FOREIGN INTERFERENCE IN ELECTIONS UNDER THE NON-INTERVENTION PRINCIPLE: WE NEED TO TALK ABOUT "COERCION"

STEVEN WHEATLEY*

This article looks at the problem of foreign state cyber and influence operations targeting democratic elections through the lens of the non-intervention principle. The work focuses on the meaning of "coercion" following the 1986 Nicaragua case, wherein the International Court of Justice concluded that "[i]ntervention is wrongful when it uses methods of coercion." The analysis shows that coercion describes a situation where (1) the foreign power wants the target state to do something and wants to be certain this will happen; (2) the outside power then takes some action, either by issuing a coercive threat, using coercive force, or engaging in the coercive manipulation of the target's decision-making process; and (3) the target then does that something. The application of this understanding to the problem of cyber and influence operations targeting elections leads to the following conclusions: the hacking of the information and communications technologies used in elections is always coercive, and therefore wrongful, because the foreign power is trying to get the target state to do something it would not otherwise do; fake news operations are coercive, and therefore prohibited, where they are designed to get the electorate to vote differently; disinformation campaigns intended to cause policy paralysis or manipulate the views of the population also constitute coercion, and, therefore, violate the non-intervention rule. By explaining the meaning of "coercion," this article demonstrates that the long-established principle of non-intervention can regulate the new problem of cyber and influence operations targeting elections.

Key words: Intervention • Democracy • Elections • Cyber • Coercion • Manipulation

---

* Thank you to Russell Buchan, Patt Caps, Harriet Moynahan, and Valentina Vadi for their comments. My thanks also to the editorial team at the journal. The usual caveat applies. Earlier versions of the paper were presented at a workshop on "The Meaning of Coercion," Centre for Law & Society, University of Lancaster, December 2018; a conference on "New Technologies: New Challenges for Democracy and International Law," University of Cambridge, March 2019; and a conference on "Legal Resilience in an Era of Hybrid Threats," University of Exeter, April 2019.

I. INTRODUCTION

This article examines the legality of foreign state cyber and influence operations targeting democratic elections. Whilst there are several ways the issue can be framed,[1] this work looks at the subject from the perspective of the non-intervention principle, which prohibits states from intervening in the internal affairs of other states. There are four reasons for this lens. First, the non-intervention principle (also referred to as the principle of non-intervention, and non-intervention rule) is well established in international law. Second, the international law that applies to the cyber domain are the same ones that apply in the physical world. Third, democratic states have framed the issue in these terms. Finally, non-intervention is the dominant way that international lawyers think about the problem of foreign interference in elections.[2]

The dangers of foreign state cyber and influence operations targeting elections first emerged following complaints that Russia meddled in the 2016 U.S. presidential election.[3] Later, in 2018, a meeting of Foreign and

1. *See* Barrie Sander, *Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 CHINESE J. INT'L L. 1, 1 (2019).

2. *See* Jens David Ohlin, *Election Interference: The Real Harm and The Only Solution* 6 (Cornell Legal Stud. Res. Paper Series, Res. Paper No. 18-50, 2018) (stating that "the basic rubric for evaluating legal election interference involves a resort to the basic standards for non-intervention.").

3. The U.S. Office of the Director of National Intelligence concluded that Russian cyber and influence operations during the 2016 Presidential election were motivated by a desire to support the candidacy of Donald Trump over Hillary Clinton and to undermine the faith of the American public in

Security Ministers of the G7 states—Canada, France, Germany, Italy, Japan, United Kingdom, and United States—highlighted the dangers of outside powers "tampering with election results" and "manipulating public discourse."[4] A 2019 speech by the U.K. Foreign Secretary outlines these concerns, where he explained that a foreign power, "armed with nothing more ambitious than a laptop computer," could manipulate the outcome of an election, either by injecting propaganda into the campaign, or even changing the result where an electronic voting system is used.[5]

Because the non-intervention principle only prohibits "coercive" interferences in the internal affairs of other states,[6] this is said to create difficulties for its application to state cyber and influence operations, as coercion is often thought to require a conscious unwilling act on the part of the victim.[7] Nazi officials subjecting "third-degree methods of pressure" to the President and Foreign Minister of Czechoslovakia in 1939, Czechoslovakia was clearly coerced— consciously, albeit unwillingly, into agreeing to the establishment of a German protectorate over Bohemia and Moravia.[8] However, this understanding of coercion does not translate easily to the cyber domain, where the principal threats are the clandestine hacking of the information and communications technologies (ICTs) used in elections. In the cyber domain, the target state is often not conscious of the hack nor of the cyber influence operations targeting citizens through social media to affect their voting patterns.

---

the democratic process. OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS, (Jan. 6, 2017). After the vote, the U.S. announced that it was introducing a range of sanctions against Russian nationals and entities, with President Obama stating that these were "a necessary and appropriate response to efforts to harm U.S. interests in violation of *established international norms of behavior.*" THE WHITE HOUSE, OFF. OF THE PRESS SEC'Y, STATEMENT BY THE PRESIDENT ON ACTIONS IN RESPONSE TO RUSSIAN MALICIOUS CYBER ACTIVITY AND HARASSMENT (Dec. 29, 2016) (emphasis added), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity. President Obama's choice of words led some to decide that the United States did not view the alleged Russian activities as violations of international law, although others took the opposite view, concluding that the responses amounted to countermeasures in reaction to a prohibited intervention in domestic political affairs.

4. *Defending Democracy—Addressing Foreign Threats*, GOV'T OF CAN. (Aug. 1, 2019), https://www.international.gc.ca/world-monde/international_relations-relationsinternationales/g7/documents/2018-04-22-defending_democracy-defendre_democratie.aspx?lang=eng.

5. Jeremy Hunt, Foreign Sec'y, U.K., Address at the University of Glasgow: Deterrence in the Cyber Age (Mar. 7 2019).

6. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27) ("Intervention is wrongful when it uses methods of coercion . . . .").

7. *See* Katharina Ziolkowski, *Peacetime Cyber Espionage: New Tendencies in Public International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 425, 433 (Katharina Ziolkowski ed., 2013).

8. *See* Int'l Law Comm'n, Rep. on the Work of its Eighteenth Session, *reprinted in* [1966] 2 Y.B. Int'l L. Comm'n 246, U.N. Doc. A/6309/Rev.1.

Presently, there is no agreement amongst international lawyers as to whether, and when, the hacking of elections and targeted disinformation campaigns can be categorized as "coercive." One consequence of this is that hostile powers can operate in a legal grey zone, avoiding condemnation, because of the lack of agreed upon norms.[9] We see the problem in attempts to evaluate the legality of the so-called "DNC hack," which occurred during the 2016 U.S. presidential election and was widely blamed on Russia.[10] Private emails belonging to the Democratic National Committee (DNC) were published on the Internet, confirming that the DNC favoured Hillary Clinton over Bernie Sanders in the presidential primaries, damaging the Clinton campaign against Donald Trump. A leading scholar on the law on election interference, Jens Ohlin, concluded that whilst the hack "was certainly corrosive" to the proper functioning of American democracy, "it is genuinely unclear whether it should count as coercive," leaving "an overall impression of illegal conduct, but without a clear and unambiguous doctrinal route towards that conclusion."[11]

Uncertainty about the notion of cyber-coercion has led some writers to call for a reformulation of the non-intervention principle for the cyber domain.[12] Others claim that we should largely abandon the non-intervention principle, and look instead to the principle of sovereignty.[13] This is the approach of the influential Tallinn Manual 2.0, which maintains that we can deduce a rule prohibiting cyber operations that interfere with elections,[14] from the more general rule that a cyber operation must not violate the

9. Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 66 (2018).

10. *See* Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SEC. J. 146, 150 (2018).

11. Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1593–94 (2017).

12. On the various proposals, *see* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 630 (2018) (quoting Duncan Hollis); Duncan B. Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, OPINO JURIS (July 25, 2016), http://opinlojuris.org/2016/07/25/russia-and-the-dn-hack-a-violation-of-the-duty-of-non-intervention [http://perma.cc/D6G8-NFCZ]; Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1, 8 (2017), https://ssrn.com/abstract=3180687; Sander, *supra* note 1, 22–23 (quoting Myers S. McDougal & Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 YALE L. J. 771, 782 (1958)).

13. For a good introduction to the debate, *see* Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, (Chatham House Res. Paper, 2019), https://reader.chathamhouse.org/application-international-law-state-cyberattacks-sovereignty-and-non-intervention?preview=1#.

14. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS at 20, 22 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

sovereignty of another state.[15] The Tallinn Manual explains that the principle of sovereignty differs from the non-intervention principle because "intervention requires an element of coercion."[16]

The drawbacks with arguments that we should avoid or evade the "problem of coercion" are threefold. First, the International Court of Justice (ICJ) did not err when it concluded that the element of coercion "defines, and indeed forms the very essence of, prohibited intervention."[17] Coercion, or its functional equivalent, such as dictatorial interference, has been an element in the non-intervention principle since the end of the nineteenth century.[18] Secondly, the role of sovereignty in the regulation of state cyber operations is the subject of significant disagreement between international lawyers,[19] and, moreover, the rule has nothing to say about influence operations.[20] Finally, the principle of non-intervention provides the established basis on which states and international lawyers, from all parts of the world, frame foreign state interference in domestic political affairs.

To make sense of the cyber non-intervention principle, states and international lawyers need to be clear about the meaning of "coercion," given the ICJ's conclusion in the *Nicaragua* case that, "Intervention is [only] wrongful when it uses methods of coercion."[21] This article fills a significant gap in the existing literature by explaining this meaning of coercion, and by applying the understanding of coercion to the problem of cyber and influence operations targeting elections.

---

15. *Id.* at 17.

16. *Id.* at 24. The Tallinn Manual 2.0 also recognizes the application of the non-intervention principle to the cyber domain in Rule 66: "A State may not intervene, including by cyber means, in the internal or external affairs of another State." The Tallinn Manual 2.0 confirms that the principle of non-intervention only applies to operations "that have coercive effect" (Rule 66, Explanatory para. 3). The example given (without further explanation) is that of "using cyber operations to remotely alter electronic ballots and thereby manipulate an election" (Explanatory para. 2).

17. Nicar. v. U.S., 1986 I.C.J. at 14, ¶ 205.

18. The association between intervention and coercion was first made by John Stuart Mill in 1859. *See* 21 JOHN S. MILL, *A Few Words on Non-Intervention* (1859), *in* THE COLLECTED WORKS OF JOHN STUART MILL 111, 123–24 (John M. Robson ed., Univ. Toronto Press, 1984). In 1925, the Draft Code of American International Law, drawn up by the Pan-American Union, concluded that "[t]he sole lawful intervention is friendly and conciliatory action without any character of coercion." J. L. Brierly, *The Draft Code of American International Law*, 7 BRIT. Y.B. INT'L L. 14, 22 (1926).

19. On the debate, *see* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017); Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017).

20. TALLINN MANUAL 2.0, *supra* note 14, at 26 ("With regard to propaganda, the International Group of Experts agreed that its transmission into other States is generally not a violation of sovereignty.").

21. Nicar. v. U.S., 1986 I.C.J. at 14, ¶ 205 (alteration in original).

The article proceeds as follows: Section 1 explains the concerns around foreign state cyber and influence operations targeting elections; Section 2 examines the non-intervention principle, outlining its evolution from the time of Emer de Vattel to the ICJ's *Nicaragua* judgment, and confirming the application of the rule to the cyber domain; Section 3 turns to the meaning of coercion, showing that it describes a situation in which one voluntary agent wrongfully exercises power over another through the deployment of coercive threats, the use of coercive force, or the coercive manipulation of the target's decision-making process; Section 4 applies this understanding of coercion to the problem of cyber and influence operations targeting elections. The article demonstrates that any cyber operations hacking the computer infrastructure used in elections are, by definition, coercive, and therefore prohibited under the non-intervention principle. On the other hand, influence operations are more complicated. Although the provision of factual information through social media is not unlawful, some fake news and disinformation campaigns can be categorized as coercive where the objective is to usurp the target state's right to make decisions.

