Typology 1 constitutes a sovereignty violation based on (1a). Typology 2 can arguably fall under (1b), if there is indeed "loss of functionality" following an alteration or deletion of data in the cyber-electoral system — though the definition of "loss of functionality" remains unsettled. Likewise, Typology 2 may arguably even fall under (1c), though the parameters for this third and lowest threshold is specifically undefined by experts at this point. Typologies

211. TALLINN MANUAL 2.0, *supra* note 52, at 20.

212. *Id.*

3 and 4 do not involve an infringement of territorial integrity and, therefore, cannot violate a State's sovereignty under Basis (1).

In relation to Basis (2), the thresholds of damage are immaterial as what is critical is that the conduct relates to inherently governmental functions. Typologies 1 and 2 amount to a violation of sovereignty as these typologies necessitate intrusion — whether physical or non-physical — into election systems, thereby amounting to an interference with or usurpation of an inherently governmental function. Typologies 3, and 4, cannot be a violation of a State's sovereignty under Basis (2) as these typologies relate to publishing information which is not an inherently governmental function.

3. Non-intervention Under Customary International Law

The norm of non-intervention has been widely accepted under both general and customary international law. In the cyber context, the Tallinn Manual 2.0 provides that an operation conducted in cyberspace violates the principle of non-intervention if these two elements concur: (1) the operation affects a State's *domaine réservé*, and (2) the operation is coercive.[213]

Typology 1 certainly satisfies both elements and thereby constitutes a violation of this norm. Typology 2 may arguably be said to meet both requirements as well and consequently be violative of the norm, considering the Tallinn Manual 2.0's definition of coercion which is "not limited to physical force."[214]

While all four typologies satisfy the first element given that all four relate to the choice of a political system which is well within a State's *domaine réservé*, the requisite of coercion is generally lacking for Typology 4 as the Tallinn Manual 2.0 distinguishes coercion from persuasion which merely involve influencing but not "factually compelling[ ] the voluntary actions of the target State, or seek no action on the part of the target State at all."[215] Meanwhile, the requisite of coercion is met by Typology 3 as the process of illicitly obtaining information for publication entails the use of coercion which,

213. Schmitt, *supra* note 26, at 48 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J., ¶ 205 & TALLINN MANUAL 2.0, *supra* note 52, at 314-17).

214. TALLINN MANUAL 2.0, *supra* note 52, at 317 (citing Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, *supra* note 122, princ. 3).

215. TALLINN MANUAL 2.0, *supra* note 52, at 318-19.

following Tallinn Manual 2.0's explanation, is "not limited to physical force."[216]

4. Due Diligence Under Customary International Law

The obligation of due diligence has been applied in different areas of international law, and, insofar as cyberspace is concerned, this obligation is regarded by the Tallinn Manual 2.0 experts as a primary rule under international law, subject to certain limitations. A particular State may violate the due diligence obligation of that State without the need for attribution as the crux of this obligation is the failure of that State to ensure that its territory is not being used for harmful cyber operations. This obligation solves or, at the minimum, mitigates the difficulties associated with attributing cyber-operations to the State in order for state responsibility to set in. Therefore, insofar as the obligation of due diligence is concerned, it is immaterial as to which typology is utilized as the mode of conducting cyber-electoral interference. The identities of the perpetrators behind the cyber-electoral interference become also immaterial given that a violation already exists when there is a failure on the part of the State to take "reasonably available and practicable" measures[217] to end harmful cyber-electoral interference mounted within that State's territory, regardless of whether the perpetrator is the State itself, its organs, or non-State actors. Thus, analyzing the violation of this obligation does not require an inquiry into the modes of committing cyber-electoral interference, but rather the State's omission or failure to stop cyber-electoral interference being conducted within its territory.

IV. SECOND STEP IN LOCATING THE NEXUS OF STATE RESPONSIBILITY FOR FOREIGN CYBER-ELECTORAL INTERFERENCE UNDER INTERNATIONAL LAW: ATTRIBUTION OF CONDUCT

A. Modes of Attribution Under ARSIWA

Aside from the element of "breach" that was tackled in the previous Part, the other element under the ARSIWA constituting an internationally wrongful act is "attribution," which "denote[s] the operation of attaching a given action or omission to a State."[218] Though the State is an organized entity duly

216. TALLINN MANUAL 2.0, *supra* note 52, at 317 (citing Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, *supra* note 122, princ. 3).

217. TALLINN MANUAL 2.0, *supra* note 52, at 43.

218. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 2 cmt. 12, at 84.

recognized as an artificial person and subject of international law, the State cannot act by itself; therefore, the acts of a particular State must involve either an act or omission on the part of a human being or a group of human beings.[219] Moreover, state responsibility "lay[s] emphasis on the existence of an internationally wrongful act[,] not [upon] the damage or injury caused[,] and the existence of a causal link between the damage and the breach of obligation."[220]

Articles 4 to 11 of the ARSIWA provide for the instances when the conduct of a person, group, or entity — which consists of a single act or omission, or a series of acts or omissions — become the conduct of the State.[221] These eight Articles govern the characterization of the circumstances by which the conduct of a person, a group, or an entity becomes considered an act of the State.[222] Based on these Articles, conduct is imputed to the State when it is the:

(1) conduct of a state organ,[223]

(2) conduct of "persons or entities exercising elements of governmental authority[,]"[224]

(3) conduct of a state organ "placed at the disposal of a State by another State[,]"[225]

(4) conduct of a state organ or person or entity "empowered to exercise elements of governmental authority" even when the conduct "exceeds its authority or contravenes instructions[,]"[226]

(5) conduct "of a person or group of persons" that "is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct[,]"[227]

---

219. *Id.* art. 2 cmts. 5-6, at 82-83.

220. Antonopoulos, *supra* note 92, at 116 (citing ARSIWA, *supra* note 8, art. 1).

221. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, pt. I, ch. II cmt. 1, at 91.

222. Amdadul Hoque, *Existence, Breach and Responses to the Breach of State Responsibility: A Critical Analysis*, 53 J. L. POL'Y & GLOBALIZATION 136, 137 (2016).

223. ARSIWA, *supra* note 8, art. 4.

224. *Id.* art. 5.

225. *Id.* art. 6.

226. *Id.* art. 7.

227. *Id.* art. 8.

(6) conduct "of a person or group of persons" that "is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority[,]"[228]

(7) conduct of an "insurrectional or other movement[,]" subject to certain conditions,[229] and,

(8) conduct that has been "acknowledged and adopted by the State as its own[.]"[230]

These will further be covered in the following Sections and will be principally discussed based on the kind of actor for ARSIWA Articles 4 to 10, in addition to ARSIWA Article 11 on acknowledgment and adoption. The length and depth of the discussion of these Articles will vary, in view of the relevance of each Article insofar as cyber-electoral interference is concerned.

