VOLUME 62, NUMBER 1, WINTER 2021

Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace

William Ossoff*

The rule of non-intervention is a longstanding rule of customary international law whose precise content has been a subject of constant contestation since its formation. As such, the rule has served as only a limited deterrent to state behavior. However, the growing prevalence of state-sponsored cyber political operations, such as Russia's interference in the 2016 U.S. presidential election, has revived interest in defining the rule of non-intervention. Powerful states who historically have not been the strongest proponents of the rule, such as the United States, are now vocal about its applicability in the cyber context.

This Note provides, in Parts I and II, an account of the historical debate over the definition of non-intervention. It provides a unique contribution to the scholarly literature through a novel comparative analysis, in Part III, of the terminology used by states to describe the rule of non-intervention's applicability to cyber operations. It then applies these various definitions, in Part IV, to a range of hypothetical cyber operations in order to help determine which operations might violate the rule of non-intervention. As the Note concludes, the rule's deterrent effect on future cyber political operations will depend in no small part on which state's definition, if any, becomes predominant.

INTRODUCTION

"America is totally unprepared for what is coming," wrote retired General Stanley McChrystal.[1] "We're not ready," said House Intelligence Committee Chairman Adam Schiff.[2] "They will be back," warned former FBI Director James Comey.[3] Russia's interference in the 2016 U.S. presidential election—a multi-pronged operation that involved hacking and leaking stolen emails, as well as spreading disinformation on social media[4]—exposed the ways in which cyber capabilities have scrambled traditional international

* J.D. Candidate (2021), Harvard Law School. I am grateful to Professor Naz Modirzadeh and Dustin Lewis for their extremely helpful feedback and guidance on early drafts of this Note. I also wish to thank the *Harvard International Law Journal* editorial team for all of their insightful comments and edits.

1. Stanley McChrystal & David Eichenbaum, *Russia's Prepared to Intervene in 2020. Will the U.S. Be Ready?*, POLITICO (July 25, 2019), https://www.politico.com/magazine/story/2019/07/25/russias-prepared-to-interfere-in-2020-will-the-us-be-ready-227477 [https://perma.cc/S33M-A4TB].

2. Eric Johnson, *"We're Not Ready" for Foreign Election Interference in 2020, Says Rep. Adam Schiff*, VOX (July 22, 2019), https://www.vox.com/recode/2019/7/22/20702196/adam-schiff-deepfakes-nancy-pelosi-google-twitter-facebook-2020-youtube-kara-swisher-decode-podcast [https://perma.cc/AV59-6H72].

3. *James Comey: U.S. Is Not Ready for Russian Interference in 2020 Election*, CBS NEWS (May 8, 2019), https://www.cbsnews.com/video/fmr-fbi-chief-james-comey-us-is-not-ready-for-the-2020-election/ [https://perma.cc/Y9Q7-7C3X].

4. *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1581 (2017).

power dynamics. The United States and other open democracies, which are committed to freedom of speech and free flow of information on the internet, are particularly vulnerable to manipulation of their elections by hostile actors.[5]

Recognition of this vulnerability by the United States and other democracies has revived their interest in a longstanding but oft-violated rule of international law: the rule of non-intervention. This rule of customary international law was once a rallying cry for developing countries against political interference by superpowers during the Cold War.[6] Now that major powers like the United States have themselves become more vulnerable to political interference, particularly in the cyber context, they have become more interested in enforcing this rule.[7] However, before the rule of non-intervention can be enforced effectively, a predicate question must be answered: What is the definition of this customary rule, particularly in the ever-evolving context of cyberspace? The answer, as demonstrated by the varying positions of states and scholars, is far from clear.

This Note explores the historical and modern contours of the debate over the precise scope of the rule of non-intervention. State conceptions of the rule of non-intervention's applicability, including in the domain of cyber political interference, vary in significant ways. These conceptual differences could hinder efforts to reach an international consensus on the scope of the rule and thus make it difficult to deter unlawful political interventions. However, the general agreement that the rule applies to cyber political interventions—including amongst major powers like the United States, which have historically been skeptical of the rule—provides a source of optimism that in this particular domain, the rule of non-intervention may finally have some real impact.

Part I examines the origins of the rule in international law and the sources that are most often cited by states as authoritative articulations of the rule. The rule is not mentioned expressly in the U.N. Charter or other globally oriented treaties. As evidence of the rule's customary status, states often point to regional treaties such as the Charter of the Organization of Ameri-

5. *See* Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations* 1 (Hoover Inst. Aegis Series, Paper No. 1806, 2018). ("Our central claim is that the United States is disadvantaged in the face of these soft cyber operations due to constitutive and widely admired features of American society, including the nation's commitment to free speech, privacy, and the rule of law; its innovative technology firms; its relatively unregulated markets; and its deep digital sophistication.").

6. *See* Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs*, 83 Am. J. Int'l L. 1, 2–4 (1989).

7. *See* Brian J. Egan, Legal Adviser, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016) (transcript available at https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/6XQW-FNNJ]).

can States ("OAS Charter"),[8] U.N. General Assembly Resolutions such as the Declaration on Principles of International Law Concerning Friendly Relations ("Friendly Relations Declaration"),[9] and International Court of Justice ("ICJ") decisions such as *Military and Paramilitary Activities in and Against Nicaragua*.[10] However, these materials all articulate the well-recognized elements of the rule in different ways. Part II analyzes the differing conceptions of the two primary elements of an unlawful intervention: (1) a state intervenes in the exclusive sovereign affairs or "domaine réservé" of another state; and (2) the intervention involves methods of "coercion."[11]

Part III closely examines the language used by the few states that have explained their understandings of how this rule applies to cyber operations: Australia, China, France, Iran, the Netherlands, the United Kingdom, and the United States. Part IV then applies these differing state conceptions of non-intervention to hypothetical scenarios involving cyber operations by one state in or against the political system of another state, assessing whether, under each state's conception of non-intervention, the operations violate the rule. As this section illustrates, differences in the terminology used to set the parameters of non-intervention could lead to significantly different conceptions of the rule's scope.

This Note concludes by assessing potential futures for the rule of non-intervention in relation to cyber operations. On the one hand, this debate over non-intervention's applicability to cyber political operations could indicate that non-intervention will maintain its historical position as a vague rule of customary international law, with violations only rarely recognized by international institutions like the United Nations or International Court of Justice. On the other hand, many of the states who want non-intervention to apply in some form to political interference have not historically been strong proponents of the rule.[12] Interestingly, a stronger norm of non-intervention in cyberspace, a position historically supported by China and other authoritarian states,[13] may actually benefit Western democracies such as the United States. If a wider range of political interferences constituted a breach of the rule of non-intervention, under the law of state responsibility, states would have the right to take both cyber and non-cyber countermeasures.[14]

8. *See* Charter of the Organization of American States art. 15, Apr. 30, 1948, 119 U.N.T.S. 3 [hereinafter OAS Charter].

9. *See* G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970) [hereinafter Friendly Relations Declaration].

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

11. *See id.* ¶ 205.

12. *See* Damrosch, *supra* note 6, at 2–4.

13. *See* Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 350 (2009).

14. *See* Int'l L. Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 22–23 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n, A/CN.4/SER.A/2001/Add.1 (Part 2).

This threat of countermeasures could deter states from taking actions that might violate the rule. Greater legal clarity about the boundaries of non-intervention, supported by institutions like the United Nations and International Court of Justice, could embolden even smaller nations to respond with countermeasures to unlawful political interventions. Ultimately, whether non-intervention becomes a new deterrent to political interference or remains mired in normative uncertainty will depend in no small part on whether states summon the political will to resolve their conceptual differences.

It is also important to note the areas of international law that this Note does not discuss. There is an ongoing debate amongst states as to whether sovereignty is a primary rule of international law, with the United Kingdom and some former U.S. officials taking the position that sovereignty is an underlying principle but not a rule that can be formally breached and justify countermeasures.[15] This Note largely sidesteps this debate and focuses specifically on the rule of non-intervention because there is general international consensus that the rule of non-intervention is a primary rule.[16] In addition, this Note focuses on political interventions that fall clearly below the threshold of the use of force. In doing so, it aims to avoid the current debate on whether cyber operations may or may not constitute an unlawful use of force in the sense of article 2(4) of the U.N. Charter and its customary counterpart.[17] Nor does this Note address the applicability of international humanitarian law in relation to cyber operations.