II. CYBER AND INFLUENCE OPERATIONS TARGETING ELECTIONS

States interfering in the electoral processes of other states is not new: between 1946 and 2000, the United States and the Soviet Union—and later Russia—interfered in approximately one in nine competitive elections in other states.[22] However, new information and communications technologies (ICTs) have created unprecedented opportunities for hostile countries to disrupt elections. Foreign powers can, for instance, disable vital computer systems, such as when hackers deleted key files and rendered the vote-tallying system inoperable during the 2014 Ukraine presidential election.[23] Additionally, a distributed denial of service (DDoS) attack, in which data requests flood a website's server and overwhelms its ability to respond, can

22. Dov H. Levin, *Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset*, 36 CONFLICT MGMT. & PEACE SCI. 88, 94 (2019). *See also*, Dov H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 INT'L STUD. Q. 189, 189 (2016).

23. Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR (June 17, 2014), https://www.csmonitor.com/layout/set/print/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers. *See also* LAURA GALANTE & SHAUN EE, ATLANTIC COUNCIL, DEFINING RUSSIAN ELECTION INTERFERENCE: AN ANALYSIS OF SELECT 2014 TO 2018 CYBER ENABLED INCIDENTS 7–8 (2018).

inhibit elections, as occurred on Bulgaria's Electoral Commission's website during the 2015 local elections.[24]

Reliance on ICTs also allows foreign powers to gain unauthorized access to a computer or computer network to affect the outcome of the vote. This can be done in four ways.[25] First, voters can be removed from the electoral roll.[26] Second, a state can interfere with the workings of electronic voting machines (where e-voting is used), changing the preferences of voters or making votes disappear. Third, the outcome of the vote can be changed by hacking the vote tabulation software. In 2014, Ukraine's presidential election was targeted by hackers, who accessed the Electoral Commission's computer, changing the result to show that the winner was a far-right, ultra-nationalist, candidate, with thiry-seven percent of the vote, as opposed to the actual one percent.[27] Finally, the legitimacy of an election can be undermined by creating confusion around the outcome. For example, false results were announced on Ghana Electoral Commission's Twitter account while the ballots were still being counted.[28]

---

24. *Huge Hack Attack on Bulgaria Election Authorities 'Not to Affect Vote Count'*, NOVINITE.COM: SOFIA NEWS AGENCY (Oct. 27, 2015, 1:14 PM), https://bit.ly/35vZQbE. A U.K. Parliamentary Committee expressed concern that the crashing of a voter registration website before the Brexit vote could have been caused by a DDoS launched by foreign powers. *See* PUBLIC ADMINISTRATION AND CONSTITUTIONAL AFFAIRS COMMITTEE, LESSONS LEARNED FROM THE EU REFERENDUM, REPORT, 2016-17, HC 496, ¶ 102–03 (UK). There is also the risk that the website of a political party could be hit by a DDoS. In 2018, a United States official blamed Russia for an attack on the website of an opposition party in Mexico during a televised presidential debate, after the website had published documents critical of another candidate. *See* David Alire Garcia & Noe Torres, *Russia Meddling in Mexican Election: White House Aide McMaster*, REUTERS (Jan. 7, 2018, 4:31 PM), https://www.investing.com/news/world-news/russia-meddling-in-mexican-election-white-house-aide-mcmaster-1073182; *see also* Daina Beth Solomon, *Cyber Attack on Mexico Campaign Site Triggers Election Nerves*, REUTERS (June 13, 2018, 4:42 PM), https://www.reuters.com/article/us-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerves-idUSKBN1J93BU.

25. *See* Scott Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J. L. REFORM 629, 636–38 (2017) (describing how foreign powers can influence an election through computer networks).

26. *See generally* Philip Bump, *When We Talk About Russian Meddling, What Do We Actually Mean*?, WASH. POST (Feb. 13, 2018, 10:37 AM), https://www.washingtonpost.com/news/politics/wp/2018/02/13/when-we-talk-about-russian-meddling-what-do-we-actually-mean/ (explaining what Russian interference consisted of in the 2016 election); *see also* Isabella Hansen & Darren J. Lim, *Doxing Democracy: Influencing Elections via Cyber Voter Interference,* 25 CONTEMP. POL. 150 (2018) (examining the influence of state-sponsored cyber voting operations).

27. NICHOLAS CHEESEMAN & BRIAN P. KLAAS, HOW TO RIG AN ELECTION 131 (Yale Univ. Press 2018). The Election Commission noticed the hack and managed to avoid naming the wrong winner. *Id.*

28. Joseph R.A. Ayee, *Ghana's Elections of 7 December 2016: A Post-Mortem*, 24 S. AFR. J. INT'L AFF. 311, 314 (2017); *see also* Michael Amoah, *Sleight is Right: Cyber Control as a New Battleground for African Elections*, 119 AFR. AFF. 68 (2019) (discussing how the growth of hacking has turned electronic data management into a key battleground in African elections).

New technologies also allow foreign powers to engage in influence operations that aim to align the political views of the target population with the interests of the foreign power.[29] Before the Internet, it was difficult for states to directly influence citizens in other states. So, between 1951 and 1956, NATO countries were reduced to sending balloons carrying propaganda leaflets into Poland, Czechoslovakia, and Hungary.[30] These days, political debates often occur in cyberspace,[31] as opposed to the past, when democratic discussion took place in the town square, in television or radio studio, or the pages of a newspaper.[32] The Internet reduces the importance of distance and national boundaries, making it much easier for foreign states to inject propaganda into election campaigns.[33] The best-known example is Russia's operation to shape the 2016 U.S. presidential election (although Russia denies responsibility).[34] The fact that foreign states can insert cyber propaganda into an election campaign is significant because the evidence shows that if you can control the information available to voters, you can determine the electoral outcome.[35]

III. THE NON-INTERVENTION PRINCIPLE

The principle of non-intervention was first explained by Emer de Vattel in the *Law of Nations*, where he writes that "no state has the smallest right to

29. *See* Duncan B. Hollis, *The Influence of War; the War for Influence*, 32 TEMP. INT'L & COMP. L. J. 31, 35 (2018) (explaining how influence operations involve the deployment of informational resources through e-mail and social media postings and the virtual collection of data).

30. LINDA ROBINSON ET AL., MODERN POLITICAL WARFARE: CURRENT PRACTICES AND POSSIBLE RESPONSES 19–20 (2018). States still engage in the practice today. Justin McCurry, *Kim Yo-jong Warns South Korea to Tackle 'Evil' Propaganda Balloons*, GUARDIAN (June 3, 2020, 11:29 PM), https://www.theguardian.com/world/2020/jun/04/kim-yo-jong-warns-south-korea-to-tackle-evil-propaganda-balloons.

31. The notion of "cyberspace" helps us make sense of the fact that we can communicate in a meaningful way via the Internet. Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 212 (2007). Whilst the idea of cyberspace as place is compelling, no one, as Mark Lemley points out, is actually "in" cyberspace. Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 523 (2003). Cyberspace is an imagined domain, made possible by a physical infrastructure of servers and computer hardware, connected by the Internet Server Protocols. *Contra* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1403 (1996) ("Cyberspace is a place. People live there. They experience all the sorts of things that they experience in real space, there.").

32. ADRIAN SHAHBAZ & ALLIE FUNK, FREEDOM ON THE NET 2019: THE CRISIS OF SOCIAL MEDIA 6 (2019).

33. Diego A. Martin et al., *Recent Trends in Online Foreign Influence Efforts*, 18(3) J. INFO. WARFARE 15 (2019).

34. KATHLEEN HALL JAMIESON, CYBERWAR: HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT: WHAT WE DON'T, CAN'T, AND DO KNOW 39 (2018); *see also* Rod Thornton & Marina Miron, *Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom*, 4 J. CYBER POL'Y 257 (2019).

35. CHEESEMAN & KLAAS, *supra* note 27, at 100–01.

interfere in the government of another."[36] Around the same time, in 1792, the British Government objected to an offer made by France to come "to the aid of all peoples who wished to recover their liberty."[37] The French Government then revoked the offer, resolving, "in the name of the French people, that it would not interfere in any manner in the government of other Powers."[38] The non-intervention rule crystalized in the period after the 1815 Congress of Vienna, as European states reacted to nations involving themselves in domestic political disputes, notably in the putting down of popular uprisings in Naples and Spain (1820), in the Greek war of independence (1821-32), and in the creation of the independent state of Belgium (1830).[39] By the middle of the nineteenth century, the principle was widely recognized.[40] The 1836 edition of *Wheaton's*, *Elements of International Law* notes, for example, that in relation to "elective governments, the choice of [those elected] ought to be freely made, in the manner prescribed by the constitution of the state, without the intervention of any foreign influence."[41]

By the twentieth century, the principle of non-intervention was firmly established.[42] The best known, and most influential, statement on the subject can be found in the 1905 first edition of *Oppenheim*, which defines intervention as a "dictatorial interference by a State in the affairs of another State for the purpose of maintaining or altering the actual condition of things."[43] The textbook also makes clear that "a State can adopt any

36. EMER DE VATTEL, *Of the Right to Security, and the Effects of the Sovereignty and Independence of Nations*, *in* THE LAW OF NATIONS, OR, PRINCIPLES OF THE LAW OF NATURE, APPLIED TO THE CONDUCT AND AFFAIRS OF NATIONS AND SOVEREIGNS § 54, at 154–55 (Joseph Chitty ed., 1870) (1758). De Vattel asserts that "affairs being solely a national concern, no foreign power has a right to interfere in them". *Id.* at ch. III § 37.

37. Lawrence Preuss, *International Responsibility for Hostile Propaganda Against Foreign States*, 28 AM. J. INT'L. L. 649, 654 (1934) (quoting Decree of Nov. 19, 1792, *Archives parlamentaires*, LIII (*1ère sér.*), p. 474).

38. *Id*. (quoting *Moniteur*, April 16, 1793).

39. P. H. Winfield, *The History of Intervention in International Law*, 3 BRIT. Y.B. INT'L L. 130, 138 (1922-1923).

40. MOUNTAGUE BERNARD, ON THE PRINCIPLE OF NON-INTERVENTION: A LECTURE DELIVERED IN THE HALL OF ALL SOULS' COLLEGE 10 (J. H. & J. Parker eds., 1860) (noting that there is "general agreement among writers on international law . . . that non-intervention is the general rule."); *see also* KENT'S COMMENTARY ON INTERNATIONAL LAW 40 (J.T. Abdy ed., 1878); THOMAS ALFRED WALKER, A MANUAL OF PUBLIC INTERNATIONAL LAW 19 (1895).

41. HENRY WHEATON, ELEMENTS OF INTERNATIONAL LAW, WITH A SKETCH OF THE HISTORY OF THE SCIENCE 97 (1836).

42. *See, e.g.*, Winfield, *supra* note 39, at 140; *see also* ELLERY C. STOWELL, INTERVENTION IN INTERNATIONAL LAW 321 (1921).

43. LASSA FRANCIS LAWERENCE OPPENHEIM, INTERNATIONAL LAW: A TREATISE 181 (1st ed. 1905).

Constitution it likes, arrange its administration in a way it thinks fit, [and] make use of [its] legislature as it pleases."[44]

The non-intervention rule was not subsumed by the general prohibition on the use of force,[45] which emerged in 1945 with the adoption of Article 2(4) of the UN Charter.[46] Article 2(7) of the Charter, which governs the relationship between the United Nations Organization and its Member States,[47] expressed the importance of non-intervention.[48] In 1949, the International Law Commission affirmed that every state "has the duty to refrain from intervention in the internal . . . affairs of any other State."[49] In 1962, the General Assembly decided to examine the principles of international law, including the obligation "not to intervene in matters within the domestic jurisdiction of any State . . .."[50] Discussions in the Special Committee led to the adoption of the 1965 Declaration on the Inadmissibility of Intervention,[51] effectively precluding further deliberation on the subject.[52] Hence, the Declaration on Friendly Relations reflects the 1965 Declaration, affirming that "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by

---

44. *Id*. at 171.