1. Organs (ARSIWA Articles 4, 6, & 7)

For state organs, ARSIWA Articles 4, 6, and 7 are applicable to attribute acts of state organs to the State.[231] The rule that the conduct of state organs is regarded as that of the State is founded on the "principle of the unity of the State[.]"[232] Under ARSIWA Article 4 (1), any state organ, regardless of function, hierarchy, and classification, may potentially be the author of an internationally wrongful act.[233] For state organs, it is irrelevant for the purpose of attribution that their conduct may possibly be classified as commercial in nature; nevertheless, it is worth noting that a contractual breach by a State does not necessarily entail a breach of international law.[234] Moreover, there is no distinction between superior and subordinate officials, provided that they act in their official capacity.[235] As long as they act "in an apparently official capacity, or under [color] of authority," their actions become that of the State by attribution.[236]

228. *Id.* art. 9.

229. ARSIWA, *supra* note 8, art. 10.

230. *Id.* art. 11.

231. *See* ARSIWA, *supra* note 8, arts. 4, 6, & 7.

232. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 4 cmt. 5, at 95.

233. *Id.* art. 4 cmts. 5-6, at 95 & ARSIWA, *supra* note 8, art. 4 (1).

234. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 4 cmt. 6, at 96.

235. *Id.* art. 4 cmt. 7, at 96.

236. *Id.* art. 4 cmt. 13, at 99.

ARSIWA Article 4 (2) also provides that "[a]n organ *includes* any person or entity which has that status in accordance with the internal law of the State."[237] The use of the word "includes" in the Article accounts for the possibility that, in some jurisdictions, both internal law and practice are what determine the status of the different entities that are regarded as state organs under the ARSIWA.[238]

A state organ may either be *de jure* or *de facto*; the latter involves non-State actors which become *de facto* state organs by virtue of such state organ being under the "absolute dependence and control of a State."[239] With *de facto* state organs being included, States can no longer simply evade responsibility by merely denying, refusing, or failing to officially designate the acting entity as an organ of the State.[240]

The conduct of state organs is likewise the subject of ARSIWA Article 7 which touches on "unauthorized or *ultra vires* acts of state organs [as well as other] entities."[241] The said Article states that the conduct of a state organ is attributable to the State "if the organ ... acts *in that capacity*, even if it exceeds its authority or contravenes instructions."[242] As clarified in the Official Commentary on the ARSIWA, the phrase "in that capacity" is indicative of the fact that the conduct being referenced in that Article is conduct of organs "purportedly or apparently carrying out their official functions, and not the private actions or omissions of individuals who happen to be organs or agents of the State" and, consequently, the question boils down to "whether they were acting with apparent authority."[243]

ARSIWA Article 6 — covering a narrowly specific situation — States that "[t]he conduct of an organ *placed at the disposal of* a State by another State shall be considered an act of the former State under international law if the organ is acting in the exercise of elements of governmental authority of the State at whose disposal it is placed."[244] The phrase "placed at the disposal of" implies that the state organ "is acting with the consent, under the authority of[,] and

237. ARSIWA, *supra* note 8, art. 4 (2) (emphasis supplied).

238. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 4 cmt. 11, at 98.

239. Antonopoulos, *supra* note 92, at 116.

240. *See id.* at 116-17.

241. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 7 cmt. 1, at 106.

242. ARSIWA, *supra* note 8, art. 7 (emphasis supplied).

243. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 7 cmt. 8, at 106.

244. ARSIWA, *supra* note 8, art. 6 (emphasis supplied) & ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 6 cmt. 1, at 103.

for the purposes of the receiving State" in such a way that such organ acts "in conjunction with the machinery of that State and under its exclusive direction and control, rather than on instructions from the sending State."[245] Notably, Article 6 does not apply for ordinary instances when States cooperate and collaborate between and among themselves, pursuant to an international agreement or otherwise.[246]

2. Person(s) or Group Exercising Elements of Governmental Authority (ARSIWA Articles 5, 7, & 9)

ARSIWA outlines the conditions by which the conduct of a person or group exercising elements of governmental authority becomes state conduct under Articles 5, 7, and 9 therein.[247] ARSIWA Article 5 provides, viz. —

> The conduct of a person or entity which is not an organ of the State under [A]rticle 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.[248]

This Article involves a person or groups that "exercise elements of governmental authority in place of state organs, as well as situations where former state corporations have been privatized but retain certain public or regulatory functions."[249] The attribution is justified based on the fact that the State's municipal law has specifically conferred and authorized elements of governmental authority for these entities to possibly exercise.[250] The entities can be conferred "independent discretion or the power to act" and it is unnecessary to show that such conduct was in fact performed under the State's control.[251]

ARSIWA Article 7 dealing with unauthorized or *ultra vires* acts likewise governs "a person or entit[ies] empowered to exercise elements of the governmental authority[,]" in the same way that state organs fall within the ambit of the said Article.[252] Meanwhile, ARSIWA Article 9 contemplates a

245. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 6 cmt. 2, at 103.

246. *Id.*

247. *See* ARSIWA, *supra* note 8, arts. 5, 7, & 9.

248. ARSIWA, *supra* note 8, art. 5.

249. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 5 cmt. 1, at 103.

250. *Id.* art. 5 cmts. 5 & 7, at 101–02.

251. *Id.* art. 5 cmt. 7, at 101–02.

252. ARSIWA, *supra* note 8, art. 7.

specific situation where the conduct of a person or group becomes attributable to the State under narrowly-defined conditions, as follows —

> first, the conduct must effectively relate to the exercise of elements of the governmental authority, secondly, the conduct must have been carried out in the absence or default of the official authorities, and thirdly, the circumstances must have been such as to call for the exercise of those elements of authority.[253]

3. Person(s) or Group Acting on the Instructions of, or Under the Direction or Control of the State (ARSIWA Article 8)

Although acts or omissions of private entities that are not state organs generally cannot become State conduct under international law, ARSIWA Article 8 supplies instances when such can be attributable to the State under certain conditions.[254] The said Article states that "[t]he conduct of a person or group of persons" becomes considered as state conduct when such "*person or group of persons* is in fact acting on the instructions of, or under the direction or control of, that State carrying out the conduct."[255] Notably, the use of the phrase "person or group of persons" in this Article reflects the fact that the contemplated conduct may possibly be committed on a "*de facto* basis" by a group lacking separate personality by legal fiction.[256]

This kind of attribution has been widely accepted under international law.[257] Whether or not those whose conduct is in question are private persons or groups is immaterial.[258] Moreover, the conduct in question should not necessarily involve "governmental activity[,]" as ARSIWA Article 8 is couched in broad terms not qualifying such conduct.[259] The most common instances of this kind of attribution arise where private persons or groups are recruited or instigated by state organs for such persons or groups to act as "auxiliaries[,]" albeit operating outside the official state hierarchy.[260] In other instances, these private persons or groups

253. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 9 cmt. 3, at 115.