I. Historical Development of the Rule of Non-Intervention

For the conceptual origin of the rule of non-intervention in international law, scholars often point to the work of eighteenth century Swiss philosopher Emer de Vattel.[18] Vattel wrote in *The Law of Nations*, "[i]f any [nation] intrude into the domestic concerns of another nation . . . they do it an

15. *See* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 Am. J. Int'l L. Unbound 207, 210 (2017); Jeremy Wright, U.K. Attorney General, Speech on Cyber and International Law in the 21st Century at Chatham House (May 23, 2018) (transcript available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [https://perma.cc/97DD-W4AR]).

16. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27); Friendly Relations Declaration, *supra* note 9.

17. *See* Michael Schmitt, *France Speaks Out on IHL and Cyber Operations: Part I*, EJIL: Talk! (Sept. 30, 2019), https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/ [https://perma.cc/4PUG-VAGA].

18. *See, e.g.*, Georges Abi-Saab, *Some Thoughts on the Principle of Non-Intervention*, in International Law: Theory and Practice: Essays in Honor of Eric Suy 225 (Karel Wellens ed., 1998) ("Historically, while one can find cursory hints at the principle in the writings of the Founding Fathers such as Grotius and even Vitoria before him, it is Vattel that gives it its first clear rendering."); Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm of Non-Intervention in the Era of Weaponized Information*, 9 Harv. Nat'l. Sec. J. 146, 162 (2018) ("One of the earliest iterations of the concept of non-intervention was introduced in 1758 by the Swiss philosopher and legal scholar Emer de Vattel.").

injury."[19] The concept of non-intervention started to gain further traction in the nineteenth century, as a response to the "hegemonic designs" of major European powers such as Austria, Prussia, and Russia—who collectively comprised the Holy Alliance.[20] The Monroe Doctrine—an 1823 declaration by U.S. President James Monroe that any European interference in the Western Hemisphere would be viewed "as the manifestation of an unfriendly disposition toward the United States"[21]—is often cited as an early example of state practice concerning the rule of non-intervention.[22]

It was not until the twentieth century, however, that the principle began to be codified in international agreements. The principle was expressly set out in treaties between certain states in the Americas. Article 8 of the Montevideo Convention on the Rights and Duties of States declares, "[n]o State has the right to intervene in the internal or external affairs of another."[23] This principle was reaffirmed in article 1 of the 1936 Additional Protocol to the Montevideo Convention Relative to Non-Intervention, in which, "[t]he High Contracting Parties declare inadmissible the intervention of any one of them, directly or indirectly, and for whatever reason, in the internal or external affairs of any other of the Parties."[24]

No provision of the United Nations Charter expressly concerns the principle of non-intervention applicable to individual states in their international relations. However, article 2(7) of the Charter does state that "[n]othing contained in the present Charter shall authorize the United Nations to intervene in matters which are *essentially* within the domestic jurisdiction of any state."[25] The League of Nations Covenant had included a similar reference to disputes "which by international law" are "solely within the domestic jurisdiction" of states, declaring in article 15(8) that the League shall make no recommendation as to the settlement of such disputes.[26] As one scholar argues, "[t]he substitution . . . of the reference to 'international law' in Art. 15(8) by the term 'essentially' [in the U.N. Charter] was designed to reinforce and widen the scope of the domestic jurisdiction clause of the Charter

19. Emer de Vattel, The Law of Nations or Principles of the Law of Nature Applied to the Conduct and Affairs of Nations and Sovereigns 12 (Joseph Chitty ed. & trans., 1844) (1758).

20. Abi-Saab, *supra* note 18, at 226. The Holy Alliance stemmed from an 1815 peace agreement between three monarchies—Austria, Prussia, and Russia—who sought to extend their influence across Europe. *See* William Penn Cresson, The Holy Alliance: The European Background of the Monroe Doctrine 1–2 (1922).

21. James Monroe, Message at the Commencement of the First Session of the 18th Congress (Dec. 2, 1823) (transcript available at https://avalon.law.yale.edu/19th_century/monroe.asp [https://perma.cc/FTE9-4DB6]).

22. *See, e.g.*, Abi-Saab, *supra* note 18, at 226; Jamnejad & Wood, *supra* note 13, at 349.

23. Convention on Rights and Duties of States art. 8, Dec. 26, 1933, 49 Stat. 3097, 165 L.N.T.S 19 [hereinafter Montevideo Convention].

24. Additional Protocol Relative to Nonintervention art. 1, Dec. 23, 1936, 51 Stat. 41, 188 L.N.T.S. 31.

25. U.N. Charter art. 2, ¶ 7 (emphasis added).

26. League of Nations Covenant art. 15, ¶ 8.

as compared to that of the League Covenant."[27] Even though article 2(7) does not cover the conduct of individual states (but rather the United Nations Organization), it could still "be informative as to the operation of the principle of non-intervention," as "the concerns that gave rise to Article 2(7) are similar to those supporting the principle of non-intervention."[28] Other articles of the Charter provide supplemental support for the general principle of non-intervention, including the article 2(1) principle of "sovereign equality" amongst member states.[29]

A number of regional instruments adopted subsequent to the U.N. Charter include prohibitions on state-to-state intervention. Articles 15 and 16 of the 1948 OAS Charter provide a detailed description of what is prohibited under the rule:

> Article 15
>
> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic and cultural elements.
>
> Article 16
>
> No State may use or encourage the use of coercive measures of an economic or political character in order to force the sovereign will of another State and obtain from it advantages of any kind.[30]

Similarly, the 2000 Constitutive Act of the African Union affirms the principle of "non-interference by any Member State in the internal affairs of another."[31] Article 2 of the 2007 Charter of the Association of Southeast Asian Nations ("ASEAN") states that ASEAN members "shall act in accordance" with the principle of "non-interference in the internal affairs of ASEAN Member States."[32] Thus, although the rule of non-intervention is not mentioned expressly in the U.N. Charter or other globally oriented treaties, a large number of states have committed to following the rule through

27. Georg Nolte, *Article 2(7)*, *in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, VOLUME I 293 (Bruno Simma et al. eds., 3d ed. 2012).

28. Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 254 (Jens David Ohlin, Kevin Govern & Clare Finklestein eds., 2015).

29. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27) (describing non-intervention as a "a corollary of the principle of the sovereign equality of States"); *see also* Nolte, *supra* note 27, at 284.

30. OAS Charter, *supra* note 8, art. 15–16.

31. Constitutive Act of the African Union art. 4(g), July 1, 2000, 2158 U.N.T.S. 3.

32. Charter of the Association of Southeast Asian Nations art. 2, Nov. 20, 2007, 2624 U.N.T.S 223.

these regional treaties, at least with regard to other parties to those instruments.[33]

Furthermore, the fact that a geographically diverse group of states has ratified these treaties provides support for the status of the rule as customary international law. Customary international law consists of two elements: (1) widespread and consistent state practice (2) that is accepted as law (opinio juris).[34] As the International Law Commission explained, "one must look at what States actually do and seek to determine whether they recognize an obligation or a right to act in that way."[35] Both elements must be present, although "it is generally accepted that verbal conduct (written or oral) may also count as State practice."[36] Furthermore, as two scholars note, modern custom is "often deduced from multilateral treaties and declarations by international fora such as the General Assembly."[37]

In addition to the multilateral treaties cited above, a number of U.N. General Assembly resolutions provide further evidence that the rule of non-intervention is reflective of customary international law. Foremost among these resolutions is the 1970 Friendly Relations Declaration. According to that Declaration, which received unanimous support from Member States, the "principles of the Charter which are embodied in this Declaration constitute basic principles of international law."[38] The Friendly Relations Declaration goes on to state a number of these principles, one of which is "[t]he principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter."[39] Thus, the unanimously adopted Friendly Relations Declaration states that there is a general rule of non-intervention connected to the U.N. Charter, defining the rule as follows:

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
>
> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to

33. For example, 100 states are party to the three treaties discussed in this paragraph.

34. *See* Int'l L. Comm'n, Rep. on the Work of Its Seventieth Session, U.N. Doc. A/73/10, at 120, 122–23 (2018).