45. Before the adoption of the UN Charter, there was a general prohibition on non-intervention, i.e., "interference in time of peace . . . through forceful measures." Preuss, *supra* note 37, at 652. There was, somewhat paradoxically, no ban on a state resorting to war to achieve the same objective. R. J. VINCENT, NONINTERVENTION AND INTERNATIONAL ORDER 293 (1974). There were also notorious breaches of the non-intervention principle, notably the involvement of European powers in the Spanish Civil War. Norman J. Padelford, *The International Non-Intervention Agreement and the Spanish Civil War*, 31 AM. J. INT'L L. 578 (1937). By the outbreak of World War II, the general view was that the classical doctrine of non-intervention had proved itself to be, in the words of Wilhelm Grewe, both "ineffective and unsatisfactory." WILHELM G. GREWE, THE EPOCHS OF INTERNATIONAL LAW 595 (Michael Byers trans., Walter de Gruyter 2000) (1984).

46. U.N. Charter art. 2, ¶ 4. *See also* Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 35 (Apr. 9).

47. *See* U.N. Charter art. 2, ¶ 7 ("Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state . . . .").

48. *See* Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 267 (Jens David Ohlin et al. eds., 2015) (discussing the importance of non-intervention).

49. G.A. Res. 375 (IV), Draft Declaration on Rights and Duties of States, art. 3 (Dec. 6, 1949).

50. G.A. Res. 1815 (XVII), art 3(c) (Dec. 18, 1962).

51. G.A. Res. 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (Dec. 21, 1965) [hereinafter Declaration on the Inadmissibility of Intervention].

52. *See generally* Piet-Hein Houben, *Principles of International Law Concerning Friendly Relations and Co-Operation among States*, 61 AM. J. INT'L L. 703, 718 (1967) (discussing the attitudes of various states toward the 1965 Declaration on the Inadmissibility of Intervention); *see also* Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Relations: A Survey*, 65 AM. J. INT'L L. 713, 729 (1971).

another State."[53] Subsequent General Assembly resolutions affirmed this position.[54]

When the non-intervention principle came before the International Court of Justice in the 1986 *Nicaragua* case, the Court confirmed that the right of every state to conduct its affairs without outside interference was "part and parcel of customary international law."[55] In coming to this conclusion, the ICJ relied on both inductive and deductive reasoning, observing that "the *opinio juris* of States . . . [was] backed by established and substantial practice. It has moreover been presented as a corollary of the principle of the sovereign equality of States."[56] The Court then asked itself, what is the exact content of the principle? The ICJ did not look to the actual practice of states, but instead drew on the rule's formulation in the Declaration on Friendly Relations to conclude the following:

> 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. . . Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[57]

The International Court of Justice outlines four elements to the non-intervention rule. First, as an inter-state doctrine, the principle regulates deliberate interferences by one state in the affairs of another. Second, the interference must concern a matter which each sovereign state should be permitted to decide freely.[58] Third, intervention is only wrongful when it uses methods of coercion.[59] Finally, a coercive interference in the affairs of

53. G.A. Res. 2625 (XXV), annex, Declaration of Principles of International Law Concerning Friendly Relations, at art. 1 (Oct. 24, 1970) [hereinafter Declaration on Friendly Relations]. According to the International Court of Justice, the Declaration on Friendly Relations "reflects customary international law." Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J 403, ¶ 80 (July 22).

54. G.A. Res. 3281 (XXIX), Charter of Economic Rights and Duties of States (Dec. 12, 1974); *see also* G.A. Res. 31/91, at 42 (Dec. 14, 1976); *see also* G.A. Res. 36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (Dec. 9, 1981).

55. Nicar. v. U.S., 1986 I.C.J. ¶ 202.

56. *Id.*

57. *Id.* ¶ 205.

58. *See id.* ¶ 263 ("The Court cannot contemplate the creation of a new rule opening up a right of intervention by one State against another on the ground that the latter has opted for some particular ideology or political system.").

59. *Id.* ¶ 205. Although the International Court of Justice noted that it was only dealing with those aspects of non-intervention relevant to the dispute before it (i.e. support for subversive or terrorist armed activities in another state), there is no doubt that coercion is an element in the non-intervention rule. The 1965 Declaration on the Inadmissibility of Intervention, *supra* note 51, at art. 2 establishes, *inter alia*, that "[n]o State may use [any] measures to *coerce* another State in order to obtain from it the subordination of the exercise of its sovereign rights . . . ." (emphasis added). The 1970 Declaration on Friendly Relations, *supra* note 53, at pmbl. reaffirms "the duty of States to refrain in their international relations

another state violates international law, unless the action can be justified as a lawful countermeasure.[60]

A. The Non-Intervention Doctrine in the Cyber Domain

Notwithstanding the conceptual challenges posed by the Internet to notions of sovereignty and jurisdiction,[61] there is growing agreement that the principle of non-intervention applies to the cyber domain.[62] The United Nations Group of Governmental Experts has, for example, affirmed that international law applies to the use of information and communications technologies (ICTs) by states[63] and confirmed that, in their use of ICTs, "[S]tates must observe . . . [the principle of] non-intervention in the internal affairs of other States."[64] In 2016, the General Assembly welcomed these conclusions,[65] and two years later, established an Open-ended Working Group and Group of Governmental Experts to discuss the issues further.[66]

Part of customary international law, the scope and content of the cyber non-intervention rule must be initially determined by an examination of state practice and *opinio juris*.[67] In terms of state practice, the U.S. Council of

---

from military, political, economic or any other form of *coercion* aimed against the political independence or territorial integrity of any State . . . ." (emphasis added).

60. *See* Nicar. v. U.S., 1986 I.C.J. ¶ 249 (confirming that the law on countermeasures applied to the non-intervention principle). Article 22 of the International Law Commission's articles on state responsibility establishes that the "wrongfulness of an act . . . is precluded if and to the extent that the act constitutes a [lawful] countermeasure." G.A. Res. 56/83, annex, Responsibility of States for internationally wrongful acts, art. 22 (Jan. 28, 2002) [hereinafter Responsibility of States].

61. There was some initial (mostly theoretical) debate about whether domestic laws and international law applied to the new domain of "cyberspace", notably in the form of the 1996 Declaration of the Independence of Cyberspace. *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence (discussing the lack of governance in the cyber sphere). States have, perhaps unsurprisingly, concluded that the Internet is not a law-free zone. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 327 (2015).

62. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SEC. L. 211, 221 (2012).

63. Rep. of the Group of Gov. Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Sec., ¶ 19, U.N. Doc. A/68/98 (June 24, 2013).

64. Rep. of the Group of Gov. Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Sec., ¶ 28, UN Doc. A/70/174 (July 22, 2015).

65. G.A. Res. 71/28, Developments in the Field of Information and Telecommunications in the Context of International Security (Dec. 9, 2016), adopted by 181 votes to 0, with 1 abstention.

66. *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. OFF. FOR DISARMAMENT AFF., https://www.un.org/disarmament/ict-security (last visited June 19, 2020).

67. Article 38(1)(b) of the Statute of the International Court of Justice lists as one of the sources of international law, "international custom, as evidence of a general practice accepted as law." To show the existence and content of custom, there must be evidence of a general practice, and evidence of a belief the practice is required by international law (the *opinio juris* element). This two-element approach has

Foreign Relations' Cyber Operations Tracker reports that twenty-eight countries are suspected of sponsoring cyber and influence operations, and that states have begun using sanctions to punish their alleged attacker.[68] There is, however, limited *public* state practice here. No country has accepted responsibility for carrying out a cyber or influence operation, and victim states often do not acknowledge that they have been attacked or invoke the right to engage in countermeasures.[69] On the question of *opinio juris*: Australia,[70] the Netherlands,[71] United Kingdom,[72] and United States[73] have all argued that cyber operations targeting elections are, or should be, violations of the non-intervention rule. Other democratic countries have not taken a public position, despite widespread concern about the dangers to democracy. France, for example, has confirmed the application of the non-intervention principle to the cyber domain but said little else beyond noting that interferences in the political system may constitute a prohibited intervention.[74] President Emmanuel Macron did, however, launch the Paris

been confirmed by the International Court of Justice in North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), Judgment 1969 I.C.J. 3, ¶ 77 (Feb. 20). *See generally* Int'l Law Comm'n, Rep. on the Work of Its Seventieth Session, UN Doc. A/73/10, at 119 (2018) (assessing the identification of customary international law).

68. Digital & Cyberspace Pol'y Program, *Cyber Operations Tracker*, COUNCIL FOREIGN REL., www.cfr.org/interactive/cyber-operations (last visited June 19, 2020).

69. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 586 (2018).

70. *2019 International Law Supplement*, AUSTL.'S INT'L CYBER ENGAGEMENT STRATEGY, https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html (last visited June 19, 2020) ("[T]he use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State . . . would constitute a violation of the principle of non- intervention.").

71. Letter from Stef Blok, Minister of Foreign Affairs, Neth., to the President of the House of Representatives on the Int'l Legal Order in Cyberspace: Appendix: International Law in Cyberspace (July 5, 2019) (on file with the government of the Netherlands) [hereinafter Letter on Int'l Legal Order in Cyberspace] ("Attempts to influence election outcomes via social media are [covered by] the non-intervention principle.").

72. Jeremy Wright, Attorney General QC MP, Cyber and International Law in the 21st Century (May 23, 2018) ("[The] use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state . . . must surely be a breach of the prohibition on intervention in the domestic affairs of states.").

73. In 2016, the U.S. State Department Legal Adviser, Brian Egan argued that "a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention." Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 175 (2017). In 2020, the United States reaffirmed this position, with the Department of Defense General Council saying that "a cyber operation by a State that interferes with another country's ability to hold an election" or that tampers with "another country's election results would be a clear violation of the rule of non-intervention." Paul C. Ney, Jr., DOD General Counsel, Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

74. Przemyslaw Roguski, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*, OPINIO JURIS (Sept. 24, 2019),

Call for Trust and Security in Cyberspace in 2018, which included a recognition of the need for states to "cooperate in order to prevent interference in electoral processes."[75]

Due to the limited evidence of state practice and *opinio juris*, we are left with the ICJ's *Nicaragua* formulation: "Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[76] There is no doubt that the outcome of an election is something that a democratic state should be permitted, by the principle of state sovereignty, to decide freely—subject to applicable human rights laws on political participation.[77] The only question is whether and when cyber and influence operations targeting elections can be categorized as coercive. The answer depends on the interpretation of "coercion",[78] left undefined by the International Court in its 1986 *Nicaragua* judgment.

The rules for the interpretation of unwritten customary international law norms are the same as those governing the written provisions of treaties.[79] The basic approach to the interpretation of treaties is explained in Article 31(1) of the Vienna Convention on the Law of Treaties:[80] "A treaty shall be

---

https://www.opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

75. Ministry for Europe and Foreign Affairs, France, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, FRANCE DIPLOMACY, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (last visited June 19, 2020) (Fr.).

76. Nicar. v. U.S., 1986 I.C.J. ¶ 205.

77. G.A. Res. 217(III)A, Universal Declaration of Human Rights, ¶ 21 U.N. Doc. A/RES/217(III) (Dec. 10, 1948) ("The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."); *see also* International Covenant on Civil and Political Rights, art. 25(b), Dec. 16, 1966, S. Exec. Rep. 102-23, 999 U.N.T.S. 171 ("Every citizen shall have the right and the opportunity . . . To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors . . . .").

78. Matthias Herdegen, *Interpretation in International Law*, *in* MAX PLANCK ENCYCLOPEDIAS OF PUB. INT'L L. ¶ 61, (Rudiger Wolfrum ed., 2012) ("It is evident that customary principles and rules also call for clarification of their scope and legal implications.").

79. *See generally*, Philip Allott, *Interpretation: An Exact Art*, *in* INTERPRETATION IN INTERNATIONAL LAW 373, 384–85 (Andrea Bianchi et al. eds., 2015) (demonstrating how customary international law is normally interpreted); Frederick Schauer, *Pitfalls in the Interpretation of Customary Law*, *in* THE NATURE OF CUSTOMARY LAW: LEGAL, HISTORICAL AND PHILOSOPHICAL PERSPECTIVES 13, 17 (Amanda Perreau-Saussine & James Bernard Murphy eds., 2007) (exploring the interpretive questions facing customary international law); Panos Merkouris, *Interpreting the Customary Rules on Interpretation* 19 INT'L CMTY. L. REV. 126, 137 (2017) (discussing the place of interpretation in the life-cycle of customary international law).