254. ARSIWA, *supra* note 8, art. 8.

255. *Id.* (emphasis supplied).

256. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 9, at 113.

257. *Id.* art. 8 cmt. 2, at 110.

258. *Id.*

259. *Id.*

260. *Id.*

become "volunteers" to other countries or otherwise sent on specific missions abroad.[261]

Challenging issues arise when the conduct was fulfilled "under the direction or control of" a State.[262] In such case, the conduct will be attributed to the State only if the conduct in question was integrally part of the operation and, consequently, will not be considered as State conduct if the part is simply either incidental or peripheral to the said operation and "escaped from the State's direction or control."[263]

In the ICJ case of *Military and Paramilitary Activities in and Against Nicaragua*, the degree of "control" was put in issue.[264] The issue was whether the conduct of the non-State Nicaraguan operatives, known as the *contras*, was attributable to the conduct of the State concerned, i.e., the U.S., in order for the U.S. to be held responsible for an internationally wrongly act under international law.[265] The ICJ ruled that not all the conduct of the *contras* was attributable to the U.S., which was responsible for "planning, direction, and support" given to the *contras*,[266] as the court explained —

> All the forms of [U.S.] participation mentioned [ ], and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the [U.S.] directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State. Such acts could well be committed by members of the *contras* without the control of the [U.S.]. For this conduct to give rise to legal responsibility of the [U.S.], it would in principle have to be proved that that State had *effective control* of the military or paramilitary operations in the course of which the alleged violations were committed.[267]

---

261. *Id.*

262. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 3, at 110.

263. *Id.*

264. *Id.* art. 8 cmt. 4, at 110–11 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 14).

265. *Id.*

266. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 4, at 110 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 51, ¶ 86).

267. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 4, at 110 (citing *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 62 & 64–65, ¶¶ 109 & 115) (emphasis supplied).

The ICJ held in the same case that a "general situation of dependence and support would be insufficient to justify attribution of the conduct to the State."[268]

Meanwhile, in *Prosecutor v. Tadić*,[269] the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia elucidated that "[t]he *degree of control* may, however, vary according to the factual circumstances of each case. The Appeals Chamber fails to see why in each and every circumstance international law should require a high threshold for the test of control."[270] In that case, the Appeals Chamber said that the required degree of control exercised by the Yugoslavian authorities over the armed forces as required under international law for determining the armed conflict to be of international character was "*overall control* going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations[.]"[271] Notably, the majority in this case disapproved of the ICJ's approach in *Military and Paramilitary Activities in and Against Nicaragua* as the legal and factual milieu dealt with by the tribunal pertained not to state responsibility, but rather to criminal responsibility.[272] In any case, the attribution of a particular conduct of a person or group of persons to the State depends on the factual circumstances of each case.[273]

As regards the conduct of private entities which are either State-owned or State-controlled, international law recognizes the separability of the corporate vehicle at the national level, except in instances when piercing the "corporate veil" is warranted as when the corporation is used as "a mere device or a vehicle for fraud or evasion."[274] Although these corporate entities are owned by the State and, in that narrow sense, is subject to state control, that fact alone will not prima facie make these entities' acts attributable to the State, unless they exercise elements of governmental authority, thereby triggering the

268. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 4, at 91.

269. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Judgment (Int'l Crim. Trib. For the Former Yugoslavia July 15, 1999).

270. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 5, at 111 (citing *Tadić*, ICTY Appeals Judgment, ¶ 117).

271. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 5, at 112 (citing *Tadić*, ICTY Appeals Judgment, ¶ 145).

272. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 5, at 112.

273. *Id.*

274. *Id.* at 112, art. 8, ¶ 6 (citing Barcelona Traction, Light and Power Company, Limited (Belg. v. Spain), Second Phase, Judgment, 1970 I.C.J. 3, 39, ¶¶ 56-58 (Feb. 5)).

application of ARSIWA Article 5.[275] Meanwhile, in the event that the corporation exercised public powers or was being used by the State — which has ownership interest therein — to accomplish a specific result, the conduct will be attributed and considered that of the State.[276]

Notably, as the phraseology of ARSIWA Article 8 stands, the words "instructions[,]" "direction[,]" and "control" are enumerated disjunctively; therefore, it is sufficient to establish any of the three.[277] Additionally, to come under the purview of Article 8, such instructions, direction, or control should "relate to the conduct which is said to have amounted to an internationally wrongful act."[278] Cases where the State instructs or directs persons or groups should be differentiated from cases where the State controls them. In cases where a State has instructed or directed an agent who later fails to observe the instructions or directions given and contravenes international obligations of the State which instructed the agent, such may be resolved by the question of "whether the unlawful or unauthorized conduct was really incidental to the mission or clearly went beyond it."[279] Generally, a State, in instructing or directing the person or group which is not a state organ, does not bear the risks involved when such instructions are carried out in an unlawful way under international law.[280] This is in contrast to instances when a person or group has done acts under the State's effective control, thereby making their conduct attributable to the State, even if the State's instructions were ignored.[281]

4. Insurrectional or Other Movements (ARSIWA Article 10)

The specific case where the conduct involved is that of an insurrectional or other movement which "becomes the new [g]overnment of the State or succeeds in establishing a new State" is properly dealt with by ARSIWA Article 10.[282] Generally, conduct of an insurrection or movement is not attributable to the State as it relies on the assumption that the movement, as well as its structures and organization, remains independent of the State which

275. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 6, at 112.

276. *Id.* art. 8 cmt. 6, at 112–13.

277. *Id.* art. 8 cmt. 7, at 113.

278. *Id.*

279. *Id.* art. 8 cmt. 8, at 113.

280. *Id.*

281. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 8 cmt. 8, at 113.

282. *Id.* art. 10 cmt. 1, at 116.

later successfully quells the uprising.[283] Under this Article, when the movement in question accomplishes its goals and either designates itself as the new government of a State, or creates a new State within the territory administered or belonging to a pre-existing State, the conduct of such successful movement will be attributable to the State with a new government or to the newly-formed State, as the case may be.[284] The conduct involved properly pertains to the conduct of the movement and should not be understood to include the conduct of the movement's members who act in their own capacity.[285] Based on the parameters for attribution set forth under ARSIWA Article 10 and considering the conduct examined in this Note, it is evident that this Article is inapplicable in the context of determining state responsibility for cyber-electoral interference.

5. Acknowledged and Adopted Conduct (ARSIWA Article 11)

In the event that the conduct is not attributable based on ARSIWA Articles 4 to 10, Article 11 may be resorted to for attribution when the conduct, though not attributable under the previous Articles, becomes "an act of [the] State ... if and to the extent that the State acknowledges and adopts the conduct in question as its own."[286] Such acknowledgment and adoption by a State may be either express or inferred from the acts or omissions of the said State.[287] Consequently, the conduct that Article 11 pertains to, in most cases, is that of a private person or group.[288] Similar to Article 10, Article 11 is another exception to the basic rule that conduct which is purely private in nature cannot be attributable to the State.[289] If there exists doubts as to whether certain conduct falls under Article 8, i.e., based on a person or group under the instructions, directions, or control of a State, Article 11 may resolve such doubts in the event the State subsequently acknowledges and adopts the said conduct — which, consequently, makes such conduct attributed to the State.[290]

283. *Id.* art. 10 cmt. 4, at 117.