35. *Id.* at 125.

36. Michael Wood & Omri Sender, *State Practice*, *in* Max Planck Encyclopedia of International Law (Oxford Univ. Press 2017).

37. Anthea Roberts & Sandesh Sivakumaran, *The Theory and Reality of the Sources of International Law*, *in* International Law 89, 104 (Malcolm D. Evans ed., 5th ed. 2018).

38. Friendly Relations Declaration, *supra* note 9.

39. *Id.*

> obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State.
>
> The use of force to deprive peoples of their national identity constitutes a violation of their inalienable rights and of the principle of non-intervention.
>
> Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State.[40]

While the Friendly Relations Declaration is the most prominent U.N. General Assembly resolution on non-intervention, given its unanimous support and express assertion that the principles of the Charter which are embodied in the Declaration constitute basic principles of international law, other resolutions about non-intervention preceded and followed it. The 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,[41] which uses language nearly identical to that of the Friendly Relations Declaration, was also adopted without opposition and with just one abstention (from the United Kingdom).[42] However, unlike with respect to the Friendly Relations Declaration, the United States stated that it viewed this resolution as no more than an assertion of political intent.[43] The 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States adopted a more expansive and specific approach to non-intervention, asserting that states are entitled to "permanent sovereignty" over natural resources and "to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations."[44] However, because it was opposed by twenty-two states, including much of Western Europe, scholars have argued that the 1981 Declaration is not reflective of customary international law.[45]

In its most widely cited and consequential decision on the subject, the ICJ addressed the significance of the Friendly Relations Declaration with respect to customary international law. In *Military and Paramilitary Activities*

---

40. *Id.*

41. *See* 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).

42. *See* Jamnejad & Wood, *supra* note 13, at 353.

43. *See id.*

44. G.A. Res. 36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (Dec. 9, 1981).

45. *See* Jamnejad & Wood, *supra* note 13, at 355.

in and Against Nicaragua, the ICJ examined state practice and opinio juris pertaining to the rule of non-intervention, pointing to both the Friendly Relations Declaration and the 1965 Declaration, while noting that the Friendly Relations Declaration carries greater weight because of its statement that it reflects "basic principles" of international law.[46] Using similar language from the Friendly Relations Declaration, the Court defined a "prohibited intervention" as "one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely," and noted that an intervention is "wrongful when it uses methods of coercion in regard to such choices."[47] The Court further stated that "[e]xpressions of an *opinio juris* regarding the existence of the principle of non-intervention in customary international law are numerous and not difficult to find,"[48] and the Court expressed its view that the rule of non-intervention is "a customary principle which has universal application."[49]

According to the ICJ, "the principle of non-intervention is backed by established and substantial practice,"[50] and yet the rule has been breached frequently in practice by a number of states. As Lori Damrosch points out, powerful states such as the United States and Soviet Union interfered politically and economically in the internal affairs of smaller developing nations in order to exert influence during the Cold War.[51] She writes, "These patterns demonstrate a rather serious gap between what a broad view of the nonintervention norm would require and what states actually do."[52] The ICJ responded to this critique in *Nicaragua* by noting, "It is not to be expected that in the practice of States the application of the rules in question should have been perfect, in the sense that States should have refrained, with complete consistency, from the use of force or from intervention in each other's internal affairs."[53] Indeed, the ICJ reaffirmed the continuing validity of the rule in another decision nearly twenty years after its *Nicaragua* judgment, in *Armed Activities on the Territory of the Congo*.[54]

Scholars and states also generally agree that the rule of non-intervention applies to cyber operations, even as states breach the rule in their operations. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, which does not purport to reflect state views but attempts to define the lex

46. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 106–07, ¶ 202–03 (June 27).
47. *Id.* ¶ 205.
48. *Id.* ¶ 202.
49. *Id.* ¶ 204.
50. *Id.* ¶ 202.
51. *See* Damrosch, *supra* note 6, at 2
52. *Id.*
53. *Nicar. v. U.S.*, 1986 I.C.J. 98, ¶ 186.
54. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 164 (Dec. 19) ("In the case concerning *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, the Court made it clear that the principle of non-intervention prohibits a State 'to intervene, directly or indirectly, with or without armed force, in support of an internal opposition in another State.'").

lata of international law in the cyber context, cites *Nicaragua* in arguing, "the fact that the prohibition is often breached does not undermine the Rule as reflecting an extant principle of international law."[55] Recent official statements from numerous states, in which they express their commitment to the rule as applied to cyber activities, provides further evidence of opinio juris for the status of the rule of non-intervention as customary international law.[56] The final report of the 2015 meeting of the U.N. Group of Governmental Experts on Information Security ("GGE"), in which a geographically diverse group of twenty states agreed that states must observe the principle of "non-intervention in the internal affairs of other States" in the use of information and communications technologies, provides further evidence that states view the rule as applicable in cyberspace.[57] However, the many variations in the ways that states define the elements of the rule—both in the cyber context and more broadly—indicate a degree of ambiguity about its precise meaning.

II. The Elements of Non-Intervention

While states and scholars generally agree that the rule of non-intervention has two primary elements, these two elements are not comprehensively defined. Experts frequently cite as authoritative the ICJ's articulation of the elements of the rule in *Nicaragua*. According to the ICJ, a prohibited intervention (1) intrudes in "matters in which each State is permitted, by the principle of State sovereignty, to decide freely," and (2) involves "methods of coercion."[58] However, many international actors have articulated these elements slightly differently from the ICJ in such a way that may affect the scope of the rule. This section will lay out the debate about the precise content of each of these elements.

A. *"Matters in which each State is permitted, by the principle of State sovereignty, to decide freely."*[59]

In *Nicaragua*, the ICJ describes the rule of non-intervention as "a corollary of the principle of the sovereign equality of States."[60] Indeed, the Friendly Relations Declaration emphasizes the prohibition on measures that prevent another state from freely exercising its "sovereign rights."[61] How-

55. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 314 (Michael N. Schmitt ed., 2013).

56. *See infra* Part III.

57. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174, at 12 (July 22, 2015).

58. *Nicar. v. U.S.*, 1986 I.C.J. 98, 108, ¶ 205.

59. *Id.*

60. *Id.* ¶ 202.

61. Friendly Relations Declaration, *supra* note 9.

ever, there remains an ongoing debate about how to define the contours of the "sovereign rights" that are protected from intervention.

One approach to defining "sovereign rights" rests on the concept of the "domaine réservé," which stems from *Nationality Decrees Issued in Tunis and Morocco*, a 1923 advisory opinion of the Permanent Court of International Justice ("PCIJ").[62] *Nationality Decrees* concerned a dispute between France and Great Britain over nationality decrees made in Tunis and Morocco.[63] To resolve this dispute, France and Great Britain asked the PCIJ to determine certain aspects of the scope of article 15(8) of the League of Nations Covenant.[64] The PCIJ interpreted the phrase, in article 15(8), "solely within the domestic jurisdiction" of a state to refer to matters that "are not, in principle, regulated by international law."[65] The PCIJ determined that such matters that are unregulated by international law are thus within the "reserved domain" or "domaine réservé" of the state.[66]

Many scholars have incorporated this notion of the domaine réservé, covering those matters which are not regulated by international law, into their conceptions of the rule of non-intervention. As noted above, article 2(7) of the U.N. Charter does use similar language to the League of Nations Covenant in stating that the Charter does not authorize the United Nations to intervene "in matters which are essentially within the domestic jurisdiction of any state."[67] However, none of the aforementioned treaties, declarations, or decisions on the general rule of non-intervention, as it applies to individual states in their international relations, employs the term "domaine réservé" or even "domestic jurisdiction." Instead, the Montevideo Convention, OAS Charter, the Friendly Relations Declaration, and *Nicaragua* refer to the "internal or external affairs" of states,[68] "sovereign will,"[69] or matters protected by the "principle of State sovereignty."[70]

According to some scholars, these terms are all essentially synonymous. Katharina Ziolkowski writes that "it can be asserted that the internal affairs of a State (domaine réservé) describe areas not regulated by international

62. *See* Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4 (Feb. 7).