80. Question of the Delimitation of the Continental Shelf Between Nicaragua and Colombia Beyond 200 Nautical Miles from the Nicaraguan Coast (Nicar. v. Colom.), Judgment, 2016 I.C.J 100, ¶ 33 (Mar. 17) (applying Article 31(1)'s general rule of interpretation to a dispute over treaty interpretation).

interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[81] Albert Bleckmann has persuasively argued that the same methodology can be applied to customary norms.[82] The International Court of Justice has followed his general approach.[83]

To establish the meaning of coercion, under the non-intervention principle, we must first look to the ordinary meaning of the term. The *Oxford English Dictionary* defines coercion as the action of "coercing," with coercing understood as "the application of force to control the action of a voluntary agent."[84] Second, we must examine the way the term is used in other areas of international law to ensure consistency. In the law of treaties, a treaty is void if consent has been procured by the coercion of the state, by the threat or use of force,[85] or by the coercion of its representative through acts or threats directed against them.[86] In the law on state responsibility, a state that coerces another state to act is responsible for that act.[87] The International Law Commission describes the coercing state as the "prime mover in respect of the [wrongful] conduct," and the coerced state as "merely

81. Vienna Convention on the Law of Treaties art. 31(1), *opened for signature* May 23, 1969, 1155 U.N.T.S. 331.

82. Albert Bleckmann, *Zur Feststellung and Auslegung von Völkergewohnheitsrecht*, 37 ZAÖERV 504, 526–28 (1977) (Ger.).

83. *See, e.g.,* Frontier Dispute (Burk. Faso v. Mali), Judgement, 1986 I.C.J. 554, ¶ 20 (Dec. 22); Arrest Warrrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), Judgment, 2002 I.C.J. 3, ¶ 53 (Feb. 14); Jurisdictional Immunities of the State (Ger. v. It.: Greece intervening), Judgment 2012 I.C.J. 99, ¶ 57 (Feb. 3). *See generally*, Peter Staubach, *The Interpretation of Unwritten International Law by Domestic Judges*, *in* THE INTERPRETATION OF INTERNATIONAL LAW BY DOMESTIC COURTS 113, 125–26 (Helmut Philipp Aust & Georg Nolte eds., 2016) (examining domestic courts' approaches to customary international law); PETER G. STAUBACH, THE RULE OF UNWRITTEN INTERNATIONAL LAW: CUSTOMARY LAW, GENERAL PRINCIPLES, AND WORLD ORDER 153–54 (1st. ed. 2020) (explaining the continued relevance of customary international law from philosophical and theoretical standpoints).

84. *Coercion*, OXFORD ENGLISH DICTIONARY ONLINE, https://www.oed.com (search "coercion" in search bar).

85. Vienna Convention, *supra* note 81, art. 52. Provides that "a treaty is void if its conclusion has been procured by the threat or use of force in violation of the principles of international law embodied in the Charter of the United Nations." Article 52 has a limited conception of coercion, resulting from "the threat or use of force," although there is some debate as to whether this extends to violations of the non-intervention principle. Olivier Corten, *Article 52*, *in* THE VIENNA CONVENTIONS ON THE LAW OF TREATIES: A COMMENTARY 1201, 1210 (Olivier Corten & Pierre Klein eds., 2011).

86. Vienna Convention *supra* note 81, art. 51. Provides that "the expression of a State's consent to be bound by a treaty which has been procured by the coercion of its representative through acts or threats directed against him shall be without any legal effect." *Y.B. Int'l L. Comm'n*, *supra* note 8, at 246 (explaining that coercion covers "any form of constraint of or threat against a representative.").

87. Responsibility of States, *supra* note 60, art. 18 (stating that "a State which coerces another State to commit an act is internationally responsible for that act if: (a) the act would, but for the coercion, be an internationally wrongful act of the coerced State; and (b) the coercing State does so with knowledge of the circumstances of the act.").

its instrument."[88] Finally, we must account for the object and purpose of the principle of non-intervention, which differentiates between unwelcome interferences by foreign powers and prohibited intermeddling in internal affairs.[89] The ban is on coercive interferences and not interferences *per se*.[90] In other words, the element of coercion establishes a high threshold, requiring evidence of control of the target state by the outside power.

Applying the basic rules for the interpretation of the word coercion provides limited guidance for the application of non-intervention to the cyber domain. The government of the Netherlands explains the point this way:

> The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.[91]

The Dutch government's position makes the point that coercion involves getting the target state to do something that it would not otherwise do voluntarily. But there is no discussion as to how the outside power can get the target to act differently. In other words, there is no detailed explanation of what constitutes coercion.

IV. THE MEANING OF COERCION

To get a deeper and more complete understanding of "coercion," this article turns to philosophical and jurisprudential debates on the notion of coercion in inter-personal relations.[92] There are two reasons for this. First, the same term is used in both the inter-personal context and in international

88. Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, U.N. Doc. A/56/10, at 65 (2001) [hereinafter Draft Articles on Responsibility of States].

89. *See* MOUNTAGUE BERNARD, ON THE PRINCIPLE OF NON-INTERVENTION 7–8 (J. H. & J. Parker eds., 1860) (illustrating the principle of non-intervention). Whilst it may be legitimate for one state to try to influence the decision-making of another, the foreign power cannot attempt to supplant the right of a state to come its own conclusions on questions of internal and external affairs, because this would undermine the sovereignty of the target state.

90. *See* Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 348 (2009) (explaining the concept of interference under the non-intervention principle).

91. Letter on Int'l Legal Order in Cyberspace, *supra* note 71. Australia has adopted a similar position, "[a] prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature)." *2019 International Law Supplement*, *supra* note 70.

92. The focus here is the relationship between voluntary agents—we are not concerned with the exercise of coercive power by the state over its citizens. In this context, the sociologist, Max Weber draws a distinction between physical coercion in the application of the law, involving arrest and detention, etc., and psychological coercion, whereby subjects feel compelled to comply with the law, without formal enforcement. *See* 1 MAX WEBER, ECONOMY AND SOCIETY 34 (G. Roth & C. Wittich trans., Univ. of Cal. Press 1978) (1921).

relations. We see this clearly in Section 2 of the Vienna Convention on the Law of Treaties, which establishes that a treaty is void, if it has been procured by the "coercion of a representative of a state" (Article 51) or by the "coercion of a state" (Article 52). Second, epistemic humility suggests that something might be gained from international lawyers engaging with the cognate disciplines of philosophy and the philosophy of law, where our colleagues have been thinking about the meaning of coercion for more than half a century.

A. Coercive Threats

Coercion is often understood in terms of a coercive threat, typically in the form of "your money, or your life." In his 1969 essay on the subject, the philosopher, Robert Nozick explains that coercion involves a threat by one voluntary agent ("P") to another ("Q") where if Q does not do a certain action ("X"), then deleterious consequences will follow for Q.[93] Coercion involves, then, a self-interested act by P,[94] which is intended to bring about a change in the behaviour of Q, by threatening deleterious consequences for Q.[95] Unlike the certain action (X), it is thus within P's control to ensure the threatened consequences come about. Q is aware of the threat. The threat spurs the change in Q's behaviour. Thus, coercion involves a conscious but unwilling act on the part of the Victim. In the case of the threat by the Robber, the Victim acts consciously when they hand over the cash, in that they know what they are doing, but do so unwillingly.[96]

B. Coercive Force

Nozick's essay triggered a flurry of articles throughout the 1970s and 1980s in the disciplines of philosophy and jurisprudence on the meaning of coercion.[97] While his account focused on coercive threats, where the victim acts for themselves but is not given a meaningful choice, other writers concluded that the term could also be applied to circumstances of physical

93. *See* Robert Nozick, *Coercion*, *in* PHILOSOPHY, SCIENCE, AND METHOD: ESSAYS IN HONOR OF ERNEST NAGEL 440, 441–45 (Sidney Morgenbesser et al. eds., 1969).

94. Threats are distinguished from warnings on the ground that warnings may not be self-interested; or might be advisory; or it might not be within P's power to ensure the deleterious consequences. *Id.* at 444–45.

95. Threats are distinguished from offers on the basis that, although negative consequences might arise in the imagined, unrealized future, if Q does not take up the offer, the consequences are not deleterious compared to the normal or expected course of events (those that would have happened had the offer not been made). *See id*. at 447.

96. *See* H. J. McCloskey, *Coercion: Its Nature and Significance*, 18 S. J. PHIL. 335, 336 (1980) ("When one is coerced, one still acts.").

97. Hiba Hafiz, *Beyond Liberty: Toward a History and Theory of Economic Coercion*, 83 TENN. L. REV. 1071, 1085–86 (2016).

coercion. The philosopher, Michael Bayles, for example, maintains that there is no difference between a situation where someone says "sign this contract, or I will kill you," and where they grab your hand and force your signature.[98] This is echoed in the Vienna Convention on the Law of Treaties, which establishes that the representative of the state can be coerced "through acts or threats directed against him."[99] Oliver Dörr and Kirsten Schmalenbach explain the difference in the Roman law terms of *vis absoluta* (physical coercion), where the representative's hand is held and guided when signing the agreement, and *vis compulsive* (moral coercion), where the representative is blackmailed into signing the treaty.[100] Giovanni Distefano notes that when physical force is used to get someone to sign a treaty, "what is at stake is almost emptying the body of the coerced person of all its free will, and substituting this for another's will."[101]

However, physical force is not coercive simply because P does something to Q.[102] If P pushes Q into the swimming pool, we say that Q has been forced into the water, not that they have been coerced into the pool.[103] Physical force is only coercive where P uses force to get Q *to do something*.[104] Thus, when P pushes Q into the pool, P forces Q into the water, but when P grabs Q's hand and forces them to sign a treaty, then P coerces Q. In other words, we speak about coercion when P exercises power over Q, by getting Q to do something they would not otherwise do.[105]

C. Coercive Manipulation

Coercion is wrong because the Victim is made to do something, without a choice in the matter. A coercive threat, for example, "is designed so that

98. *See* Michael D. Bayles, *A Concept of Coercion*, *in* COERCION: NOMOS XIV 16, 18 (J. Roland Pennock & John W. Chapman eds., 1972); *see also* Martin Gunderson, *Threats and Coercion*, 9 CAN. J. PHIL. 247, 248 (1979).

99. Vienna Convention, *supra* note 81, art. 51.

100. VIENNA CONVENTION ON THE LAW OF TREATIES: A COMMENTARY 862 (Oliver Dörr & Kirsten Schmalenbach eds., 2012); *see also* H.G. de Jong, *Coercion in the Conclusion of Treaties: A Consideration of Articles 51 and 52 of the Convention on the Law of Treaties*, 15 NETH. Y.B. INT'L. L. 209, 224 (1984).

101. Giovanni Distefano, *Article 51*, *in* THE VIENNA CONVENTIONS ON THE LAW OF TREATIES: A COMMENTARY 1179, 1192 (Olivier Corten & Pierre Klein eds., 2011).

102. *See* Craig L. Carr, *Coercion and Freedom*, 25 AM. PHIL. Q. 59, 59 (1988).

103. *See* Peter Westen, *"Freedom" and "Coercion"—Virtue Words and Vice Words*, 1985 DUKE L. J. 541, 565 (1985).

104. *See* Gunderson, *surpa* note 98, at 250 (defining physical coercion in terms of P forcing Q to "do X," so that X "is not an action of Q").

105. *See* Robert A. Dahl, *The Concept of Power*, 2 BEHAV. SCI. 201, 203 (1957).

only one option will be regarded as acceptable."[106] In the case of coercive force, P bypasses Q's decision-making process altogether, using Q as a "mere mechanical instrument."[107] In both cases, P wants Q to do something, and P wants to be certain this will happen. This leaves Q without a meaningful choice in the matter. This can also be done by way of coercive manipulation.[108] In this case, P targets Q's decision-making process,[109] either by changing the information available to Q, or by changing the way that Q responds to existing facts.[110]

There are lots of ways that we can get someone to "decide" to do something they would not otherwise do, and this is not always wrongful. Take the example of a charity worker who elicits a donation by telling a deliberately emotional true story about the child who will be helped by the gift. The relevant issue is, thus, whether we leave the other person with a choice.