284. *Id.*

285. *Id.*

286. ARSIWA, *supra* note 8, art. 11.

287. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 11 cmt. 9, at 123.

288. *Id.* art. 11 cmt. 2, at 121.

289. *Id.* art. 11 cmt. 3, at 121.

290. *Id.* art. 11 cmt. 5, at 122.

In relation to the word "acknowledgment," mere support or endorsement by a State does not fall within the coverage of Article 11 given the clear qualification of its phrase "acknowledges and adopts the conduct in question *as its own*."[291] This is the case in situations when States merely approve or endorse a particular conduct in the general sense but do not assume any responsibility.[292] A general acknowledgment by the State of a factual situation is not sufficient as what is required, under this Article, is that the conduct in question must be identified by the State which must make such conduct its own.[293] Likewise, mere acknowledgment or verbal approval by the State in relation to the factual existence of certain conduct is not enough to attribute such conduct to the State under this Article.[294]

As regards the word "adoption" as used in the Article, such term denotes the idea that the State acknowledged the conduct "as, in effect, its own conduct."[295] As long as the State manifests its intent to accept responsibility for conduct which would otherwise be not attributable to itself, Article 11 may possibly contemplate cases where a State takes responsibility "for conduct of which it did not approve, which it had sought to prevent[,] and which it deeply regretted."[296]

Withal, Article 11 only operates insofar as the question of attribution is concerned.[297] Thus, even though certain conduct was acknowledged and adopted by a State, the wrongfulness of such act under international law, i.e., the breach, must still be considered in order to establish an internationally wrongful act.[298] In the same vein, in the event a State acknowledges and adopts conduct that is lawful under international law, the State will not bear any responsibility even though the conduct in question is considered unlawful acts of the person or group concerned — unless the State agrees to carry the additional responsibility of indemnifying the said conduct of another.[299]

The phrase "if and to the extent that" implies that the State may possibly acknowledge and adopt conduct only to a certain extent in that it may choose

291. *Id.* art. 11 cmt. 6, at 122 (emphasis supplied).

292. *Id.* art. 11 cmt. 6, at 123.

293. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 11 cmt. 6, at 123.

294. *Id.* art. 11 cmt. 6, at 122-23.

295. *Id.* art. 11 cmt. 6, at 123.

296. *Id.*

297. *Id.* art. 11 cmt. 7, at 123.

298. *Id.*

299. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 11 cmt. 7, at 123.

to do so only in relation to some, and not all, of the conduct involved.[300] Such phrase also indicates that the State's act of acknowledgment and adoption must be made in a clear and unequivocal manner — whether through words or deeds.[301]

B. Attribution of Cyber-Electoral Interference

Based on the previous Section, attribution to the State of acts of cyber-electoral interference may therefore be permissibly made where the act is that of a: state organ, person(s) or group exercising elements of governmental authority, or person(s) or group acting on the instructions of, or under the direction or control of the State, or where the conduct has been acknowledged and adopted by the State. Notably, the mode of attribution involving the conduct of insurrectional or other movements under ARSIWA Article 10 will not apply as the conduct examined in this Note relates to cyber-electoral interference.

Problems concerning attribution readily arise with respect to these emerging forms of cyber-electoral interference given the animosity which is inherent in the digital architecture and nature of the Internet. Unlike the physical and visible space, cyberspace is unique given "its borderless character, its inherent interconnectedness, the anonymity it affords and its accessibility," among others.[302]

Although ascribing certain acts to the State may prove to be a challenge in the advent of emerging modes of cyber-electoral interference, there is no reason to "sweepingly deny as a matter of principle the application of the rules of attribution provided in [ARSIWA] to conduct in cyberspace."[303] Though attributing cyber operations to the State may be difficult, it is not impossible.[304]

That notwithstanding, the architecture of cyberspace guarantees, to a large extent, anonymity in such a way to possibly deny the identification of the

300. *Id.* art. 11 cmt. 8, at 123.

301. *Id.*

302. Russell J. Buchan, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, 21 J. CONFLICT & SEC. L. 429, 429 (2016).

303. Antonopoulos, *supra* note 92, at 119.

304. United States Office of the Director of National Intelligence, A Guide to Cyber Attribution, at 2, *available at* https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf (last accessed Jan. 30, 2022) [https://perma.cc/8NX3-EKUA].

computer or machine behind particular conduct performed in cyberspace.[305] Moreover, identifying the person or group operating such computer responsible for an act may not be proven with certainty in that attribution can practically only be made through the internet protocol (IP) address that identifies a computer's precise location.[306] Thus, it would appear that an international wrongful act committed in cyberspace will be "ascribed to a particular computer whereas the identity of the person [or group] operating it may be established either by way of presumption or on the basis of inside information disclosed by government agents of the State perpetrating the internationally wrongful act[.]"[307] As an illustration, if an internationally wrongful act is ascribed to a specific computer which is identified to be located in the premises of a State's governmental office (e.g., the premises of a State organ), then such act may be attributed to that State by way of the presumption that the operator is a state agent or the presumption that the premises where the computer is located "falls under the exclusive and complete control of [that] State."[308] Notably, a malicious cyber operation which is identified to originate from within one State's territory does not necessarily translate to the said State being responsible, considering that the actor must fall under the possible modes of attribution enumerated under the ARSIWA.[309] In addition, given the complexity of cyber operations, coupled with the anonymity that cyberspace provides, the possibility of misattribution is high.[310]

The process of legal attribution, in such example, has two separable elements: the "technical attribution," or the process of identifying the identity and location of the cyber infrastructure or machine involved, and "political attribution," or the process of identifying the person or group operating such machine.[311] Thereafter, the legal nexus must be established through the process of linking the actor — the person or group — and the State, using the modes of attribution properly laid out in the ARSIWA.[312] Stated otherwise, attribution of conduct in cyberspace is not simply identifying who conducted such operation, as it instead involves "a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that

305. Antonopoulos, *supra* note 92, at 119.

306. *Id.* *See* Buchan, *supra* note 302, at 430.

307. Antonopoulos, *supra* note 92, at 119-20.

308. *Id.* at 120.