63. *See id.*

64. *See id.*

65. *Id.* at 23–24.

66. *Id.* In this particular case, the PCIJ noted that while questions of nationality are typically within this domaine réservé, the facts of this particular case implicated international legal obligations and interest on the part of Great Britain and thus could not be decided exclusively within France's domestic jurisdiction. *See id.* at 27–32.

67. U.N. Charter art. 2, ¶ 7.

68. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 108 ¶ 205 (June 27); OAS Charter, *supra* note 8, art. 15; Montevideo Convention, *supra* note 23, art. 8.

69. OAS Charter, *supra* note 8, art. 16.

70. Friendly Relations Declaration, *supra* note 9; *Nicar. v. U.S.*, 1986 I.C.J. 98, ¶ 205.

norms."[71] Terry Gill likewise notes that non-intervention "relates to the right of States to exercise jurisdiction over their territory and abroad within the limits posed by international law and to the relative notion of domestic jurisdiction, or domaine réservé."[72] According to the *Tallinn Manual*, "[t]he notion of 'internal affairs' derives from the concept of domaine réservé, which consists of matters 'not, in principle, regulated by international law.'"[73]

If the only matters prohibited from foreign intervention are those which are in the "domaine réservé"—that is, those matters that are not regulated by international law—the rule of non-intervention has less impact than it may have had a century ago. In *Nationality Decrees*, the PCIJ noted that the scope of the domaine réservé is "essentially relative" and "depends upon the development of international relations."[74] As Gill points out, "many matters which formerly were considered to be wholly or essentially within the internal affairs of States are now, to a greater or lesser extent, regulated by international law."[75] Thus, as compared to 1923 when international law was still relatively limited, the domaine réservé likely covers a far narrower range of activities in the contemporary period. For example, given that the choice of a political system is widely considered to be within the scope of the domaine réservé,[76] some countries have hinted that interference in another state's election by spreading disinformation—through fake social media accounts that deliberately post lies and false information, for example—may be prohibited by the rule.[77] However, internet communication is governed at least in part by international legal agreements such as the Constitution of the International Telecommunications Union.[78] Thus, it is unclear if preventing such online disinformation campaigns could be said to fall within a state's domaine réservé.

Recognizing that the domaine réservé concept would severely limit the scope of the rule of non-intervention, many have pointed out that the notion of "domaine réservé" fails to capture the entirety of "matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[79] Jens David Ohlin criticizes the lack of clarity in the concept, noting, "de-

71. 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, 434 (Katharina Ziolkowski ed., 2013).

72. Terry D. Gill, *Non-Intervention in the Cyber Context*, *in* Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy 217, 217 (Katharina Ziolkowski ed., 2013).

73. Tallinn Manual, *supra* note 55, at 314.

74. Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 24 (Feb. 7).

75. Gill, *supra* note 72, at 217.

76. *See* Watts, *supra* note 28.

77. *See infra* Part IV.D.

78. *See* Ziolkowski, *supra* note 71.

79. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 108 ¶ 205 (June 27).

spite the patina of precision in its French rendering, the concept has little internally generated content" and fails to define "which domains or activities should be off-limits because they fall within a State's domaine réservé and which domains are subject to foreign action."[80] Harriet Moynihan also points out that domaine réservé "does not include a state's external affairs, which, as the ICJ made clear in *Nicaragua*, form part of the scope of the nonintervention principle."[81]

Indeed, the concept provided in *Nicaragua* appears far broader than just the domaine réservé as defined by the PCIJ. The ICJ also expressed its view that under the rule, states are free to decide "the choice of a political, economic, social and cultural system, and the formulation of foreign policy."[82] The Friendly Relations Declaration similarly stated, "Every State has an inalienable right to choose its political, economic, social and cultural systems."[83] Both the Friendly Relations Declaration and the OAS Charter also prohibit intervention "against the personality of the State or against its political, economic and cultural elements."[84]

However, while slightly more concrete than domaine réservé, this focus on a state's "political, economic, social, and cultural system" is also vague and can be interpreted in multiple ways.[85] For example, Moynihan argues that states have the right to make "policies" related to the choice of these systems without foreign intervention.[86] By this definition, a wide range of government policies could be deemed relevant to the "choice of a political, economic, social and cultural system" and protected from foreign intervention.[87] Conducting elections is widely considered to be a sovereign activity tied to the "choice of a political system" that should be protected from intervention.[88] More contested is whether states have the right, as stated in the 1981 Declaration on the Admissibility of Nonintervention and Noninterference, to develop "their system of information and mass media" without intervention in order "to promote their political, social, economic and cultural interests and aspirations."[89] For example, states such as China and Russia are currently defending their respective efforts to censor Internet communications under a framing of "cyber sovereignty."[90] Certain other

80. Ohlin, *supra* note 4, at 1587, 1588.

81. Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* 34 (Chatham House Research Paper, 2019).

82. *Nicar. v. U.S.*, 1986 I.C.J. 108, ¶ 205.

83. Friendly Relations Declaration, *supra* note 9.

84. *Id.*; OAS Charter, *supra* note 8, art. 15.

85. Friendly Relations Declaration, *supra* note 9.

86. *See* Moynihan, *supra* note 81, at 34.

87. *Nicar. v. U.S.*, 1986 I.C.J. 108, ¶ 205.

88. *See* Egan, *supra* note 7; Wright, *supra* note 15.

89. G.A. Res. 36/103, *supra* note 41, annex ¶ 2(I)(c).

90. *See, e.g.*, Adam Segal, *Year in Review: Chinese Cyber Sovereignty in Action*, Council on Foreign Relations (Jan. 8, 2018), https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action [https://perma.cc/FWC7-4GN4] ("In March 2017, Tencent and other companies were told to close websites that hosted discussions on the military, history, and international affairs."); *Russia Internet: Law*

states, including the United States, have criticized such censorship as inconsistent with protected freedom of expression under international human rights law.[91] This conflict of views underscores the uncertainty surrounding the scope of "sovereign" activities that are protected by this rule of customary international law.

B. "Methods of coercion"

Even if the first element is interpreted broadly, the second element mentioned by the ICJ in *Nicaragua*—the use of "methods of coercion"—limits the scope of activities that would violate the rule of non-intervention. The ICJ stated its view that coercion "defines, and indeed forms the very essence of, prohibited intervention."[92] However, the ICJ did not further define the term coercion, and as multiple scholars have pointed out, there is no settled definition of "coercion" in international law.[93] Like the domaine réservé, it can be interpreted in multiple ways. As will be explained further below, some states and scholars argue that "coercion" involves forcing a state to make a decision that it would not otherwise make, whereas others argue that the key aspect of "coercion" is deprivation of control.

Merriam-Webster's legal dictionary defines coercion as "intimidating behavior that puts a person in immediate fear of the consequences in order to compel that person to act against his or her will."[94] Indeed, the Friendly Relations Declaration prohibits a state from coercing another state by "subordinat[ing]. . .the exercise of its sovereign rights,"[95] and the OAS Charter similarly prohibits a state from attempting to "force the sovereign will" of another state.[96] Some have interpreted this conception of coercion to mean that states cannot force other states to make a choice they would not otherwise have made. For example, the *Tallinn Manual* states, "the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action that it would otherwise take)."[97] Moynihan likewise describes coercion as activity designed "to compel an outcome in, or conduct with respect to, a matter

Introducing New Controls Comes Into Force, B.B.C. NEWS (Nov. 1, 2019), https://www.bbc.com/news/world-europe-50259597 [https://perma.cc/FF7G-474F] (discussing a new Russian law that "allows the government to block content without judicial consent and leaves users unaware about what information is being blocked and why").