To make sense of the notion of coercive manipulation, we must see coercion as part of a spectrum of force. The legal philosopher, Joel Feinberg, explains that there are many ways of getting a person to act but only some can be described as forcing them to act. He explains that the various techniques can be placed on a spectrum of force, running from physical compulsion on one end, to manipulation, persuasion, enticement, and simple requests for action at the other.[111] Thus, if P wants Q to stay in a room, P can: hold the door shut (compulsion), tell Q that, if they leave the room, P will kill them (coercion), tell Q there is a terrorist outside, with a suicide vest, when this is not true (manipulation), tell Q that P will be upset if Q leaves (again, manipulation), tell Q that they will get $1,000, if they stay in the room (enticement), or simply ask Q to stay in the room (request for action). In all cases, P's objective is the same: get Q to stay in the room. The division is between P's actions that leave Q with a meaningful choice, and those that do not.

There is no problem with P getting Q to do something they would not otherwise do by giving them new facts. Thus, if Q refuses to give up smoking tobacco, P can show them graphic photographs of the damage that smoking

106. Grant Lamond, *Coercion and the Nature of Law*, 7 LEGAL THEORY 35, 40 (2001); *see also* ALAN WERTHEIMER, COERCION 172 (1988).

107. E. ALLEN FARNSWORTH, FARNSWORTH ON CONTRACTS § 4.16 (1982).

108. *See* JOSEPH RAZ, THE MORALITY OF FREEDOM 373 (1986); *see also* T. M. Wilkinson, *Nudging and Manipulation*, 61 POL. STUD. 341, 351 (2013).

109. *See* Michael Kligman & Charles M. Culver, *An Analysis of Interpersonal Manipulation*, 17 J. MED. & PHIL. 173, 187 (1992).

110. *See* Gideon Yaffe, *Indoctrination, Coercion, and Freedom of Will*, 67 PHIL. & PHENOMENOLOGICAL RES. 335, 342 (2003).

111. JOEL FEINBERG, HARM TO SELF 189 (1986).

does to a person's lungs. But this is not wrongful, because it does not undermine Q's agency. The constitutional lawyer, Cass Sunstein, notes that an "action does not count as manipulative merely because it is an effort to alter people's behavior."[112] He explains that if P is "just providing the facts," in a sufficiently fair and neutral way, "it is hard to complain of manipulation."[113]

P can also try and change Q's behaviour by warning of deleterious consequences, if Q does not do what P wants. Here, P introduces a new piece of information into Q's decision-making process. For example, P might threaten to give Q the silent treatment if Q refuses to give up smoking.[114] But there is nothing intrinsically wrongful about this. P is a voluntary agent, with the right to have their own views and opinions about Q's behaviours, and P is entitled to impose costs on the voluntary actions of Q. To conclude otherwise would be to require P to accept all the consequences of Q's actions.

P's warnings are only wrongful in terms of the difference between getting someone to act and forcing them to act, where they create a forced choice, leaving Q without a meaningful decision. The philosopher, Joel Rudinow explains the difference in terms of resistible and irresistible incentives, with an irresistible incentive defined as one "that no one could reasonably be expected to resist."[115]

However, this differs from P lying about the facts in order to get Q to do something that they would not otherwise do.[116] A lie is a statement made by someone who does not believe in the truth of the statement, made with the intention that someone else shall be led to believe it.[117] By lying, P deceives Q by changing Q's perception of the true facts of the world and, therefore, changes the basis on which Q makes a decision. Hugo Grotius explains that lying is wrongful because it undermines the right of the target to "liberty of judgment," that is Q's right to come to their own conclusion based on a proper understanding of the facts.[118] All lies are deceptive, in the sense of deceiving the target about the reality of the situation. Recall our

112. Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 215 (2016).

113. *Id.*

114. The silent treatment is a recognized tactic of manipulation, often explained as emotional blackmail. *See generally* David M. Buss et al., *Tactics of Manipulation*, 52 J. PERSONALITY & SOC. PSYCHOL. 1219, 1221 (1987).

115. Joel Rudinow, *Manipulation*, 88 ETHICS 338, 341(1978).

116. *See* Patrick Todd, *Manipulation*, *in* THE INTERNATIONAL ENCYCLOPEDIA OF ETHICS 3139, 3139 (Hugh LaFollete ed., 2013).

117. ARNOLD ISENBERG, *Deontology and the Ethics of Lying*, *in* AESTHETICS AND THEORY OF CRITICISM: SELECTED ESSAYS OF ARNOLD ISENBERG 245, 249 (William Callaghan et al. eds., 1973).

118. HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE, INCLUDING THE LAW OF NATURE AND OF NATIONS bk. III, ch. I § XI (Walter Dunne 1901) (1625).

example of P getting Q to stay in the room by saying, "do not go outside, there is a terrorist, with a suicide vest." If Q believes the lie, Q will be certain to stay in the room: Q will have been made to do something they would not otherwise have done, and they will have been given no choice in the matter. In these circumstances, lying is the functional equivalent of coercion,[119] because "[b]oth are ways of exerting control over the victim."[120]

Another way that P can gain power over Q is by undermining Q's faith in their ability to make their own decisions. This can be done by constantly lying to Q, through blatant denials of things which are true, or by telling Q they are imagining things. This is often described in the literature as gaslighting,[121] which is the functional equivalent of coercion. With gaslighting, P exercises control over Q by undermining Q's confidence in their capacity to decide things for themselves, so that Q comes to rely on P and, therefore, does what P wants.[122]

P can also look to gain control over Q through the systematic infliction of physical violence and psychological trauma, with the objective of destroying Q's "sense of self" in relation to others.[123] The result is often that P can get Q to do what P wants, without the constant need for the threat or use of physical violence so that, for example, Q appears to outsiders to be acting on their own accord.[124] This can be seen in the practice of brainwashing, also known as coercive persuasion.[125] Brainwashing describes a deliberate attempt to change what a person thinks by imposing an exacting

119. Allen W. Wood, *Coercion, Manipulation, Exploitation*, *in* MANIPULATION: THEORY AND PRACTICE 17, 35 (Christian Coons & Michael Weber eds., 2014) ("Deception by *flat-out lying* . . . feeds the person false information, on the basis of which he makes choices the person presumably might not have made if he had known the truth." (emphasis in original)).

120. David A. Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334, 354 (1991); *see also* SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 22 (1999) ("Deception, then, can be coercive. When it succeeds, it can give power to the deceiver . . . .").

121. The expression "gaslighting" was taken from Patrick Hamilton's 1938 play, *Gas Light*, later made into a film starring Ingrid Bergman, which tells the story of a man intent on convincing his wife she is insane, so that she will be hospitalized and he can gain access to her jewels.

122. *See* Kate Abramson, *Turning Up the Lights on Gaslighting*, 28 ETHICS 1, 2 (2014).

123. JUDITH LEWIS HERMAN, TRAUMA AND RECOVERY 77 (1992). The phenomenon has been observed in prisoners of war, in political prisoners, hostages, and victims of human trafficking. In the case of domestic violence, the term "coercive control" is often applied. Evan Stark has successfully argued that the notion of coercive control can be extended to intimate partner relationships, because the objective is to achieve power over another person. EVAN STARK, COERCIVE CONTROL: HOW MEN ENTRAP WOMEN IN PERSONAL LIFE 370 (2007). Coercive control has been criminalized in a few jurisdictions. Serious Crime Act 2015 § 76(1) (Eng.); Domestic Violence Act 2018 § 39(1) (Act No. 6/2018) (Ir.); Domestic Abuse (Scotland) Act 2018, (ASP 5) § 1, ¶ 2.

124. *See* Elizabeth Hopper & José Hidalgo, *Invisible Chains: Psychological Coercion of Human Trafficking Victims*, 1 INTERCULTURAL HUM. RTS. L. REV. 185, 209 (2006).

125. EDGAR H. SCHEIN, COERCIVE PERSUASION: A SOCIO-PSYCHOLOGICAL ANALYSIS OF THE "BRAINWASHING" OF AMERICAN CIVILIAN PRISONERS BY THE CHINESE COMMUNISTS 18 (1971).

regime requiring absolute obedience with severe physical and psychological punishments for non-compliance.[126] The term was coined by Edward Hunter in 1950,[127] and it was used to explain the fact that some American troops captured in the Korean War returned from prisoner-of-war camps as apparently committed communists, "ready to denounce their country of birth and sing the praises of the Maoist way of life."[128] In the 1958 draft of what became Article 51 of the Vienna Convention on the Law of Treaties ("coercion of a representative of a state"), the International Law Commission's Special Rapporteur, Gerald Fitzmaurice, explained that the notion of coercion included "certain modern methods of compulsion summed up by the term 'brainwashing.'"[129]

V. THE COERCIVENESS OF CYBER AND INFLUENCE OPERATIONS

The philosopher, Scott Anderson, explains that coercion is commonly understood as "a use of a certain kind of power for the purpose of gaining advantages over others . . . and imposing one's will on the will of other agents."[130] We have seen, in the previous section, that one person can gain power and control over another through the deployment of coercive threats, the use of coercive force, and through coercive manipulation targeting the decision-making process. The notion of "coercion" can, then, be formulated in the following way: (1) P wants Q to do something and wants to be certain that this will happen–this second element distinguishes efforts to exercise power from mere influence; (2) P then takes some action to get Q to do that something, either by uttering a coercive threat, using coercive force, or engaging in coercive manipulation; and (3) because of P's actions, Q does that something.

We also must be clear about the difference between "coercion" and "coercive behaviour." When the Robber says to the Victim, "your money, or

126. *Brainwashing*, ENCYCLOPÆDIA BRITANNICA, https://www.britannica.com/topic/brainwashing (last visited June 19, 2020). For a (critical) introduction to the "dubious psychological syndrome" of brainwashing, *see* James T. Richardson, *Brainwashing as Forensic Evidence*, *in* HANDBOOK OF FORENSIC SOCIOLOGY AND PSYCHOLOGY 77 (Stephen J. Morewitz & Mark L. Goldstein eds., 2014). Brainwashing is sometimes pleaded as a defense in domestic criminal cases, most notably, in the prosecution of the heiress Patty Hearst for joining her kidnappers in a bank robbery. *See* Joshua Dressler, *Professor Delgado's "Brainwashing" Defense: Courting a Determinist Legal System*, 63 MINN. L. REV. 335 (1979).

127. Edward Hunter, *Author and Expert On 'Brainwashing,'* N.Y. TIMES, June 25, 1978, at 28.

128. KATHLEEN TAYLOR, BRAINWASHING: THE SCIENCE OF THOUGHT CONTROL 3 (2d. ed. 2017).

129. G.G. Fitzmaurice (Special Rapporteur), *Third Report on the Law of Treaties*, 2 Y.B. Int'l L. Comm'n 58, U.N. Doc. A/CN.4/115 (1958).

130. Scott Anderson, *Coercion*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY § 1 (Edward N. Zalta ed., 2017), https://plato.stanford.edu/archives/win2017/entries/coercion.

your life," and the Victim hands over the cash, we have all three elements of coercion. But, even if the efforts of the Robber are not successful, it is coercive behaviour[131] where an action was "*intended* to force someone to do something."[132] In other words, only the first two elements of coercion constitute coercive behavior, i.e., where (1) P wants Q to do something and wants to be certain that this will happen; and (2) P then takes some action to get Q to do that something. But how can we know P's intentions given the impossibility of knowing with certainty the motivations of others? The simple answer is that we cannot, but voluntary actions are presumably motivated. In the case of the utterance, "your money or your life," the Robber's presumed intention is to get the Victim to give them the cash. Otherwise, why would the Robber choose this formulation of words?

