Influence operations in cyberspace

On the applicability of public international law during influence operations in a situation below the threshold of the use of force

Pijpers, B.M.J.

Publication date
2022

Chapter 3

CHAPTER 3: SOVEREIGNTY AND NON-INTERVENTION –THE LEGAL FRAMEWORK

While cyber operations which have the aim to influence the electoral process in a specific State will not involve the threat or use of armed force, as was explained previously, this does not imply that such operations cannot result in serious violations of international law. In particular the international legal rules pertaining to the respect for the sovereignty of other States can be affected by such operations of they have certain characteristics and consequences.

This chapter distinguishes between coercive and non-coercive interferences with sovereignty. Though a violation of the prohibition of intervention is *ipso facto* a violation of sovereignty, the two notions of sovereignty and non-intervention will be assessed separately.[1] Coercive interference in the reserved domain of a State is an intervention, and non-coercive infringement could amount to a violation of sovereignty. This chapter will assess the legal bases for both sovereignty and non-intervention in international law, the core characteristics, and the scope and intent of sovereignty and non-intervention in cyberspace.

This chapter concludes with answering the second sub-question of this research: *"Identify how rules and principles of international law, related to sovereignty and non-intervention apply, in cyberspace, to States in their conduct with other States or political systems?"*

Section 3.1.: International law in cyberspace

"The point is that virtual entities point to their own potency:
the virtual sovereign did not need to be crowned"[2]

In general States agree that international law applies to cyberspace but,[3] nevertheless, there is room for interpretation. The question whether international law applies to cyberspace

1 As is common in legal writings, see e.g. German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace," 2021. or Michael N. Schmitt, "Foreign Cyber Interference in Elections," *International Law Studies (Naval War College)* 97, no. 739 (2021).

2 Marilyn Strathern, "Abstraction and Decontextualization:An Anthropological Comment," in *Virtual Society? : Technology, Cyberbole, Reality*, 2002, 302–13. Strathern. p. 305.

3 See United Nations GGE 2013 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/68/98," 2013. And the United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174," vol. 12404, 2015.; United Nations General Assembly, "Final Substantive Report," *Open-*

has been subject to legal discourse, and 'how' this must be done or whether additional legislation is needed, still is.[4] In this section a description is given of the applicability of international law to cyberspace, how it applies to cyberspace, and what challenges remain.

In the early days of cyberspace Barlow announced the independence of cyberspace, declaring sovereignty to the domain,[5] based on its a-territorial, boundless and ubiquitous character. However, since the physical network layer of cyberspace (i.e. computers, cables, routers) is part of the territory of the State, and within disposition and territorial jurisdiction of a State, Barlow's declaration proved flawed from a legal perspective.[6] More broadly, also the persons who use cyberspace as a means of communication are located in the territory of a State or subject to the jurisdiction of one or more States.

At present, there is agreement *that* international law applies to cyberspace. The legal opinions of States underlying this have been provided via several unilateral statements,[7] collectively via reports of international organisation,[8] or via ad hoc declarations.[9]

The question of *how* international law should be applied to cyberspace remains a matter of debate.[10] The discourse is prominent between China and the Russian Federation (RF) on the one hand, and Western countries on the other.[11] Though both sides agree that legal lacunas and differences in interpretation exist, the views on how to bridge them differs, ranging from

Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021. pp. 5-6.

4 See e.g. the considerations of Kilovaty and Watts on this topic in Just Security, Ido Kilovaty, "The Democratic National Committee Hack: Information as Interference," *Just Security*, 2016.; Sean Watts, "International Law and Proposed: U.S. Responses to the D.N.C. Hack," *Just Security*, 2016.

5 John P Barlow, "A Declaration of the Independence of Cyberspace," *Choice Reviews Online* 48, no. 03 (1996): 2.

6 Harold Hongju Koh, "International Law in Cyberspace," *Faculty Scholarship Series* 4854 (2012): 1–9. pp. 2-3; James R Crawford, *Brownlie's Principles of Public International Law*, 9th ed. (Oxford, United Kingdom: Oxford University Press, 2019). pp. 191-192.

7 Ministry of Foreign Affairs, "Letter to the Parliament on the International Legal Order in Cyberspace" (2019).; Australian Government Department of Foreign Affairs and Trade, "Public Consultation: Responsible State Behaviour in Cybersapce in the Context of International Security at the United Nations," no. November (2019).; Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace," 2019.; Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace.

8 United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174."; United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security - A/RES/70/237," 2015.

9 Internet Governance Forum, "Paris Call for Trust and Security in Cyberspace," 2018.

10 Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," in *Governing Cyberspace*, ed. Dennis Broeders and Bibi van den Berg, 2020, 45–64. p. 45; The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 2011. p. 9.; See also the Cuban resentment regarding the proposed 2017 UN GGE conclusions: Representaciones Diplomaticas de Cuba, "71 UNGA : Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2017.