309. Jensen & Watts, *supra* note 185, at 1560.

310. Denton, *supra* note 141, at 206.

311. Sander, *supra* note 46, at 26.

312. *Id.* at 27-28. *See* Chircop, *supra* note 187, at 645-49.

perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation."[313]

On the process of legal attribution, one scholar explains the challenges relating to conduct mounted within cyberspace, thus —

> With respect to legal attribution, a specific challenge arises in the context of cyber influence operations on elections when States outsource aspects of influence campaigns to non-State actors [—] a prominent example being the [IRA] which conducted various aspects of the cyber influence operation on the 2016 U.S. presidential election. In such circumstances, a State may operate strategically to evade the relevant standards of attribution, for example by ensuring that non-State actors do not act under its 'effective control' for the purposes of attribution pursuant to Article 8 of the [ARSIWA]. Equally, non-State actors may engage in cyber influence operations without any degree of State involvement [—] a possibility heightened by the diffusion of power within cyberspace. In each of these circumstances, the duty of due diligence may offer a partial solution, though only if the target State is able to demonstrate that each of its core elements [—] knowledge of the cyber operation, failure to take reasonably feasible measures, and acting contrary to the rights of the target State with serious adverse consequences [—] have been met on the facts at hand.[314]

Meanwhile, the Tallinn Manual 2.0 takes a "rather cautious approach" in the attribution of acts conducted in cyberspace to a State,[315] as it elucidates that —

> Traditionally, the use of governmental assets, in particular military equipment like tanks or warships, has long constituted a nearly irrefutable indication of attribution due to the improbability of their use by persons other than State organs. This traditional rebuttable presumption cannot be easily translated into the cyber context. In particular, another State or a non-State actor may have acquired control over government cyber infrastructure and is using it to conduct cyber operations. Accordingly, the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to

313. United States Office of the Director of National Intelligence, National Intelligence Council, *supra* note 2, at 2.

314. Sander, *supra* note 46, at 28.

315. Antonopoulos, *supra* note 92, at 121.

> that State. That said, such usage can serve as an *indication* that the State in question may be associated with the operation.[316]

The Tallinn Manual 2.0 goes on to say that

> [e]ven less compelling as an indication of State involvement is the mere fact that a harmful cyber operation has been mounted using private cyber infrastructure in a State's territory. This is a particularly important limitation in light of the possibility of creating botnets using zombie computers to mount distributed [DoS] attacks.[317]

In any case, attribution under the international legal framework on state responsibility is primarily a question of law rather than a "mere recognition of a link of factual causality."[318] That said, the Tallinn Manual 2.0 does not propose any alternative, leaving the issue of attribution plagued with ambiguity; hence, this suggests that the injured State has a wide latitude of discretion to decide on the legal question of attribution based on possibly extra-legal factors, including the diplomatic relationship between the injured State and another State.[319] Thus, without any alternatives provided, what is seemingly favored is "a more flexible application of the current legal framework of attribution by an injured State on a case-by-case basis."[320]

Ultimately, given that attribution of an internationally unlawful act is properly a matter of evidence, it has been submitted "that a very liberal approach to evidence is called for by the very nature of cyberspace" — an approach that will aggregate information obtained from technical expertise and the media.[321] While the law on state responsibility, as evinced by ARSIWA, does not provide for standards or quantum of proof when States go through the process of legal attribution, States are required to "act 'reasonably' in the circumstances."[322]

Likewise, as one scholar explains succinctly —

316. TALLINN MANUAL 2.0, *supra* note 52, at 91 (emphasis supplied).

317. *Id.*

318. Antonopoulos, *supra* note 92, at 121 (citing ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, pt. I, ch. II cmt. 4, at 91).

319. Antonopoulos, *supra* note 92, at 121.

320. *Id.*

321. *Id.* at 122.

322. Sander, *supra* note 46, at 27-28 (citing TALLINN MANUAL 2.0, *supra* note 52, at 81-83).

> attribution means who is responsible, or assigning a cause to an action. In the cyber domain, attribution means 'identifying the agent responsible for the action.' Because the Internet facilitates anonymous communications and 'was not designed with the goal of deterrence in mind,' attribution of cyber intrusions can be challenging, particularly when the exploiters craft their intrusions to confound finding who is responsible.[323]

That said, "[t]his difficulty in attribution should underscore an underlying point: actors with little to no state direction can still wield formidable influence and execute network exploitation operations. It is not only the impact of these techniques that is the most troubling [—] it is also their ease of replication."[324]

Attributing a state organ's conduct to the State is "[t]he most straightforward form of attribution" in which an organ such as a State's intelligence agency can commit not just acts of espionage, but also, possibly, electoral interference.[325] Consequently, while it is clear that conduct of state organs is attributed to the State, it is highly likely that such State will perceivably and conveniently circumvent state responsibility by instead tapping on entities that are not state organs to interfere in elections of other States as emerging forms of cyber-electoral interference become more pervasive and easily replicable in the coming years.

In most cases, cyber-electoral interference is conducted by non-State actors who do so based "on the instructions of, or under the direction or control of" another State.[326]

Moreover, technical problems will further complicate proving attribution in that activities conducted over the Internet can hardly be traced and, even assuming that the victim State proves that the activity is linked to infrastructure owned by another State, this does not conclusively establish that the other

323. William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1492 (2017) (citing David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 531 (2011)).

324. GALANTE & EE, *supra* note 33, at 15.

325. Schmitt, *supra* note 26, at 59-60.

326. Annachiara Rotondo & Pierluigi Salvati, *Fake News, (Dis)information, and the Principle of Nonintervention: Scope, Limits, and Possible Responses to Cyber Election Interference in Times of Competition*, CYBER DEF. REV., 2019, at 214 (citing ARSIWA, *supra* note 8, art. 8).

State is responsible as it may be the case that other interested States took control of such infrastructure to further sow confusion.[327]

In any event, while attribution of cyberspace operations to the State proves to be a challenge, "governments have become increasingly public in attributing malicious cyber activity. These public attribution statements and their counteractions serve as strong indicators of the norms that have been emerging in this area over the last several years."[328]

V. CONSEQUENCES FOLLOWING AN INTERNATIONALLY WRONGFUL ACT

According to the ARSIWA, the consequences flowing from an internationally wrongful act are that the State found responsible has the obligation "to cease that act, if it is continuing[,]" and "to offer appropriate assurances and guarantees of non-repetition, if circumstances so require[,]" under ARSIWA Article 30,[329] and that such responsible State must "make full reparation for the injury caused by the internationally wrongful act," consistent with ARSIWA Article 31.[330] Such "[f]ull reparation for the injury caused by the internationally wrongful act" shall either be "restitution, compensation[,] and satisfaction, either singly or in combination[.]"[331]

Cessation involves "the basic obligation of compliance with international law, which in principle remains due in spite of any breaches" and "is required, not as a means of reparation but as an independent obligation, whenever the obligation in question continues to exist."[332] Meanwhile, reparation "refer[s] to all measures which may be expected from the responsible [S]tate, over and above cessation[,] [and] it includes restitution, compensation, and satisfaction."[333] Restitution, as part of the broader term reparation, "refers to restitution in kind, a withdrawal of the wrongful measure, or the return of