The difference between coercion and coercive behaviour is important to the non-intervention principle because the International Court of Justice in the *Nicaragua* case was not concerned with the success of the United States' conduct. The ICJ determined that "intervention is wrongful when it uses *methods of coercion*",[133] and that where a state "*with a view to the coercion* of another state, supports [an insurrectionist group], that amounts to an intervention."[134] A violation of the non-intervention rule does not, then, require evidence of a successful interference. Evidence that a foreign power[135] intended to interfere decisively in the internal political affairs of the target state is sufficient. With respect to election interference, given the expenditure of time, money and the risk of condemnation if discovered, it is implausible to conclude that a foreign state would hack the ICTs used in an election, or engage in a sustained influence operation, for any reason other than to decisively influence the outcome of the vote.

The following sections apply this understanding of the notion of coercion and the related concept of coercive behaviour, what the ICJ refers to as "methods of coercion,"[136] to the problem of foreign state cyber and influence operations targeting elections, to explain the content of the non-intervention principle in this context.

---

131. Grant Lamond, *Coercion*, *in* INTERNATIONAL ENCYCLOPEDIA OF ETHICS 840, 841 (Hugh Lafollette ed., 2013).

132. Grant Lamond, *The Coerciveness of Law*, 20 OXFORD J. LEGAL STUD. 39, 52 (2000).

133. Nicar. v. U.S., 1986 I.C.J., ¶ 205 (emphasis added).

134. *Id.* ¶¶ 241, 292.

135. On the problems created by the architecture of the Internet for the factual attribution of state responsibility, *see generally* Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229 (2012); *see also* Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 INT'L & COMP. L. Q. 643 (2018) (arguing due diligence should be a secondary rule of international law in the realm of cyber security).

136. Nicar. v. U.S., 1986 I.C.J., ¶ 205.

A. Cyber Threats

The standard notion of coercion, which is of a coercive threat ("your money, or your life"), can be applied to international relations where an outside power makes a demand that leaves the target without a meaningful choice. For example, if a foreign power threatened a military invasion if the population voted a certain way in an election,[137] this constitutes a coercive threat, and consequently, violates the non-intervention rule.

Coercion establishes the dividing line between the unwelcome deployment of diplomatic, political, and economic pressure[138] and unlawful intervention. Thus, when President Barack Obama asked the British public to vote against Brexit in the 2016 referendum, warning that the United Kingdom would be at the "back of the queue" in any trade deal with the U.S. if the U.K. chose to leave the European Union,[139] this was an interference in domestic political affairs. However, he did not violate the non-intervention principle: it was not a threat that the electorate could not reasonably ignore. Warning of deleterious consequences is not by itself unlawful, provided that the targeted government or population remains free to make its own decision, which includes awareness of the position of the foreign power.[140]

Express threats to the electorate or the political class in the target state can obviously be made via social media.[141] New information and communications technologies also allow for the delivery of implied threats. In 2007, a distributed denial of service (DDoS) attack on Estonia caused the websites of the President, Prime Minister and Parliament, amongst others, to crash, resulting in massive disruption to the political system. The attack

---

137. The *New York Times* reported that, in 1996, "China fired missiles toward Taiwan in the days before the island's first democratic presidential election in an attempt to intimidate voters from casting ballots for the democratic reformer Lee Teng-hui." Chris Horton, *Specter of Meddling by Beijing Looms Over Taiwan's Elections*, N.Y. TIMES (Nov. 22, 2018), https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html; *see also* Danny Gittings, *China Threatens to Attack Taiwan*, GUARDIAN (Feb. 22, 2000, 10:07 AM), https://www.theguardian.com/world/2000/feb/22/china.

138. *See* Quincy Wright, *Subversive Intervention*, 54 AM. J. INT'L L. 521, 532 (1960). Others take a different view, for example, Maziar Jamnejad and Michael Wood conclude that intervention covers any situation "where one state becomes involved in the internal political processes of another." Jamnejad & Wood, *supra* note 90, at 368.

139. Anushka Asthana & Rowena Mason, *Barack Obama: Brexit would put UK 'Back of the Queue' for Trade Talks*, GUARDIAN (Apr. 22, 2016, 3:30 PM), https://www.theguardian.com/politics/2016/apr/22/barack-obama-brexit-uk-back-of-queue-for-trade-talks.

140. *See US Warns Turkey over Russian S-400 Missile System Deal*, BBC (Apr. 4, 2019), https://www.bbc.com/news/world-us-canada-47809827.

141. U.S. President Trump using his twitter account to warn Iran of "consequences the likes of which few throughout history have ever suffered" if the leadership in Iran continued to threaten the United States. Austin Ramzy, *Trump Threatens Iran on Twitter, Warning Rouhani of Dire 'Consequences,'* N.Y. TIMES (July 22, 2018), https://www.nytimes.com/2018/07/22/world/middleeast/trump-threatens-iran-twitter.html.

began after the Estonian government decided to relocate the statue of the Bronze Soldier, which represents the Soviet Union's victory over Nazism–a move that incensed Russia.[142] There is an agreement in the literature that, if Russia was responsible, the DDoS attack would amount to a prohibited intervention,[143] a coercive cyber threat in the form "Do not relocate the Bronze Soldier, or else."[144] But it is important to recall that Estonia did move the statue in the face of strong Russian protests.[145] In other words, this failed attempt to intervene in domestic political affairs was still categorized as coercive—and a violation of the non-intervention rule—because the *intention* was to get the Estonian government not to do something it would otherwise have done.

B. Cyber Power

The term coercion describes a situation in which State P gets State Q to do something that Q would not otherwise do. One way this can be done is by using force. In its 1986 *Nicaragua* judgment, the International Court of Justice confirmed that "the element of coercion . . . is particularly obvious in the case of an intervention which uses force."[146] However, intervention is not solely concerned with the use of force. Where this is the case, the International Court of Justice uses the language of "use of force" and "violations of sovereignty."[147] The principle of non-intervention also protects the target state from being *made to do something* by the outside power.[148] In the *Nicaragua* case, the the U.S. was trying to "coerce the

142. *See* Adrian Blomfield, *War of Words over Bronze Soldier*, TELEGRAPH (Feb. 5, 2007, 12:01 AM), https://www.telegraph.co.uk/news/worldnews/1541641/War-of-words-over-bronze-soldier.html; *see also* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC (Apr. 27, 2017), https://www.bbc.com/news/39655415.

143. *See* Buchan, *supra* note 62; *see also* William Mattessich, *Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage*, 54 COLUM. J. TRANSNAT'L L. 873, 881 (2016).

144. Nicholas Tsagourias explains the point this way: "To the extent that they were intended to put such pressure on Estonia to change its decision . . . they would constitute prohibited intervention." Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 45, 48 (Dennis Broeders & Bibi van den Berg eds., 2020).

145. *See* Steven Lee Myers, *Russia Rebukes Estonia for Moving Soviet Statue*, N.Y. TIMES (Apr. 27, 2007), https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html.

146. Nicar. v. U.S., 1986 I.C.J., ¶ 205.

147. *Id.* ¶ 251 ("[D]irect attacks . . . not only amount to an unlawful use of force, but also constitute infringements of the territorial sovereignty of Nicaragua.").

148. It is therefore wrong to see non-intervention as one part of a hierarchy, with the use of force "above the threshold" and non-intervention "below." The notion of a threshold implies that the crucial distinction is the amount of pressure involved, but this is a mistaken view, as Ellery Stowell pointed out in 1921: "[To] make the actual employment of force the criterion of interference. . . . [i]s to confuse the means with the purpose." STOWELL, *supra* note 42, at 319 n.48. The crucial difference is that, in the case

government of Nicaragua into the acceptance of United States policies and political demands."[149]

The political scientist, Joseph Nye, pointed out that cyber power creates new opportunities for states to get other countries to do something they would not otherwise do, through their information and communications technologies.[150] This kind of cyber operation is coercive in the same way that grabbing the hand of a state's representative and forcing them to sign a treaty is coercive. The outside power forces the target state to do something, leaving them with no choice. To illustrate:

> State P hacks the Electoral Commission's computer in State Q, so that State P's preferred candidate is (wrongly) declared President.

Without outside interference, the population in State Q will decide on their President, and the votes will be counted fairly by the Electoral Commission, which will then declare the winner. State P wants the Electoral Commission to declare its preferred candidate the winner. State P then hacks the Electoral Commission's computer and changes the electoral result. When the Commission (wrongly) declares P's preferred candidate the winner, the government body will have done something that it would not have done without P's involvement, without any choice in the matter. State P's cyber operation therefore violates the non-intervention rule. Furthermore, the operation's scale is irrelevant. Even the insertion of a few bits of data into a software program constitutes coercion, because it involves forcing the target to do something it would not otherwise do.

Cyber operations targeting the underlying ICTs used in elections, whether successful, or not, constitute prohibited interventions in internal affairs, because the foreign power acts with the intention of forcing the underlying technical infrastructure of the target state to do something (by taking control of its ICTs), or to not do something (by disabling its computers, computer networks, and websites), treating the government institution responsible for the conduct of the election as a "mere mechanical instrument"[151] of the outside power.

---

of use of force, the target state is acted upon; in the case of intervention, the outside state achieves its objectives by *working through* the target state. This distinction was recognized in 1922 by Percy Winfield, who explained that the objective of intervention was not "the infliction of a blow upon the resources of a state, but the usurpation of some part of its powers of government." Winfield, *supra* note 39, at 142.

149. Nicar. v. U.S., 1986 I.C.J., ¶ 239.

150. *See* Joseph S. Nye, Jr., *Cyber Power*, BELFER CTR. SCI. & INT'L AFF. 7 (2010), available at belfercenter.org/sites/default/files/files/publication/cyber-power.pdf.

151. On the notion that the coerced state is the "mere instrument" of the outside power. *See* Draft Articles on Responsibility of States, *supra* note 88; FARNSWORTH, *supra* note 107, at § 4.16.

C. Cyber Influence Operations

Cyber influence operations represent a new form of inter-state propaganda.[152] One feature of the Internet is that it allows foreign powers to directly influence political discussions in other states, by making news stories, opinion pieces, and other forms of communication publicly available on websites and social media. Influence operations are wrongful, under international law, when they fall under a proscribed category of communication, notably the prohibition on subversive propaganda,[153] or the influence operation uses, in the words of the *Nicaragua* judgment, "methods of coercion in regard to such choices, which must remain free ones."[154] There is no doubt that an election concerns a choice that should remain free. The only question is whether cyber influence operations can be categorized as coercive.

1. Information Campaigns

There is widespread agreement in the literature that providing the citizens of another country with factual information, including information critical of the government of that state,[155] does not constitute a prohibited intervention.[156] Genuine news broadcasts by state-owned and state-controlled media do not necessarily fall within the definition of unlawful propaganda, "for news broadcasts are the transmission of facts." The same holds for commentaries on the news, defined as "an intellectual appraisal or

152. John Martin explains that propaganda involves "a systematic attempt through mass communications to influence the thinking and thereby the behavior of people." L. JOHN MARTIN, INTERNATIONAL PROPAGANDA: ITS LEGAL AND DIPLOMATIC CONTROL 12 (1958). He makes the point that inter-state propaganda "involves appealing to the masses, as opposed to governments." *Id.* at 16.

153. The prohibition on subversive propaganda is "a deep-rooted principle of customary international law." Eric de Brabandere, *Propaganda*, *in* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L. para. 13 (2012). *See*, H. Lauterpacht, *Revolutionary Propaganda by Governments*, 13 TRANSACTIONS GROTIUS SOC'Y 143, 146 (1927); John B. Whitton, *Propaganda and International Law*, 72 COLLECTED COURSES HAGUE ACAD. INT'L L. 542, 582–83 (1948). The prohibition establishes a limited, albeit absolute, prohibition on inter-state propaganda that calls on the population to reject an established sovereign authority. *See*, for example, the 1970 Declaration on Friendly Relations, *supra* note 53, which provides that no State shall organize "subversive . . . activities directed towards the violent overthrow of the regime of another State."

154. Nicar. v. U.S., 1986 I.C.J., ¶ 205. *See*, on this point, Richard A. Falk, *The United States and the Doctrine of Nonintervention in the Internal Affairs of Independent States*, 5 HOW. L. J. 163, 186 (1959).

155. *See* Philip Kunig, *Intervention, Prohibition of*, *in* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L. para. 24 (2008).