91. *See* Egan, *supra* note 7 ("Some States invoke the concept of State sovereignty as a justification for excessive regulation of online content, including censorship and access restrictions. . .Any regulation by a State of matters within its territory, including use of and access to the Internet, must comply with that State's applicable obligations under international human rights law.").

92. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 108 ¶ 205 (June 27).

93. *See, e.g.*, TALLINN MANUAL, *supra* note 55, at 317.

94. *Legal Definition of Coercion*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/coercion#legalDictionary [https://perma.cc/BV4F-36JE] (last visited Apr. 13, 2020).

95. Friendly Relations Declaration, *supra* note 9.

96. OAS Charter, *supra* note 8, art. 16.

97. TALLINN MANUAL, *supra* note 55, at 319.

reserved to the target state."[98] However, this sets a high bar for proving the existence of legally cognizable coercion: it must be proven that the coerced state would not (otherwise) have made the decision that it was allegedly coerced to make. Under this approach, to prove that Russian interference in the 2016 election was sufficiently coercive, the United States would have to prove that the American people would not have elected Donald Trump if not for Russian intervention. This level of causation is extremely difficult to prove, given the large number of variables that influence every citizen's vote.

Both the Friendly Relations Declaration and the OAS Charter employ an additional phrase that would seem to broaden the scope of prohibited coercive activity: activity designed to obtain "advantages of any kind" from another state.[99] Based on this phrasing, some scholars have argued that the key aspect of coercion is not forcing a state to make a decision it would not otherwise have made; it is the deprivation of control over that decision-making process. This was the minority position taken within the International Group of Experts who contributed to the *Tallinn Manual*.[100] Ido Kilovaty similarly argues, "the nonintervention standard ought to focus on the deprivation of free choice, on which the current coercion standard only lightly touches."[101] Nicholas Tsagourias agrees, asserting that control is "the baseline of coercion."[102]

If control is the key axis on which coercion turns, then the threshold for breaching the rule of non-intervention is far lower. A covert disinformation campaign in another country's electoral process would seem to deprive the target state of "control" over the process of choosing political leaders.[103] Openly spreading any information, even legitimate information, could also arguably violate the state's control over the electoral process if it is indeed entitled to total control. The latter example would be unlikely to violate the rule, as state practice indicates that states have been spreading propaganda in other countries for decades.[104] Regardless, this discussion indicates that differences in the way that "coercion" is defined could have marked impacts on the scope of the rule of non-intervention.

98. Moynihan, *supra* note 81, at 29.

99. OAS Charter, *supra* note 8, art. 16; *see* Friendly Relations Declaration, *supra* note 9.

100. *See* Tallinn Manual, *supra* note 55, at 318.

101. Ido Kilovaty, *The Elephant in the Room: Coercion*, 113 Am. J. Int'l L. Unbound 87, 90 (2019).

102. Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, EJIL: Talk! (Aug. 26, 2019), https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/ [https://perma.cc/ZQ9B-UU6U].

103. *See* Harold Hongju Koh, *The Trump Administration and International Law*, 56 Washburn L.J. 413, 450 (2017).

104. *See* Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 Chi. J. Int'l L. 30, 46 (2018).

III. State Views on the Application of Non-Intervention to Cyber Operations

Ultimately, this conceptual debate about the scope of the customary rule of non-intervention can only be resolved by looking to state practice and opinio juris. In recent years, a number of high-level state officials have articulated their states' views on the application of non-intervention to cyber operations. However, as the foregoing discussion demonstrates, the differences in the language that is used to describe the rule, while subtle, could lead to substantial differences in the applicability of that rule. This section will examine closely the language used in statements made by high-level officials in seven states on the rule of non-intervention in cyberspace: the Netherlands, the United Kingdom, the United States, Australia, France, Iran, and China. The geographic scope of the countries surveyed is admittedly narrow, as few countries have shared their views on this exact topic. The development of custom in this area would benefit from more statements from a broader range of countries, which might help resolve some of the ambiguity that will be outlined below.

Table 1: Defining the Elements of Non-Intervention[105]

Country	Protected Domain of State Actions	Coercion
Netherlands	"Exclusive authority"	"Compel" state to take action it would not otherwise take
United Kingdom	Matters "at the heart" of sovereignty	"Coercive intervention"
United States	"Core functions"	Actions without a state's "consent" in "contravention of its rights"
Australia	Matters of "sovereignty"	Depriving a state of "control" over governance
France	"Political, economic, social and cultural system"	"Harm"
Iran	"Political, economic, social, and cultural organs"	"Impediment, denying, and…restricting" sovereign rights
China	"Stability"	"Undermine"

A. Netherlands

The Dutch foreign minister laid out a narrow vision of the rule of non-intervention in a July 2019 letter to the Dutch parliament that aimed to explain the government's official views on "the international legal order in

105. Citations for the quotes in this table are included later in this section when the quotes are discussed in the main text.

cyberspace."[106] Broadly, the letter defines intervention as "interference in the internal or external affairs of another state with a view to employing coercion against that state."[107] It goes on to note, "such affairs concern matters over which, in accordance with the principle of sovereignty, states themselves have exclusive authority."[108] This emphasis on matters over which states have "exclusive authority," while vague, aligns the Dutch formulation with the idea of the "domaine réservé," the narrow scope of activities which are untouched by international law and over which states have exclusive authority. The letter refers specifically to conducting elections, recognizing states, and joining international organizations as activities that are exclusively sovereign.[109] The statement also defines coercion in a narrow way that aligns with the definition used in the *Tallinn Manual*. It explains that coercion "means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue."[110] As noted above, proving that a state would not otherwise have pursued a course of action could be difficult. Furthermore, the only specific example of coercion provided is the use of force, which both provides little additional clarity and suggests that the Netherlands views the bar for what constitutes coercion to be relatively high.

B. United Kingdom

Then-U.K. Attorney General Jeremy Wright laid out the views of the United Kingdom on "Cyber and International Law in the 21st Century" in a May 2018 speech.[111] Wright, citing the ICJ's *Nicaragua* judgment, said that the principle of non-intervention protects against "external, coercive intervention in the matters of government which are at the heart of a state's sovereignty, such as the freedom to choose its own political, social, economic and cultural system."[112] Thus, like the Dutch focus on "exclusive" sovereign rights, Wright's emphasis on matters "at the heart" of sovereignty suggests that the United Kingdom takes a relatively narrow view of which activities are completely protected from intervention. Wright notes that the "precise boundaries of this principle are the subject of ongoing debate" and does not provide further explanation as to what he views as "coercion."[113] However, he does cite a few concrete examples of activities that the United Kingdom

106. Letter from the Dutch Minister of Foreign Affairs to the Parliament on the International Legal Order in Cyberspace (July 5, 2019) (available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [https://perma.cc/GF9L-5DT3]).

107. *Id.*

108. *Id.*

109. *See id.*

110. *Id.*

111. *See* Wright, *supra* note 15.

112. *Id.*

113. *See id.*

believes would violate the rule of non-intervention: "use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system."[114] The emphasis on altering results of an election, rather than just interfering by spreading disinformation, as well as on the *fundamental* operations of Parliament, provide additional evidence that the United Kingdom views the scope of the rule rather narrowly.

C. United States

The views of the United States on this issue are illustrated most thoroughly by two speeches: first by President Obama's State Department Legal Adviser Brian Egan in November 2016,[115] and then by President Trump's Department of Defense General Counsel Paul Ney in March 2020.[116] Egan and Ney provide a similar formulation of the rule to that of the United Kingdom. Also invoking *Nicaragua*, Egan states, "this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system."[117] He then describes it as a "relatively narrow rule of customary international law."[118] Ney only slightly tweaked this formulation by describing "the choice of political, economic, or cultural system" as one of a State's "core functions."[119] Ney also provided more clarity than Egan as to how the United States conceives of "coercion," noting, "[b]ecause the principle of non-intervention prohibits 'actions designed to coerce a State . . . in contravention of its rights,' it does not prohibit actions to which a State voluntarily consents."[120] By contrasting coercion with consent, Ney suggests that the U.S. view of coercion is slightly broader than the narrow Dutch emphasis on compulsion to change a specific policy, and may be closer to the Australian emphasis on control.