327. Rotondo & Salvati, *supra* note 326, at 215 (citing TALLINN MANUAL 2.0, *supra* note 52, at 91).

328. GALANTE & EE, *supra* note 33, at 14.

329. ARSIWA, *supra* note 8, art. 30 & ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 28 cmt. 2, at 192.

330. ARSIWA OFFICIAL COMMENTARIES, *supra* note 92, art. 28 cmt. 2, at 192 (citing ARSIWA, *supra* note 8, art. 31).

331. ARSIWA, *supra* note 8, art. 34.

332. CRAWFORD, *supra* note 93, at 553.

333. *Id.*

persons or assets seized illegally."[334] Compensation, as reputed international law scholar James Crawford explains, is "reparation in the narrow sense of the payment of money in the measure of the wrong done."[335] Satisfaction is defined as a "means of redressing a wrong other than by restitution or compensation."[336] Satisfaction may be in various forms, even cumulative, such as "apologies or other [acknowledgment] of wrongdoing by means of payment of an indemnity or a ... salute to the flag[,]" subjecting the perpetrators to trial and punishment, or employing measures to prevent the harm from occurring again.[337]

There are, according to Crawford, possible remedies for the victim State, which he discusses in this wise —

> In the event of an internationally wrongful act by a [S]tate or other subject of international law, other [S]tates or subjects may be entitled to respond. This may be done by invoking the responsibility of the wrongdoer, seeking cessation, and/or reparation, or (if no other remedy is available) possibly by taking countermeasures. ... There are important differences between them: cessation and reparation are obligations which arise by operation of law on the commission of an internationally wrongful act, whereas countermeasures (if available at all) are an ultimate remedy which an injured [S]tate may take after efforts to obtain cessation and reparation have failed. They are responsive not just to the breach as such but to the responsible [S]tate's failure to [fulfill] its secondary obligations[.][338]

While these remedies are available to the victim State, such may be limited considering the effects of electoral interference. The damage may already be irreparable, considering the unquantifiable and extensive nature of these emerging forms of cyber-electoral interference.[339]

One scholar has argued for the use of countermeasures in relation to an internationally wrongful act rooted in an act of electoral interference by a foreign State, viz. —

> Although there are numerous other limitations on the taking of countermeasures, the option allows for flexibility in two regards. First,

---

334. *Id.*

335. *Id.*

336. *Id.*

337. *Id.* at 561.

338. CRAWFORD, *supra* note 93, at 552.

339. Hanson and Thomas conclude that "[t]here [is] a lack of empirical data on the impacts of foreign interference and the effectiveness of various attempts to combat it, such as fact-checking services." Hanson & Thomas, *supra* note 32.

> countermeasures need not be directed at the entity that launched the initial unlawful cyber operation. 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. 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.[340]

Otherwise stated, the flexibility of countermeasures lies in the usage of different means to achieve the purpose that is to end the act of electoral interference — which may possibly be directly aimed at crippling the infrastructure or indirectly by imposing pressure through economic sanctions.[341]

VI. THE INADEQUACY OF THE CURRENT INTERNATIONAL LAW FRAMEWORK ON STATE RESPONSIBILITY FOR FOREIGN CYBER-ELECTORAL INTERFERENCE

A. Current Framework

Based on the discussion in the previous Parts, the current framework under international law for state responsibility for cyber-electoral interference may be summarized as follows:

Step 1: The determination of the typology[342] is initially assessed based on the target: Does the act of cyber-electoral interference target: (1) election infrastructure, or (2) the voting public or a segment thereof?

Step 2: If the target is (1) election infrastructure, then the typology is characterized based on the effects: did the act cause kinetic effects, i.e., producing physical damage? If yes, then the act falls under Typology 1. If not, then the act falls under Typology 2. If the target is (2) the voting public or a segment thereof, then the typology is characterized based on the type of information released: did the act involve either: (2a) the release of illicitly-obtained private or confidential information to the voting public or a segment thereof or (2b) the mounting of an information campaign? If the act involved

340. Schmitt, *supra* note 26, at 65 (citing TALLINN MANUAL 2.0, *supra* note 52, at 112–13 & 128–29).

341. *Id.*

342. *See* discussion *supra* Part II (on the four typologies).

is (2a), then it falls under Typology 3. If the act involved is (2b), then it falls under Typology 4.

Step 3: The act must then be attributed to the State using the modes of attribution under the ARSIWA: Can the act be traced to the computer or machine, then traced to the actor/group that must be (a) a state organ, (b) person(s) or group exercising elements of governmental authority, or (c) person(s) or group acting on the instructions of, or under the direction or control of the State? Alternatively, has the act been (d) acknowledged and adopted subsequently by the State? If either or both of the questions are answered in the affirmative, then the act is attributed to the State and then Step 4 consequently follows. If both questions are answered in the negative, the act cannot therefore be attributed to the State.

Nevertheless, whether or not the conduct in question has been attributed to the State, where "consequences ... are 'serious'" and "'contrary to the rights' of the target State," and the State fails to "tak[e] all feasible measures to put an end to ... cyber operations," "in the face of ongoing harmful cyber activities, or ones in which a material step has been taken towards execution," then the State is liable for breaching its obligation of due diligence under international law.[343]

Step 4: In case such act has been attributed to the State in Step 3, the breach of the obligation will depend on the typology, as follows:

If Typology 1 applies, then the following are certainly breached by the State: (1) the prohibition on the use of force under the UN Charter, (2) the State's sovereignty, and (3) the duty of non-intervention.

If Typology 2 applies, then: (1) sovereignty may certainly be breached on the basis that the act is considered an "interference with or usurpation of inherently governmental functions;" or, alternatively, sovereignty may arguably be breached *if* such results in "loss of functionality" or on a threshold lower than "physical damage" and "loss of functionality," and (2) the duty of non-intervention may arguably be breached *if* coercion is "not limited to physical force."

If Typology 3 applies, then: the duty of non-intervention may arguably be breached by virtue of the process of illicitly obtaining such information *if* coercion is "not limited to physical force."

343. *See* Schmitt, *supra* note 26, at 54 (citing TALLINN MANUAL 2.0, *supra* note 52, at 34, 43-44, & 47).

If Typology 4 applies, then: the duty of non-intervention, in contrast to Typology 3, may arguably not be breached as coercion may be distinguished from mere persuasion and influence.

Moreover, given the presence of breach/es under Step 4 and the breach of due diligence under Step 3, then there is an internationally wrongful act that will then require certain obligations from the responsible State and afford the victim State certain remedies.[344]

B. Assessment of the Current Framework

As seen in the previous Section, there are certainly numerous gaps in the framework — there are breaches which may arguably exist provided that certain qualifications are met and possible interpretations are recognized. Verily, cyber-electoral interference clearly can neither squarely fit nor be encapsulated by the current norms and principles under international law.