156. Eric de Brabandere explains that propaganda is a method of communication "aimed at influencing and manipulating the behaviour of people in a certain predefined way. The element of influenc[e] and manipula[tion] is at the centre of the concept [of propaganda] and distinguishes it from mere factual information." Brabandere, *supra* note 153, at para. 1.

evaluation, . . . founded upon facts, . . . [and] the result of honest opinion."[157] In the same way that attempting to influence another person by "just providing the facts" is not wrongful,[158] efforts by one state to influence the population of another by providing factual information and commenting on news stories is not prohibited under international law.[159]

The general rule that providing facts does not violate the non-intervention rule applies to the practice of "doxfare." Doxfare involves the hacking of private computer systems and putting any sensitive information obtained into the public domain, with the intention of influencing the internal affairs of another state.[160] The best known example is the DNC-hack, which occurred during the 2016 U.S. presidential election.[161] The practice was also seen in the 2017 French presidential election when emails from Emmanuel Macron's campaign were leaked onto the web,[162] and there have been major

157. ANN VAN WYNEN THOMAS & A. J. THOMAS JR., NON-INTERVENTION: THE LAW AND ITS IMPORT IN THE AMERICAS 291 (1956).

158. *See* Sunstein, *supra* note 112.

159. When we speak about "factual information", we are concerned with things that are actually the case, i.e. things that correspond to the "truth." The meaning of "truth" has been debated in philosophy for hundreds of years, and there is much discussion today about the notion of "post-truth." All of this is beyond the scope of this paper.

160. Kilovaty, *supra* note 10, at 152–53. Kilovaty's position is clearly normative, making the case that "international law *should* adapt to the digital era's threats." *Id.* at 147 (emphasis added).

161. On the international law applicable to the "DNC hack", *see* Logan Hamilton, *Beyond Ballot-Stuffing: Current Gaps in International Law Regarding Foreign State Hacking to Influence a Foreign Election*, 35 WIS. INT'L L. J. 179 (2017); *see also* Duncan B. Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, OPINIOJURIS (July 25, 2016), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/.

162. Andy Greenberg, *The NSA Confirms It: Russia Hacked French Election 'Infrastructure'*, WIRED (Sept. 5, 2017, 12:36 PM), https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/. The outgoing President, François Hollande "openly warned Russia to let up its attacks on the Macron campaign . . . ." ERIK BRATTBERG & TIM MAURER, CARNEGIE ENDOWMENT FOR INT'L PEACE, RUSSIAN ELECTION INTERFERENCE: EUROPE'S COUNTER TO FAKE NEWS AND CYBER ATTACKS 11 (2018), *available at* https://carnegieendowment.org/files/CP_333_Brattberg_Maurer_Russia_Elections_Interference_Brief_FINAL.pdf. Whether Russia was responsible is unclear. *See* LAURA GALANTE & SHAUN EE, ATLANTIC COUNCIL, DEFINING RUSSIAN ELECTION INTERFERENCE: AN ANALYSIS OF SELECT 2014 TO 2018 CYBER ENABLED INCIDENTS 12 (2018), *available at* https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf.

data hacks of politicians in Australia,[163] Cambodia,[164] and Germany.[165] Angela Merkel, Chancellor of Germany, threatened Russia with "consequences" if it happened again.[166] There is no question that doxfare raises issues around data protection and the privacy rights of individuals, but it is difficult to see how it can be categorized as a prohibited intervention because the objective is to place *factual* information in the public domain. Consequently, unless we can show the existence of some international law equivalent to the fruit of the poisonous tree rule in U.S. criminal law (which excludes the admission into court of evidence obtained through illegal means), doxfare is not a violation of the principle of non-intervention, because "just providing the facts" is not prohibited although the facts are unlawfully obtained.

There is one exception to the general rule that "just providing the facts" is not unlawful: that is where the outside power inundates the information environment in the target state with a single political narrative, drowning out all other voices. Elections require citizens to choose between different political options. Where one actor (normally the domestic government) ensures that citizens hear only one side of the argument, people are left without a proper choice when voting, because there will seem to be only one viable option. This is wrongful, even if the communications are factually accurate, or reflect genuinely held positions. In his major study on *The International Law of Propaganda*, first published in 1968, Bhagevatula Satyanarayana Murty explains that government propaganda is coercive when it exerts strong psychological pressure on the population to adopt a position. Whereas attempts at persuasion leave the citizen with several options, "coercion may be said to have been exercised when a person is subjected to a high degree of constraint in the choice of alternatives in shaping his conduct."[167]

Before the Internet, it was almost impossible for an outside power to overwhelm the information environment of another country. This remains

163. Michael Jensen, *We've Been Hacked—So Will the Data be Weaponised to Influence Election 2019? Here's What to Look for*, CONVERSATION (Feb. 21, 2019, 4:54 PM), https://theconversation.com/weve-been-hacked-so-will-the-data-be-weaponised-to-influence-election-2019-heres-what-to-look-for-112130.

164. Yuichiro Kanematsu, *Fears of Chinese Cybermeddling Grow After Cambodia Election*, NIKKEI (Aug. 18, 2018, 6:01 AM), https://asia.nikkei.com/Politics/International-relations/Fears-of-Chinese-cybermeddling-grow-after-Cambodia-election.

165. Janosch Delcker, *Germany Whacked by Big Data Hack*, POLITICO (Jan. 4, 2019, 5:09 PM), https://www.politico.eu/article/germany-data-hack-merkel-whacked/.

166. Oliver Moody, *Merkel Anger over Russian Hacking*, TIMES (May 14, 2020, 12:01 AM), https://www.thetimes.co.uk/article/merkel-anger-over-russian-hacking-lkhwnn05w.

167. B.S. MURTY, THE INTERNATIONAL LAW OF PROPAGANDA: THE IDEOLOGICAL INSTRUMENT AND WORLD PUBLIC ORDER 28 (1989).

largely the case today. But as more people get their news and commentaries from social media, the dangers of a foreign power inundating the information environment with a single political narrative increase. The *Washington Post* reports, for example, that, during Taiwan's 2018 local elections, "citizens were bombarded with anti-[Government] content through Facebook, Twitter and online chat groups . . . ."[168] The presumed objective of the People's Republic of China, the assumed source of the information operation, was to undermine the governing Democratic Progressive Party, which supports Taiwanese independence from mainland China.[169] Each individual communication might fall into the category of factual information or fair comment. But bombarding citizens with news stories and commentaries to develop a dominant political narrative violates the non-intervention rule, where the objective is to drown out all other voices, and therefore constrain the choices available to voters.

2. Lies and Deception: Fake News

Although influence operations can involve the dissemination of factual information, the primary concern is fake news.[170] According to a common definition, "fake news items are lies– that is, deliberately false factual statements, distributed via news channels."[171] In other words, fake news mimics the traditional news media, but lacks its commitment to accuracy.[172] Although the main worry is the dissemination by domestic actors, states have also expressed concern about foreign powers spreading deliberately false news stories in order to disrupt the functioning of democracy.[173] For example, the British Prime Minister, Theresa May complained in 2017 that

168. Josh Rogin, *China's Interference in the 2018 Elections Succeeded—In Taiwan*, WASH. POST (Dec. 18, 2018, 8:25 AM), https://www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan/.

169. Horton, *supra* note 137.

170. *See* SAMANTHA BRADSHAW & PHILIP N. HOWARD, OXFORD, CHALLENGING TRUTH AND TRUST: A GLOBAL INVENTORY OF ORGANIZED SOCIAL MEDIA MANIPULATION 6 (2018). Studies have shown that people often struggle to distinguish fact from fiction on the Internet and in social media. Anthony J. Gaughan, *Illiberal Democracy: The Toxic Mix of Fake News, Hyperpolarization, and Partisan Election Administration*, 12 DUKE J. CONST. L. & PUB. POL'Y 57, 66 (2017).

171. Björnstjern Baade, *Fake News and International Law*, 29 EUR. J. INT'L L. 1357, 1358 (2019).

172. David M. J. Lazer et al., *The Science of Fake News: Addressing Fake News Requires a Multidisciplinary Effort*, 359 SCI. MAG. 1094, 1094 (Mar. 9, 2018).

173. The use of "bots"—short for "robots," software applications that pretend to be human and reproduce content in social media on a massive scale—ensures that fake news spreads quickly. The head of the U.K.'s domestic counter-intelligence and security agency complained that, "[a]ge-old attempts at covert influence and propaganda have been supercharged in online disinformation, which can be churned out at massive scale and little cost." Andrew Parker, MI5 Director General, U.K., Speech to BFV Symposium in Berlin (May 14, 2018), www.mi5.gov.uk/news/director-general-andrew-parker-speech-to-bfv-symposium.

Russia was "seeking to weaponize information[,] [d]eploying its state-run media organisations to plant fake stories and photo-shopped images in an attempt to sow discord in the West and undermine our institutions."[174]

Fake news does not, by definition, enjoy the protection accorded to factual information under the principle of non-intervention, but there is no specific prohibition on fake news.[175] Fake news is therefore only wrongful when it can be categorized as coercive. Coercion, as we have seen, describes a situation in which State P forces the government or citizens in State Q to do something they would not otherwise do. One way this can be done is by disseminating fake news, that is by lying with the intention of deceiving the target into thinking and acting differently.[176] Take the following hypothetical example:[177]

> During a presidential election campaign in State Q, the intelligence agency in State P creates and then releases on the Internet a fake video that appears to show, in convincing detail, the sitting President Jones engaged in sexual acts with a child.

To get the population in State Q to vote for someone other than Jones, State P releases the deep fake[178] that shows President Jones doing something he never did. We have seen that all lies are deceptive, in the sense of deceiving the target about the reality of the situation, but some lies are intentionally structured so that they lack any choice as to what to think, and therefore what to do. If the electorate votes for a different candidate because of the video, citizens will have been deceived into doing something they would not otherwise have done. Moreover, they will have been given no meaningful choice, because they were given a false perception of Jones.

When evaluating the coerciveness of a fake news story attributable to a foreign power, we must ask two questions: (1) Was the message communicated with the intention of deceiving the target audience into

---

174. Theresa May, Prime Minister, U.K., Speech to the Lord Mayor's Banquet 2017 (Nov. 13, 2017), www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

175. The 1981 General Assembly Declaration on the Inadmissibility of Intervention includes an obligation for states "to combat . . . the dissemination of false or distorted news which can be interpreted as interference in the internal affairs of other States . . ." G.A. Res. 36/103, *supra* note 54, ¶ 2(III)(d). Because the Declaration was adopted by 120 votes to 22, following opposition by Western states, it is not generally regarded as reflecting customary international law.

176. Björnstjern Baade explains that fake news, in the strict sense of a false news item, which is intentionally fabricated, is "coercive," because "the projection of a different set of facts constrains one's freedom to act by making certain options and conclusions no longer seem viable or making others seem mandatory." Baade, *supra* note 171, at 1364.

177. On the practice of releasing deep fake sex tapes, *see generally* Ben Collins, *Russia-Linked Account Pushed Fake Hillary Clinton Sex Video*, NBC NEWS, (Apr. 11, 2018, 4:49 PM), https://www.nbcnews.com/tech/security/russia-linked-account-pushed-fake-hillary-clinton-sex-video-n864871.

178. On "deep fakes" *see generally*, Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019).

believing a falsehood?[179] (2) Would a reasonable observer judge that the communication was intended to influence the target's decision-making to such an extent that they would be left without a meaningful choice about what to think, and therefore what to do? If the answer to both is in the affirmative, the communication violates the principle of non-intervention. Consider two of the best known lies told during the 2016 U.S. presidential election: that "Hillary Clinton [was] in very poor health due to a serious illness," and that "Pope Francis [had] endorsed Donald Trump for president."[180] The first lie would be one intended to get voters to question Clinton's fitness for office, but it is difficult to conclude that the second, concerning papal endorsement, was meant to play a decisive role in the electorate's decision-making. In other words, the invented claim concerning Clinton's health–if attributable to a foreign power–would violate the non-intervention rule, whereas the false reporting of the Pope's views would not.