Furthermore, in the examples of prohibited interventions that they provide, Egan and Ney suggest that the U.S. view of political interventions might be slightly broader than the United Kingdom's. Egan notes that a cyber operation that "manipulates another country's election results" *or* "interferes with another country's ability to hold an election" would violate the

114. *Id.*

115. *See* Egan, *supra* note 7.

116. *See* Paul C. Ney, General Counsel, U.S. Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), (transcript available at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/N58M-MPWV]).

117. Egan, *supra* note 7.

118. *Id.*

119. Ney, *supra* note 116.

120. *Id.*

rule.[121] The latter phrase would suggest that a wider range of activities, including disinformation campaigns, might fall under the purview of the rule. Ney echoed this language about election interference in his 2020 speech.[122]

D. Australia

Australia provided a detailed account of its views on non-intervention in a working paper to the September 2019 U.N. Open Ended Working Group "on developments in the field of information and telecommunications in the context of international security."[123] On its face, the working paper suggests that Australia has an expansive view of the rule of non-intervention. It states, "A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely."[124] Australia provides a broader definition of coercion than the Dutch formulation in that it emphasizes a lack of "control" or ability to "govern."[125] As noted above, it is far easier to prove that an operation deprived a state of complete control over matters of governance than to prove that the operation forced a state to make a decision that it did not want to make. Australia's articulation of the first element is nearly identical to the formulation in *Nicaragua*, focusing on "matters that a state is permitted by the principle of state sovereignty to decide freely."[126] This articulation also lacks the additional qualifiers to sovereignty added by the Dutch ("exclusive") and British ("at the heart").[127] Australia does cite the same examples of illegal interventions that Wright used: altering election results, intervening in the "fundamental operation of Parliament," and impacting the "stability of States' financial systems."[128] Nonetheless, overall, the wording used in this statement suggests a conception of the rule that would deem a broader range of activities to be illegal.

121. Egan, *supra* note 7.

122. *See* Ney, *supra* note 116.

123. Australian Mission to the United Nations, Australian Paper to the U.N. Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2019) (available at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf [https://perma.cc/U7TK-VDHZ]) [hereinafter Australian Paper].

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

E. France

The French Ministry of Defense also released a major statement on the application of international law to cyberspace in September 2019. The statement articulates the rule of non-intervention in a vague but broad way: "Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention."[129] It is notable that the statement does not use the word "coercion," instead using the far less precise term "harm," which seems to encompass a far broader range of activities.[130] Furthermore, it defines the scope of sovereign activities in an expansive way, noting that any harm to France's "political, economic, social and cultural system," rather than just the "choice" of such a system, might constitute a violation.[131] One could imagine this formulation of the rule of non-intervention being used by authoritarian states to justify censorship and argue that any outside information would constitute "harm" to its "social and cultural system."[132] It is also important to note, however, that the entire statement is qualified by the word "may" in the final clause, suggesting that France's views on this are not definitive and may continue to evolve.[133] Nonetheless, it is important to highlight the sweeping implications of a literal interpretation of this statement, which would lower the bar of illegality significantly as compared to, for example, the Dutch formulation.

F. Iran

The General Staff of the Iranian Armed Forces released a Declaration in July 2020 "Regarding International Law Applicable to the Cyberspace," which laid out in detail Iran's conception of non-intervention's applicability to cyberspace.[134] The Declaration defines the scope of sovereign activities in a similar way to the French statement, noting that threats "against the per-

129. French Ministry of Defense, International Law Applied to Operations in Cyberspace 7 (2019).

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

134. *General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat*, NOURNEWS (Aug. 18, 2020), https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat [https://perma.cc/64J9-9MBK] [hereinafter Iran Declaration]. This statement was released through a number of news sources tied to the Iranian government, including the source cited above. It has been cited as credible and reflective of Iranian government views by a number of reputable sources, including in an article by Professor Michael Schmitt, a leading expert on these topics. *See* Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions—Part II: Iran*, Articles of War (Aug. 27, 2020), https://lieber.westpoint.edu/iran-international-cyber-law-positions/?s=09 [https://perma.cc/SM6F-MVAX]; *see also* Przemyslaw Roguski, *Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace*, Just Sec. (Sept. 3, 2020), https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/ [https://perma.cc/5ZJY-BREA].

sonality of state or political, economic, social, and cultural organs of it through cyber and any other tools are regarded as unlawful."[135] The Declaration then emphasizes, in language mirroring the 1981 Declaration, that states have "the inherent right to the full development of information system and mass media and their employment, without intervention."[136] Along with this broad conception of the protected sovereign domain of media activities, which goes beyond those of the statements discussed above, the Declaration also describes coercion broadly as "impediment [of], denying, and or restricting" the exercise of sovereignty.[137] In combination, these definitions suggest that Iran views cyber and media governance as an exclusively sovereign domain that states have the right to control without "impediment."

Indeed, the examples of unlawful intervention included in the Declaration illustrate that Iran views non-intervention as applying to a sweeping range of cyber activities. The Declaration mentions not only "cyber manipulation of elections," but also "engineering the public opinions on the eve of the elections" and "sending mass messages in a widespread manner to the voters to affect the result of the elections in other states" as examples of "forbidden intervention."[138] This suggests that the Iranian military would view any state actions to share information to its electorate—both legitimate information and disinformation—as unlawful. Iran's very broad conception of non-intervention would thus make unlawful most forms of political interference in another state.

G. China

Like Australia, China also submitted a working paper to the September 2019 U.N. Open Ended Working Group. Like the Iranian Declaration, this Chinese paper would outlaw most forms of cyber political interference under the rule of non-intervention. China affirms its support for the rule of "non-intervention in the internal affairs of other states," describing it as one of the principles that is a "cornerstone of a just and equitable international order in cyberspace."[139] Although it does not define the rule of non-intervention directly, the paper does talk about similar concepts that underscore the very broad way in which China conceives of unlawful intervention. China argues that, "States should exercise jurisdiction over the ICT [information and communications technology] infrastructure, resources as well as ICT-related activities within their territories. States have the right to make ICT-related

135. Iran Declaration, *supra* note 134.
136. *Id.*
137. *Id.*
138. *Id.*
139. China's Submissions to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2019) (available at https://www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf [https://perma.cc/SC5M-DR27]) [hereinafter China's Submissions].

public policies consistent with national circumstances to manage their *own* ICT affairs."[140] This indicates that China, like Iran, views internet governance as an exclusively sovereign matter in which other states cannot intervene. The paper further emphasizes, "States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability."[141] The use of the word "stability" frames the domain of protected activities extremely broadly.[142] Likewise, "undermine" is far broader than "coerce" and would seem to encompass other types of activities that do not either deprive the target state of control or force it to make a decision that it would not otherwise make.[143] The breadth of this formulation is consistent with China's emphasis on "cyber sovereignty" and its efforts to restrict the information that penetrates its networks from outside the country.[144]

IV. Comparing the Definitions: Which Political Operations in Cyberspace Would Violate the Rule of Non-Intervention?

The variation in the language used to discuss the rule of non-intervention indicates that states may disagree over whether certain cyber operations violate the rule. This section will examine some of these potential disagreements by applying each state's formulation of the rule to a series of hypothetical cyber operations that might amount to an unlawful intervention. It will focus in particular on political interference, or in the language of *Nicaragua*, operations that impact the "choice of a political . . . system."[145] Depending on how states classify the scope of this "choice" that is immune from foreign intervention, or the degree of "coercion" that is necessary to constitute an unlawful intervention in this choice, certain operations may fall below the threshold of illegality in some states' conceptions but not others.