This Note submits that, based on the current state of international law, as well as the body of literature interpreting international law, only Typology 1 can certainly and absolutely fall under the violations of the prohibition on the use of force under the UN Charter,[345] sovereignty, and the norm of non-intervention. However, as discussed, Typology 1 has not even manifested itself as a real-life example, primarily because States will certainly avoid Typology 1 and choose instead to exploit gray and disputed areas under international law.

The gaps and difficulties arise at the outset for Typologies 2, 3, and 4. Although these three typologies constitute interference in another State's elections, these typologies do not rise to the threshold of physical use of force under the UN Charter. Therefore, a resort to obligations under customary international law is made. In relation to these three typologies, there is basis arguably to pin the breach to a certain obligation under customary international law; however, such remains arguable absent any binding international agreement, or established interpretation of the related principles in light of the nature of cyber-electoral interference. For Typology 4, uncertainty remains as to whether such can be violative of a State's obligations relating to the use of force, sovereignty, and non-intervention as merely "influencing" may not amount to coercion or force as currently conceived and understood. Thus, as it stands, only the obligation of due diligence may come into play insofar as Typology 4 is concerned.

344. *See* discussion *supra* Part V.

345. *See* U.N. CHARTER art. 2, ¶ 4.

While there is basis to use the obligation of due diligence for all typologies in order to solve the difficulty of attribution in cyberspace, there remains uncertainty as to what constitutes "serious" consequences for due diligence to be invoked. Moreover, inasmuch as the duty of due diligence may provide basis for Typology 4 to be tantamount to a breach, the issue relating to how the effects to the voting public or a segment thereof under Typology 4 will be measured — in order to amount to a "serious" consequence — remains an open question.

In sum, given the current state of international law, not all typologies violate each of the pertinent rules under customary international law chiefly because the law has not caught pace with the increased proliferation of cyber-electoral interference in the past years. At present, there are many gray areas which cannot be definitively settled by the different sources of international law. These gray areas cannot be settled by a reading of any convention or treaty as there exists none squarely tackling cyber-electoral interference of States. Nor can such gray areas, brought to light by the recent emerging forms of interference, be firmly resolved given the lack of state practice and *opinio juris* in order to evince and prove custom. Likewise, a resort to scholars and highly qualified publicists who refer, interpret, and draw analogies from international principles, norms, and past international decisions is another gray area to tread as such interpretations and analogies are subject to much debate and critique, with arguments that cut both ways.

Ultimately, the Author is of the view that legal gaps in the current international law framework need to be addressed. There is an urgent necessity to provide for a set of rules that should govern States moving forward, which lays down what acts constitutes cyber-electoral interference by a State under international law.

VII. RECOMMENDATIONS AND CONCLUSIONS TOWARD ADDRESSING STATE RESPONSIBILITY FOR FOREIGN CYBER-ELECTORAL INTERFERENCE

The Author is of the view that the gaps identified in this Note should be addressed through a treaty.[346] Currently, there are numerous UN resolutions affirming the States' obligations to respect sovereignty and the norm of non-intervention in the electoral processes of States.[347] While UN resolutions

346. *See infra* Annex.

347. Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 44/147, U.N. Doc. A/RES/44/147 (Dec. 15, 1989); Respect for the Principles of National

"represent the dynamic development of international legal norms and reflect the commitment of [S]tates to move in certain directions, abiding by certain principles[,]"[348] they nonetheless remain non-binding.

Consequently, there is a pressing need for States to enter into a binding instrument, which is exemplified by a treaty, in order to hold States truly responsible and accountable for cyber-electoral interference.

Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 45/151, U.N. Doc. A/RES/45/151 (Dec. 18, 1990); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 46/130, U.N. Doc. A/RES/46/130 (Dec. 17, 1991); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res/47/130, U.N. Doc. A/RES/47/130 (Dec. 18, 1992); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 48/124, U.N. Doc. A/RES/48/124 (Dec. 20, 1993); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Process, G.A. Res. 49/180, U.N. Doc. A/RES/49/180 (Dec. 23, 1994); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 50/172, U.N. Doc. A/RES/50/172 (Dec. 22, 1995); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res. 52/119, U.N. Doc. A/RES/52/119 (Dec. 12, 1997); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, G.A. Res 54/168, U.N. Doc. A/RES/54/168 (Dec. 17, 1999); Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Electoral Processes as an Important Element for the Promotion and Protection of Human Rights, G.A. Res. 56/154, U.N. Doc. A/RES/56/154 (Dec. 19, 2001); Respect for the Principles of National Sovereignty and Diversity of Democratic Systems in Electoral Processes as an Important Element for the Promotion and Protection of Human Rights, G.A. Res. 58/189, U.N. Doc. A/RES/58/189 (Dec. 22, 2003); & Respect for the Principles of National Sovereignty and Diversity of Democratic Systems in Electoral Processes as an Important Element for the Promotion and Protection of Human Rights, G.A. Res. 60/164, U.N. Doc. A/RES/60/164 (Dec. 16, 2005).

348. United Nations Permanent Forum on Indigenous Issues, Frequently Asked Questions: Declaration on the Rights of Indigenous Peoples, at 2, *available at* https://www.un.org/esa/socdev/unpfii/documents/FAQsindigenousdeclaration.pdf (last accessed Jan. 30, 2022) [https://perma.cc/8ZUY-K8CW].

Given that the status of cyber-electoral interference in international law remains unclear, States are left on their own, without any definitive guide to characterize and calibrate their legal lenses in comprehending cyber-electoral interference attributed to other States. Thus, the Author submits that a treaty is the most feasible, efficient, and practical way forward. By formulating new, specific, and definitive obligations which States must follow, cyber-electoral interference will, in no uncertain terms, be recognized as a breach of a State's obligations under international law. With the four typologies observed to be emerging in recent years, it remains to be seen if there may be new techniques employed in the future which may not fall under any of these four typologies and will warrant a new typology. Thus, in view of the uncertainty that the future may bring vis-à-vis cyber-electoral interference, the treaty shall lay down guidelines and parameters defining cyber-electoral interference and delineating the obligations of the State Parties in the said treaty. This recognizes the fact that the current state of international law cannot adequately address the four typologies in this study, let alone novel modes by which cyber-electoral interference may be committed in the future. The treaty will pave the way for cases involving cyber-electoral interference to be brought to the ICJ and will likewise justify the use of countermeasures following such interference. Based on the rules and principles of international law that currently govern, countermeasures may not be justified and the victim State pursuing such countermeasures may be the one performing an internationally wrongful act under this gray area of international law — especially when there exists no clear-cut legal basis to support the assertion that cyber-electoral interference is a breach of international law. In fine, by having a treaty, the gaps in the primary sources of international law are addressed and countermeasures would find basis for their exercise.