11 Zhixiong Huang and Kubo Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," *Chinese Journal of International Law* 16, no. 2 (2017): 271–310. pp. 275-278.; United Nations GGE 2017 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A /72/327" 13985, no. August (2017).

drafting new conventions to establishing cyber norms, based on State practice. The debate has also entered the academic realm where scholars have identified hiatus, some of whom arguing that new legislation is needed.[12] Hollis is doubtful whether existing international law is suited to regulate the effects on the cognitive dimension and pleas for new rules for cyberspace due to 'problems of uncertainty, complexity and insufficiency'.[13] Tsagourias argues that ideally new legislation must be considered, but does not assess this a viable option.[14] Also Schmitt concludes that 'the prospects for *new* laws applicable to cyberspace are slim'.[15]

A lack of agreement on how international law should be applied to cyberspace may result in so-called grey areas,[16] examples of which are the discourse on whether sovereignty is a binding legal obligation in cyberspace, as will be discussed in § 3.3.3, or on the attribution of activities of non-State actors to States. Though States are the first and primary subjects of public international law,[17] they are not the sole actors in the international arena. Attributing actions to States is challenging in general,[18] especially in cyberspace,[19] not least due to numerous supporting, routing or transferring States involved.
These grey areas of international law are not merely 'susceptible to exploitation when conducting cyber operations',[20] but lack of clarity in attributing a violation of international law or uncertainty on whether a norm of international law is binding, impacts the international legal system as a whole since it denies States the possibility to invoke redress.

12 Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations," *International Review of Law, Computers and Technology* 32, no. 1 (2018): 37–57. p. 55, arguing for a treaty-based improvement of the security of communication in the digital domain.

13 Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46. p. 44.

14 Nicholas Tsagourias, "The Legal Status of Cyberspace," in *Research Handbook on International Law and Cyberspace*, 2015, 13–29. p. 29.

15 Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law," *Texas National Security Review* 3, no. 3 (2020). p. 47.

16 Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law* 42, no. 2 (2017): 1–21. pp. 4-19.

17 Malcolm N. Shaw, "International Law" (Cambridge, U.K. ; Cambridge University Press, 2003). p. 175.; Antonio Cassese, *International Law in a Divided World* (Clarendon Press Oxford, 1986). p. 74. See also: International Law Commission, "Draft Declaration on Rights and Duties of States," General Assembly Resolution 375 (IV) § (n.d.). The preamble states that "the States of the world form a community governed by international law"; Robert Jennings and Arthur Watts, *Oppenheim's International Law*, 9th ed., vol. I (Longman, 2008). p. 14; Reparations for Injuries suffered in the service of the United Nations - Advisory Opinion, ICJ Reports (1949). p. 179.

18 Actions can be attributed to a State if a person or entity is empowered by the State; if the State explicitly acknowledges the act (e.g. RIIA Rainbow Warrior case) or if the entity operates under the instructions of the State (ICJ Nicaragua, Bosnian Genocide & ICTY Tadic Appeal case). See: Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations." pp. 38-39; James Crawford, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries*, ed. James (James Richard) Crawford (Cambridge: Cambridge University Press, 2002). p. 91. See also § 1.2.3.

19 Björnstjern Baade, "Fake News and International Law," *European Journal of International Law* 29, no. 4 (2018): 1357–76. pp. 1361-1362.

20 Schmitt, "Grey Zones in the International Law of Cyberspace." p. 3.

Based on Article 2 of the Articles on State Responsibility,[21] an international wrongful act consists of a breach of an international obligation[22] attributable to a State.[23] Repairing a breach of an international rule resulting in the violation of an injured State cannot be redressed if it is impossible to attribute the act to a State.

Existing legal lacunas, including the lack of clarity on attribution, reparation and norms,[24] fuel the discourse on how international law applies to cyberspace, and even whether or not there should be specific new conventions on cyberspace.[25] In 2018 and 2019 respectively, the United Nations (UN) established the 'Open Ended Working Groups' (OEWG)[26] and the 6th iteration of the UN GGE[27] to further develop norms, rules and principles on confidence building measures, and on how international law applies to cyberspace.[28] Apart from the lack of State practice, developing norms is challenging given the failure of the 2017 UN GGE rounds,[29] and the fact that the OEWG acts in parallel with the UN GGE.

In sum, it is widely accepted *that* the existing body of international law (*lex lata*) is applicable to cyberspace. The remaining question is *how* public international law should be applied to cyberspace.[30]

21 Crawford, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries*. p. 81.

22 Crawford. p. 81. See also: United States Diplomatic and Consular Staff in Tehran (USA v Iran), Judgment, ICJ Reports 3 (1980).; PCIJ, Phosphates in Morocco - Preliminary Objections, Series A/B Collection of Judgments, Orders and Advisory Opinions (1938). p. 28.

23 The notions of sovereignty and non-intervention only applies to relations between States. Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Second ed. (Cambridge, United Kingdom ; SE - xli, 598 pages ; 24 cm: Cambridge University Press, 2017). Rule 33, p. 175. Though Article 2(7) of the UN Charter prohibits the UN and its agencies 'to intervene in matters which are essentially within the domestic jurisdiction of any state', meaning that the prohibition of intervention also accounts for alliances or collections of States. Article 2(7) does not apply to NSAs.