140. *Id.* (emphasis added).
141. *Id.*
142. *Id.*
143. *Id.*
144. *See* Jun Mai, *Xi Jinping Renews 'Cyber Sovereignty' Call at China's Top Meeting of Internet Minds*, S. China Morning Post (Dec. 3, 2017), https://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top [https://perma.cc/ML9J-XZCT] (noting that the website Google and a number of apps on Apple's App Store, among other online content, are banned in China).
145. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 108 ¶ 205 (June 27).

Table 2: Is the Cyber Operation Illegal?

	Dutch	U.K.	U.S.	Australia	France	Iran	China
Altering Election Results	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disrupting Government Operations	Maybe	Yes	Yes	Yes	Yes	Yes	Yes
Politically Motivated Doxing	Maybe	Maybe	Maybe	Yes	Yes	Yes	Yes
Covert Disinformation Campaigns	No	No	Maybe	Maybe	Yes	Yes	Yes
Open Propaganda Campaigns	No	No	No	No	Maybe	Maybe	Maybe

A. Altering Election Results

All of the states surveyed would likely agree that a cyber operation that alters election results—by, for example, hacking into voting machines and changing the vote counts—would violate the rule of non-intervention. The United States, the United Kingdom, Iran, and Australia all specifically cite such operations as examples of unlawful interventions.[146] The Netherlands cites "national elections" as an example of internal affairs that are protected from intervention.[147] Even with the high bar that the Netherlands sets for coercion—activity that compels a state to make choices that it would not otherwise make—altering election results to change the winner clears that bar because it alters the choice that the state would otherwise have made.[148] Altering election results without the target state's consent would also seem to "harm" the "political system," as the French define illegal intervention, or "undermine" political "stability," as the Chinese define it.[149]

B. Disrupting Government Operations

Cyber intrusions into another government's servers that disrupt the state's ability to conduct governmental operations would also constitute an illegal intervention under most states' definitions. Such intrusions could include, for example, distributed denial of service operations that aim to deny a user access to a network by flooding the network with requests.[150] Such operations often cause no physical damage and thus would likely fall below the

146. *See supra* Part III.

147. Letter from the Dutch Minister of Foreign Affairs to the Parliament, *supra* note 106.

148. *See id.*

149. *See supra* Part III.

150. *See* William Mattessich, Note, *Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage*, 54 Colum. J. Transnat'l. L. 873, 884 (2016).

threshold of use of force.[151] However, they might still violate the rule of non-intervention. Under the Dutch definition of coercion, if the operation is designed to compel a state to change its policies in a particular area by shutting down the government's ability to function, it might violate the rule. If it merely disrupts governmental operations without a demand for policy changes, it might not violate the rule under the Dutch conception. However, such operations would violate the rule of non-intervention under every other country's definition. The United Kingdom and Australia directly cite disrupting the operations of parliament as an example of an illegal intervention.[152] It would also probably be illegal under the U.S. definition, which is similar to that of the United Kingdom, as well as the broader definitions used by France, Iran, and China.

C. Politically Motivated Doxing

During the 2016 election, Russian hackers stole and leaked sensitive personal emails sent by Hillary Clinton's campaign chairman John Podesta, a practice known as doxing.[153] Ido Kilovaty has termed this specific type of politically motivated doxing, "Doxfare."[154] While Russia's aim in doxing Podesta during the 2016 election was to spread unfavorable information about the Clinton campaign in order to help Trump win the election,[155] one could imagine other forms of Doxfare. For example, one state could hack and leak embarrassing information about high-ranking government officials in another state in order to coerce that state to change its policies. Under the Dutch definition of non-intervention, such an operation would be illegal if it can be proven that the operation sought to directly alter a state's decision on a matter within the state's "exclusive authority," such as the recognition of states. This could include, for example, if China conducted a doxing operation against a foreign leader to compel her to recognize China's claims in the South China Sea. Even if such an operation is not directly linked to a specific attempt to change another state's behavior, it would still likely have the effect of intimidating the state in such a way as to deprive it of complete policymaking "control," or to "harm," "restrict," or "undermine" sovereign decisionmaking. Thus, under the Australian, French, Iranian, and Chinese conceptions of non-intervention, politically motivated doxing would likely violate the rule. While it is less clear that such an operation would violate the vaguer U.S. and U.K. definitions of coercion, one could argue that manipulating a high-level government official's decision-making with-

151. *See id.* at 886.

152. *See* Wright, *supra* note 15; Australian Paper, *supra* note 123.

153. Robert S. Mueller III, U.S. Dep't of Justice, Report on the Investigation Into Russian Interference in the 2016 Presidential Election 4 (2019).

154. *See* Kilovaty, *supra* note 18, at 152.

155. *See* Mueller, *supra* note 153, at 4.

out their "consent" constitutes "coercive" intervention into matters "at the heart" of sovereignty.

D. Covert Disinformation Campaigns

While less inherently coercive, a sophisticated and coordinated disinformation campaign aimed at changing another state's behavior could violate the rule of non-intervention. In addition to hacking and releasing stolen emails during the 2016 campaign, Russian "trolls" engaged in an extensive campaign on social media to share and amplify false, damaging stories about Hillary Clinton.[156] Some scholars have suggested that this campaign crossed the line from mere "propaganda" into coercive intervention. As Schmitt argues, "the covert nature of the troll operation deprived the American electorate of its freedom of choice by creating a situation in which it could not fairly evaluate the information it was being provided . . . thus [its] ability to control [its] governance [ ] was weakened and distorted."[157] Under the high bar set by the Dutch conception of non-intervention, it would be difficult to prove that such an operation could "compel" a state to choose a particular course of action; that is, it would be hard to prove that the disinformation campaign swayed an election result. However, there is merit to Schmitt's argument that such an operation could deprive a state of "freedom of choice" and thus violate the Australian conception of non-intervention. Given Iran's statement that "sending mass messages in a widespread manner to the voters" constitutes unlawful intervention, disinformation campaigns would likely violate Iran's definition of the rule.[158] Such an operation would also arguably "harm" or "undermine" elections so as to violate the broad French and Chinese definitions. Former U.S. State Department Legal Adviser Brian Egan's statement notably refers to an unlawful operation as one that *either* "interferes with another country's ability to hold an election *or* that manipulates another country's election results."[159] Under a broad reading of "ability to hold an election," one could argue that a coordinated disinformation campaign violates the U.S. conception of non-intervention. Former U.K. Attorney General Wright's statement refers more directly to altering election results, and so it is harder to argue that a disinformation campaign would violate the U.K. conception of non-intervention.[160]

E. Open Propaganda Campaigns

Of the five examples presented here, open propaganda campaigns are least likely to violate the rule of non-intervention, as there is ample practice of

156. *See id.*
157. Schmitt, *supra* note 104, at 51.
158. *See* Iran Declaration, *supra* note 134.
159. Egan, *supra* note 7 (emphasis added).
160. *See* Wright, *supra* note 15.

states seeking to infiltrate other states with factual information or opinion. For example, the United States started Radio Free Europe/Radio Liberty during the Cold War as a means to spread news to people living under communist regimes, and it continues to broadcast in numerous countries.[161] Russia Today and Sputnik, as well as China Daily and Xinhua, aim to spread news in a way that favorably depicts Russia and China, respectively.[162] Many scholars have distinguished "propaganda" from coercive interventions.[163] As compared to covert disinformation campaigns, citizens can more fairly evaluate the source of the information, and it is harder to argue that they have been deprived of "control" over their decision-making.[164] Open propaganda campaigns—even those that share false or exaggerated information—are thus unlikely to violate the U.S., U.K., or Australian conceptions of non-intervention (or the far stricter Dutch definition). One could make the argument under the French or Chinese definitions that propaganda "harms" or "undermines" a state's ability to make sovereign decisions.[165] In particular, the Chinese definition of "cyber sovereignty" entails the ability to have complete control over information flows on the internet in one's territory.[166] One could also argue that any form of "mass messages" to voters, whether true or false, would constitute a violation under the Iranian definition.[167] However, while one could make a semantic argument that propaganda violates the rule under these definitions, extensive state practice, including by China itself, directly counters the argument that the customary rule of non-intervention makes such activities unlawful.