With cyber-electoral interference becoming more rampant as the world progresses in this information age, States should be certain that the development of international law proceeds in the right direction. After all, in the words of retired Supreme Court Associate Justice Antonio T. Carpio, "[t]he ultimate goal of a just society is the rule of justice, not just the rule of law." [349] Hopefully, this Note serves an initial effort to develop the international law regime in relation to cyber-electoral interference in order to

349. Antonio T. Carpio, Former Associate Justice, Supreme Court, *Follow the Rule of Law, but Aspire for the Rule of Justice*, Address at the 73d Commencement Exercises of the School of Law, Ateneo de Manila University (July 14, 2019) (transcript *available at* https://2012.ateneo.edu/sites/default/files/2019%20Commencement%20Speech%20by%20JU.S.TICE%20ANTONIO%20CARPIO.pdf (last accessed Jan. 30, 2022) [https://perma.cc/S2TK-CN8U]).

achieve the "rule of justice." As States tread and illuminate these murky areas of international law in the coming years, they must know fully well that the fate of the free world hangs in the balance.

ANNEX: PROPOSED TREATY

CONVENTION ON THE PREVENTION AND PUNISHMENT OF FOREIGN ELECTORAL INTERFERENCE CONDUCTED IN CYBERSPACE

Approved and proposed for signature and ratification or accession on [date]

Entered into force on [date], in accordance with Article IX

The Contracting Parties,

Reaffirming the purpose of the United Nations to develop friendly relations among nations based on respect for the rule of sovereignty and non-intervention,

Considering that interference through cyberspace in another State's elections is contrary to the spirit and aims of the United Nations and condemned by the civilized world,

Recognizing that cyber-electoral interference remains rampant yet squarely unaddressed under international law,

Recognizing that electoral systems of States are shifting to more automated systems which become vulnerable and susceptible to interference conducted through cyberspace,

Recognizing that the voting populations of various States are using the Internet more pervasively, therefore becoming targets of malicious information campaigns aimed at interfering with electoral processes,

Recognizing that States have obligations toward other States in cyberspace including the obligation to uphold the Charter of the United Nations, the obligation to respect another State's sovereignty, the obligation to respect the norm of non-intervention, and the obligation of due diligence,

Recognizing that electoral processes of a State involve matters which a State should freely decide upon by virtue of sovereignty, free from foreign interference, and that coercion is not limited to physical force as it may be performed in cyberspace,

Recognizing that cyber-electoral interference attributable to States may take various forms, including, but not limited to: attacking election infrastructure, manipulating voting and transmission systems, publicizing illicitly-obtained information, and mounting information campaigns, with the main goal of undermining electoral processes,

Recognizing that attributing cyber-electoral interference to a State in consonance with international law, as codified in the 2001 Responsibility of States for Internationally Wrongful Acts, is attended with much difficulty in the medium of cyberspace,

Welcoming the commitment of all State Parties to this Convention toward eliminating forms of cyber-electoral interference in view of the pervasive effects that electoral interference conducted in cyberspace causes,

Hereby agree as hereinafter provided:

Article I

Each State Party undertakes not to engage in any form of electoral interference conducted in cyberspace against another State. Failure by any State Party to observe the obligations set forth herein will constitute a breach of international law which shall make the said State liable for an internationally wrongful act, in conformity with the international legal framework on State Responsibility.

Article II

In the present Convention, cyber-electoral interference is defined as the act of meddling, through cyberspace, in a State's formal electoral processes of selecting a person for public office or of accepting or rejecting a political proposition by voting, in order to disturb the territorial State's ability to perform the said formal process as it wishes. Cyber-electoral interference includes, but is not limited to:

(a) Attacking election infrastructure in another State's elections which causes kinetic effects or produces physical damage to such infrastructure, thereby interfering with or usurping the said State's inherently governmental function of conducting elections;

(b) Manipulating voting and transmission systems in another State's elections which results in damage such as, but not limited to, physical damage and loss of functionality of the said systems, thereby interfering with or usurping the said State's inherently governmental function of conducting elections;

(c) Publicizing illicitly-obtained private or classified information of another State, including any act which constitutes an unconsented cyberspace intrusion into a private or classified system or database to extract information and release the same, with the goal of depriving the voters of that State of their freedom of choice or to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way;

(d) Mounting information campaigns intended to force voters of another State to vote in some specific way brought about by force, threats, or overwhelming pressure.

Article III

The following acts shall be punishable under this Convention:

(a) Cyber-electoral interference, as defined under Article II, which is attributable to a State Party, pursuant to the international legal framework on State Responsibility;

(b) Attempt to commit cyber-electoral interference, as defined under Article II, directly or by overt acts, which are attributable to a State Party, pursuant to the international legal framework on State Responsibility;

(c) Failure on the part of a State Party to employ reasonably available and practicable measures to prevent cyber-electoral interference in another State, which is being conducted within the State Party's territory.

Article IV

State Parties committing cyber-electoral interference or any of the other acts enumerated in Article III shall constitute a breach of their obligations under international law.

Article V

The State Parties undertake to enact, in accordance with their respective Constitutions, the necessary legislation to give effect to the provisions of the present Convention, and, in particular, to provide effective measures to suppress any and all forms of cyber-electoral interference being conducted within its territory.

Article VI

States charged with cyber-electoral interference or any of the other acts enumerated in this Convention shall be tried by the International Court of Justice.

Article VII

Any State Party may call upon the competent organs of the United Nations to take such action under the Charter of the United Nations as they consider appropriate for the prevention and suppression of acts of cyber-electoral interference or any of the other acts enumerated in Article III.

Article VIII

Disputes between the State Parties relating to the interpretation, application, or fulfillment of the present Convention, including those relating to the responsibility of a State for cyber-electoral interference or for any of the other acts enumerated in Article III, shall be submitted to the International Court of Justice at the request of any of the parties to the dispute.

Article IX

The present Convention shall be open for signature on behalf of any Member of the United Nations and of any non-member State to which an invitation to sign has been addressed by the General Assembly.

The present Convention shall be ratified, and the instruments of ratification shall be deposited with the Secretary-General of the United Nations.

Instruments of accession shall be deposited with the Secretary-General of the United Nations.

On the day when the first ten instruments of ratification or accession have been deposited, the Secretary-General shall draw up a procès-verbal and transmit a copy thereof to each Member of the United Nations and to each of the non-member States contemplated in the first paragraph of this article.

The present Convention shall come into force on the thirtieth day following the date of deposit of the tenth instrument of ratification or accession. Any ratification or accession effected subsequent to the latter date shall become effective on the thirtieth day following the deposit of the instrument of ratification or accession.

Article X

Any State Party may at any time, by notification addressed to the Secretary-General of the United Nations, extend the application of the present Convention to all or any of the territories for the conduct of whose foreign relations that State Party is responsible.

Article XI

The original of the present Convention shall be deposited in the archives of the United Nations.

A certified copy of the Convention shall be transmitted to each Member of the United Nations and to each of the non-member States contemplated in Article IX.

Article XII

The present Convention shall be registered by the Secretary-General of the United Nations on the date of its coming into force.