3. Disinformation Campaigns

The basic political question in any democracy is: what should we do? This is answered by a general election or referendum, and by the governing political class—those involved in making political decisions—at other times, with a recognition of the importance of maintaining the support of the electorate for policy positions. Political will-formation depends on the availability of reliable information, and the capacity of the public and the political class to deliberate and decide on the best course of action. Fake news feeds false information, in order to get them to act differently. Disinformation campaigns also rely on fabricated information,[181] but the objective is to undermine the capacity of the population or the political class to make decisions in their own interests.

Disinformation is misleading information that is likely to create false beliefs, where it is "*no accident* that it is misleading."[182] Similar to lying, disinformation involves a deliberate attempt to mislead, but in the case of

179. Hugo Grotius defines lying as:

> [T]he known and deliberate utterance of any thing contrary to our real conviction, intention, and understanding. . . . [T]he propagation of a truth, which any one believes to be false, in him amounts to a lie. There must be in the use of the words therefore an intention to deceive, in order to constitute a falsehood in the proper and common acceptation.

HUGO GROTIUS, *supra* note 118, at bk. III, ch. I, § X (emphasis in original).

180. Richard Gunther et al., *Trump May Owe His 2016 Victory to 'Fake News,' New Study Suggests*, CONVERSATION (Feb. 15, 2018, 6:34 AM), https://theconversation.com/trump-may-owe-his-2016-victory-to-fake-news-new-study-suggests-91538.

181. *See generally*, Henning Lahmann, *Information Operations and the Question of Illegitimate Interference Under International Law*, 53(2) ISR. L. REV. 189 (2020) (examining state-led information campaigns designed to undermine democratic decision-making processes in other states).

182. Don Fallis, *What Is Disinformation?*, 63 LIBR. TRENDS 401, 406 (2015) (emphasis added).

disinformation the objectives and goals are "often political."[183] The most widely cited example of a disinformation campaign is the 2016 "Our Lisa" case in Germany, involving the dissemination of the untrue story about the abduction and rape of an underage Russian-German girl by Arab migrants.[184] The security expert, Constanze Stelzenmüller, explains that the widespread reporting of the story on social media by Russian actors was intended "to sow confusion, doubt, and distrust."[185] This was part of a wider influence campaign by Russia, intended to undermine the confidence of German citizens, including the three million ethnic Russian-German minority,[186] in the leadership of the Chancellor, Angela Merkel, regarding her stance on Russia's interventions in Crimea and eastern Ukraine.[187]

The objectives of a disinformation campaign are to create decision-making paralysis and/or to shift the policy position of the target so it comes to align with the interests of the foreign power. Decision-making paralysis is achieved by creating confusion about the facts of the situation and undermining confidence in the capacity of the democratic system to deliver the best policy outcomes. The outside power can then feed information and disinformation into the political debate in order to get the target population or political class to move themselves to a policy position that aligns with the interests of the outside power.[188] This is described in the literature in terms of reflexive control.[189]

---

183. James H. Fetzer, *Disinformation: The Use of False Information*, 14 MINDS & MACH. 231, 232 (2004). On "disinformation" *see generally*, W. Lance Bennett & Steven Livingston, *The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions*, 33 EUR. J. COMM. 122 (2018) (discussing recent disinformation campaigns meant to disrupt the normal political order); L. John Martin, *Disinformation: An Instrumentality in the Propaganda Arsenal*, 2 POL. COMM. 47 (1982) (providing a Cold War perspective distinguishing disinformation from run-of-the-mill propaganda).

184. Stefan Meister, *The "Lisa Case": Germany as a Target of Russian Disinformation*, NATO REV. (July 25, 2016), https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

185. *The Impact of Russian Interference on Germany's 2017 Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 44 (2017) (statement of Constanze Stelzenmüller, Fellow, Royal Swedish Academy for War Sciences).

186. The target of a disinformation campaign can be the entire population, or one section, exploiting divisions in society. The resulting lack of political cohesion can make it difficult for a democratic government to act. *See* MARTIN MOORE, DEMOCRACY HACKED: POLITICAL TURMOIL AND INFORMATION WARFARE IN THE DIGITAL AGE 80 (2018).

187. *See* Kaan Sahin, *Germany Confronts Russian Hybrid Warfare*, CARNEGIE ENDOWMENT FOR INT'L PEACE, (July 26, 2017), https://carnegieendowment.org/2017/07/26/germany-confronts-russian-hybrid-warfare-pub-72636.

188. *See* Timothy L. Thomas, *Russia's Reflexive Control Theory and the Military*, 17 J. SLAVIC MIL. STUD. 237, 241 (2004).

189. *See* Han Bouwmeester, *Lo and Behold: Let the Truth Be Told: Russian Deception Warfare in Crimea and Ukraine and the Return of "Maskirovka" and "Reflexive Control Theory"*, *in* NETHERLANDS ANNUAL REVIEW OF MILITARY STUDIES *2017* at 125, 140 (Paul Ducheine & Frans Osinga eds., 2017).

There is commonly a double deception at the heart of disinformation campaigns. First, there is deception of the target. Second, there is often an attribution deception, whereby the foreign power hides its identity through the use of sock puppets.[190] A sock puppet is defined, in the context of the Internet,[191] as a "pseudonym adopted by someone who has made a posting to some social media forum and then follows it up with a supportive posting using the pseudonym."[192] During the 2016 U.S. presidential election, Russian social media accounts often represented themselves as American citizens.[193] In cases like this, the foreign power clearly hopes to achieve a level of influence by concealing the source of the communication, which it could not achieve through open and transparent messaging.[194]

Disinformation campaigns that result in decision-making paralysis, or that cause a realignment of the policy position of the population or political class, so it comes to align with the interests of the foreign power, clearly violate the principle of non-intervention. Even when the efforts of the foreign power are not successful, disinformation campaigns can still be categorized as "methods of coercion,"[195] and therefore violations of the non-intervention rule, in one of two circumstances. First, where we see a sustained campaign of disinformation by a foreign power which a reasonable observer would conclude was intended to create confusion about the facts of the situation and/or undermine the faith of the local population in the democratic system.

On the application of the notion to Russian efforts in the 2016 U.S. presidential election, *see* Annie Kowalewski, *Disinformation and Reflexive Control: The New Cold War*, GEO. SEC. STUD. REV. (Feb. 1, 2017), http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

190. *See* Diego A. Martin et al., *Recent Trends in Online Foreign Influence Efforts*, 18 J. INFO. WARFARE no. 3, 15, at 16 (2019).

191. The OXFORD ENGLISH DICTIONARY defines the term "sock puppet" as a person whose actions are controlled by another. *Sock, n.1*, OXFORD ENG. DICTIONARY ONLINE (June 2020), https://www.oed.com/view/Entry/183797.

192. A DICTIONARY OF THE INTERNET (Darrel Ince ed., 4th ed. 2019).

193. *See* Jens David Ohlin, *Election Interference: The Real Harm and The Only Solution* 7 (Cornell Legal Stud. Res. Paper Series, No. 18-50, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3276940; *see generally*, Christopher T Stein, *Hacking the Electorate: A Non-Intervention Violation Maybe, but Not an "Act of War"*, 37 ARIZ. J. INT'L & COMP. L. 29 (2020) (analyzing how to categorize the Russian disinformation operations during the 2016 U.S. election under international law).

194. The social media platform, Facebook, has responded to the problem of, what it calls, "coordinated manipulation campaigns" by focusing on the issue of transparency, with its Head of Cybersecurity Policy explaining that: "The real issue is that the actors behind these campaigns are using deceptive behaviors to conceal the identity of the organization behind a campaign." He describes "Foreign-led efforts to manipulate public debate in another country" as a "particularly egregious" example of a coordinated manipulation campaign. Nathaniel Gleicher, *How We Respond to Inauthentic Behavior on Our Platforms: Policy Update*, FACEBOOK (Oct. 21, 2019), https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/.

195. Nicar. v. U.S., 1986 I.C.J, ¶ 205.

Second, where we see a sustained disinformation campaign that uses sock puppets, because, in these circumstances, it is clear the foreign power wants to manipulate the domestic debate, but also that it wants the population to believe that political discussions were not subject to outside interference. These disinformation campaigns are coercive, because the objective, in both cases, is to usurp the process of democratic self-determination, replacing the will of the local population with that of the outside power.

VI. CONCLUSION

The aim of this article was to explain how we can apply the long-established principle of non-intervention to the new problem of state cyber and influence operations targeting elections. There is general agreement that the formulation in the 1986 *Nicaragua* case provides the starting point for any discussion: a prohibited intervention must both concern a matter "which each State is permitted to decide freely," and use "methods of coercion."[196] There is also no doubt that the outcome of an election is a matter that democratic states should be permitted to decide freely, without outside intermeddling—this point has been clear from the emergence of the non-intervention rule.[197] The only question is whether and when cyber and influence operations targeting elections can be categorized as coercive—and that depends on how we understand the term.

Words for international lawyers mean what international lawyers decide they mean.[198] The agreed meaning of coercion will crystallise through the utterances of states, courts, tribunals, international law practitioners, and academics. It is, therefore, important for democratic countries to explain publicly which cyber and influence operations they consider to be violations of the non-intervention principle, or how and why certain forms of cyber and influence operation can be categorized as coercive.

This article developed an argument for how we can, and should, understand the notion of coercion, by drawing on the arguments of our colleagues in the cognate disciplines of philosophy and the philosophy of law. The work showed that the function of the non-intervention rule is to protect the state from coming under the control of an outside power through its intermeddling in the *information* that voters and the political class rely on

196. *Id.*

197. *See* WHEATON, *supra* note 41.

198. The point is made clear in *Whaling in the Antarctic*, where the International Court of Justice drew a clear distinction between the way that scientists use the term "scientific research" and its international law meaning, with the ICJ deciding that "[t]heir conclusions as scientists . . . must be distinguished from the interpretation of the Convention, which is the task of this Court." Whaling in the Antarctic (Austl. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 226, ¶ 82 (Mar. 31).

when making a decision; the capacity of the population and political class to engage in meaningful political *deliberation*; the right of the state to *decide* freely; or the sovereign right of the state to *act* for itself. The analysis led to the following conclusions.

First, the provision of factual *information* and commentaries on the news by foreign states, including by state-owned and state-controlled news media, does not violate the principle of non-intervention, no matter how unfriendly or unwelcome.[199] Consequently, the practice of doxfare is not a violation of the rule. Nor are comments made by the leaders of outside powers seeking to influence the outcome of a democratic election or referendum. Lying to the electorate, on the other hand, defined as providing deliberately false information, is prohibited where the intention is to get the population to vote differently. Fake news, in this narrow sense, involves the coercive manipulation of the decision-making process, because the objective is to deceive the target population into doing something it would not otherwise have done, absent the false information.

Second, sustained disinformation campaigns are unlawful where the objective is to frustrate the target state's capacity for meaningful democratic *deliberation*. This can be done in two ways: by paralyzing the decision-making process, through the creation of confusion about the facts of the situation and undermining confidence in the ability of the system to deliver the correct policy outcomes; and by systematically feeding information and disinformation into political debates, in order to move the position of the population or political class so that it comes to align with the interests of the foreign power. Both involve methods of coercion because the objective is to usurp the target's right to decide for themselves. Where there is evidence that a foreign power is using sock puppets, such as individuals pretending to be local citizens, and spreading disinformation, this clearly violates the non-intervention rule.

Third, where information and communications technologies are used to communicate to a government or population that they *must* decide a particular way, this constitutes a coercive threat and a violation of the non-intervention rule. States are entitled to make representations and to warn of deleterious consequences if the government or population makes a certain decision. What outside powers are not permitted to do is frame the warning as a threat that could not reasonably be ignored because this creates a forced choice situation where the target is required to make the *decision* preordained by the foreign power.

199. The one exception is an influence campaign designed to overwhelm the information environment with a single political narrative, as this prevents the electorate from making a meaningful choice between competing positions.

Finally, where a state cyber operation takes control of, or disables the functioning of, the ICTs that underpin the holding of elections, to ensure that the target *acts* as intended by the foreign power, this involves the coercive use of cyber power and constitutes a prohibited intervention. All uses of cyber power of this type are coercive, and therefore wrongful, because the outside power achieves its objective by working through bodies like the Electoral Commission, compelling them to do something they would not otherwise do–and thus making the target state's institutions the instrument of a foreign power.