Conclusion: Normative Uncertainty or Improved Deterrence?

On the surface, the preceding analysis suggests that the meaning of non-intervention remains highly contested. Indeed, whether a cyber operation that interferes in another country's political system is deemed illegal would depend upon which state's definition is used as a baseline. All countries would probably agree that altering the vote count in an election would constitute an unlawful intervention. At the other end of the spectrum, it is hard to argue that openly spreading propaganda violates the rule. While doxing and disinformation campaigns may be clear violations of non-intervention under the broader French, Iranian, and Chinese definitions, they may not

161. *See* A. Ross Johnson, *History*, Radio Free Europe/Radio Liberty, https://pressroom.rferl.org/history [https://perma.cc/P8XG-YWME] (last visited Nov. 17, 2020).

162. *See* Christopher Walker, *How Anti-Democratic Propaganda Is Taking Over the World*, Politico (Mar. 3, 2017), https://www.politico.com/magazine/story/2017/03/anti-democratic-propaganda-beijing-moscow-214858 [https://perma.cc/U4DN-KAQR].

163. *See* Tallinn Manual, *supra* note 55, at 318; Schmitt, *supra* note 104, at 46; Jamnejad and Wood, *supra* note 13, at 374.

164. Australian Paper, *supra* note 123.

165. French Ministry of Defense, *supra* note 129; China's Submissions, *supra* note 139.

166. Mai, *supra* note 144.

167. Iran Declaration, *supra* note 134.

cross the line of illegality under the narrower Dutch and U.K. definitions. Even cyberattacks on essential government infrastructure may not violate the Dutch conception of non-intervention.

One could conclude from this analytical confusion that, as applied to cyber political interference, non-intervention will maintain its historical position as a norm that states universally recognize but that is the subject of broad disagreement as to its applicability. Just as during the Cold War, states may claim violations of the rule but disagreements about its content may stymie efforts to enforce it.[168] States may respond to the normative uncertainty about international rules in cyberspace by regarding such rules as optional.[169] While this challenge is not unique to cyberspace, "[i]t is the combination of contested rules and low enforcement prospects that renders cyberspace exceptionally difficult to regulate," Dan Efrony and Yuval Shany argue.[170]

Despite this uncertainty about its precise applicability, however, non-intervention arguably has broader global support in the context of cyber political interference than in any other context. During the Cold War, non-intervention was a tool utilized primarily by developing countries against interventions by superpowers.[171] Humanitarian interventions have also been criticized as violating the rule of non-intervention.[172] As noted above, however, the United States and some other Western democracies, who have historically been on the side of refuting that operations violate the rule of non-intervention, have explicitly argued for applying non-intervention to cyber political interventions. Furthermore, particularly in the case of the French and Australian conceptions, but also in a broad reading of the U.S. conception, some of these states have articulated quite expansive views of the rule of non-intervention.

This growing recognition by Western democracies of non-intervention's applicability to political interference may in part be linked to these states' vulnerabilities to such interference, particularly in cyberspace. As Jack Goldsmith and Stuart Russell point out, "digital networks in an open society not only make it easier to spread false or disruptive information; they also make it harder to counter the false or disruptive information with truthful, coherent information."[173] As a result, the United States and other democracies with open internet networks and a relatively unregulated news media are more vulnerable to doxing and disinformation campaigns than authoritarian states. President Barack Obama acknowledged this, noting, "We do have some special challenges, because . . . we have a more open

168. *See* Damrosch, *supra* note 6, at 2.

169. *See* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 648 (2018).

170. *Id.* at 652.

171. *See* Damrosch, *supra* note 6, at 2.

172. *See* Jamnejad & Wood, *supra* note 13, at 360.

173. Goldsmith & Russell, *supra* note 5, at 10.

society and engage in less control and censorship over what happens over the Internet."[174]

Thus, the United States may be in the rare position of advocating for stronger rules of international law that would constrain its own behavior. The United States has historically been criticized for its inconsistency toward rules of international law, and in particular for its reluctance to constrain its own behavior.[175] Scholars have described international law as a resource for smaller states to constrain the behavior of countries like the United States, as "an instrument for the critique of power."[176] In this area in which they are asymmetrically vulnerable, however, powerful countries like the United States, United Kingdom, and France have all argued, in high-level statements, that states should seek to clarify how the rule of non-intervention should apply.[177]

If such an effort to clarify the rule is successful, it could serve as a greater deterrent to cyber meddling in other countries' political systems. If these states translate their desire for clarity into a binding Security Council resolution, or soft law instruments such as a General Assembly resolution or report from the GGE, states would have a clearer basis for claiming violations of international law. They might feel more emboldened to respond to cyber interventions with a range of countermeasures, including non-cyber measures like freezing assets or suspending trade agreements, that could deter the intervening state from conducting the operation in the future.

However, the effectiveness of this deterrent will depend upon which conception of the rule of non-intervention ultimately prevails. If something approximating the Dutch vision is adopted, states will feel emboldened to conduct a range of operations that fall below the legal threshold, including Doxfare and covert disinformation campaigns, and the target state will not legally be able to respond with countermeasures. This world would not differ substantially from the status quo; the difference, however, would be that operations like the Russian interference in the 2016 U.S. election would become legally permissible, rather than legally ambiguous. This could in turn lead to similar political interventions in cyberspace across the globe. Furthermore, states would likely hesitate to respond with countermeasures like violating treaty agreements, because such countermeasures would not be

174. Barack Obama, Year-End Press Conference (Dec. 16, 2016) (transcript available at https://www.presidency.ucsb.edu/documents/the-presidents-news-conference-1139 [https://perma.cc/2BT3-BDEJ]).

175. *See* Harold Hongju Koh, *America's Jekyll-and-Hyde Exceptionalism*, *in* AMERICAN EXCEPTIONALISM AND HUMAN RIGHTS 111 (Michael Ignatieff ed., 2005). As an example, Koh notes, "Even while asserting its own right to preemptive self-defense, the United States has properly hesitated to recognize any other country's claim to engage in forced disarmament or preemptive self-defense in the name of homeland security." *Id.* at 128.

176. Martti Koskenniemi, *What Is International Law For?*, *in* INTERNATIONAL LAW 28, 46 (Malcolm D. Evans ed., 5th ed. 2018).

177. *See, e.g.*, Egan, *supra* note 7 ("States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace.").

legally justified if the political intervention did not constitute a breach of international law.

Alternatively, a more robust definition of the rule of non-intervention could help to protect elections from such interventions. If a definition closer to the Australian and French conceptions is adopted and activities like Doxfare and covert disinformation campaigns are strictly prohibited under international law, states will hesitate to conduct such operations for fear of retaliation through countermeasures. Russia may ultimately calculate that the risks of countermeasures, such as suspended trade agreements or proportional cyberattacks targeting its infrastructure, outweigh the benefits of future political interference. The deterrent effect could be particularly strong if more countries endorse the concept of collective cyber countermeasures, promoted by Estonian President Kersti Kaljulaid in a 2019 speech.[178] As Schmitt argues, "States that lack the capacity to confidently deal with hostile cyber operations on their own would want collective cyber countermeasures to be on the table in order to deter powerful opponents from targeting them in cyberspace and to respond effectively should deterrence fail."[179]

Thus, those states that are interested in applying the rule of non-intervention to cyberspace must seek to close the gaps in conceptions of the rule's scope. Given the scarcity of opinio juris on the applicability of non-intervention to cyber operations, additional statements and additional states are needed to help fill in these gaps and determine which definition of the rule of non-intervention ultimately prevails. The fear of suffering the same fate as Hillary Clinton's 2016 U.S. presidential campaign may be strong enough to motivate leaders—including in powerful countries like the United States—to finally clarify and strengthen this famously ambiguous rule of international law.

178. Michael Schmitt, *Estonia Speaks Out on Key Rules for Cyberspace*, JUST SEC. (June 10, 2019), https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/ [https://perma.cc/PF6W-C2AF].

179. *Id.*