24 Related to attribution or remedies for victim (or injured) States, see: François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?," *Israel Law Review* 52, no. 3 (2019): 295–326. pp. 317-325.

25 Iran Minstry of Foreign Affairs, "Intervention by Delegation of the Islamic Republic of Iran on International Law," (2020). The Iranian delegation argues in their intervention at the OEWG that "What is left is a legally binding instrument to fill the legal gaps arising from unique features of ICTs, including the wider possibilities for its use and misuse, from one side, and from the other side, the limitations of existing international law."

26 United Nations General Assembly, "Resolution on Establishment of OEWG - A/RES/73/72," 2018.

27 United Nations General Assembly, "Resolution of Establishment of UN GGE - A/RES/73/226," *UN*, 2019.

28 Dan Efrony, "Entering the Third Decade of Cyber Threats: Toward Greater Clarity in Cyberspace," *Lawfare*, no. December 2018 (2019).

29 Alex Grigsby, "The End of Cyber Norms," *Survival* 59, no. 6 (2017): 109–22. p. 113.

30 See Sheetal Kumar and Lea Kaspar, "Reporting Back from the Second Substantive OEWG Meeting," golbal Partners Digital, 2020, https://www.gp-digital.org/reporting-back-from-second-substantive-oewg-meeting/.

Section 3.2.: Infringements of Sovereignty

"The man in the desert is free, he is sovereign, he can do nothing because he has no power. To talk about sovereignty in the absence of power is to live in a world of fiction."[31]

States' activities in cyberspace do not solely violate public international law when force is used, but also when the rules and principles of international law, related to sovereignty and non-intervention are breached. Before addressing sovereignty (§ 3.3) and intervention (§ 3.4) this section draws a line of demarcation between the various sorts of infringements in other States, ranging from activities applying the use of armed force to minimal violation of sovereignty, thereby emphasizing the boundaries of this research.

An infringement in the sovereignty of a State may differ range in intensity from a mild unintended violation of the territory of another State to a coercive act, even constituting the use of armed force.

The different forms of infringement are interrelated. The unauthorised use of (armed) force is *ipso facto* a breach of the prohibition of intervention and also a violation of the sovereignty of the State. In the 1986 *Nicaragua* Case,[32] it was stated that the 'principle of respect for territorial sovereignty inevitably overlaps with those of the principles of the prohibition of the use of force and of non-intervention'.[33] Also in the 2005 *Armed Activities* Case, the International Court of Justice (ICJ) 'accordingly concludes that Uganda has violated the sovereignty and also the territorial integrity of the Democratic Republic of Congo (DRC). Uganda's actions equally constituted an interference in the internal affairs of the DRC and in the civil war raging there. The unlawful military intervention by Uganda was of such a magnitude and duration that the Court considered it to be a grave violation of the prohibition on the use of force expressed in Article 2, paragraph 4, of the Charter'.[34]

International legal rules related to infringements and the use of force have evolved considerably and continuously over the past century.[35] Since the enactment of the 1945

31 Lord Heseltine, November 2018 interview during parliamentary Brexit discussions https://twitter.com/haggis_uk/status/1062672007081484288

32 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Para 195, pp. 104-105.

33 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 251. p. 128.

34 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports (2005). Para 165, p. 227.

35 The ICJ also acknowledges this related to terms in treaties, see Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua) Judgment, ICJ Reports 213 (2009). Para 66, p. 243. See also: Terry D. Gill and Kinga Tibori-Szabó, *Twelve Key Questions on Self-Defense against Non-State Actors – and Some Answers*, *International Law Studies (Naval War College)*, vol. 95, 2019. pp. 469-474.

Charter of the UN, the use of force is prohibited and this includes any form of armed intervention against another State not falling under either of the two exceptions of the prohibition, namely self-defence and a mandate from the UN Security Council.[36]

Coercion is an essential element of the principle of non-intervention, as will be elaborated on in § 3.4. Coercion may entail the use of force,[37] but since not all forms of coercion involve the use of force there are two separate rules. One is the prohibition of the threat or use of force as recognised in Article 2(4) of the UN Charter,[38] which covers the armed intervention. The other rule is related to coercive intervention in general which includes various forms of political, economic or diplomatic coercion.[39] In this sense, an intervention by armed force is a specific type of intervention, subject to a separate rule both under the UN Charter and customary international law.

Though an armed attack as recognised in Article 51 of the UN Charter, or the prohibition of the use of force as laid down in Article 2(4) UN Charter, constitute a breach of the non-intervention principle[40] as well as an unlawful breach of sovereignty of a State, there is granularity in these infringements.[41] Moreover, the reverse is not the case: a violation of sovereignty such as unauthorised overflights,[42] or exercising jurisdiction on foreign territory without permission,[43] does not per se constitute a breach of the prohibition of the use of force. Additionally, the various categories of infringements also have different consequences

36 Vaughan Lowe, *International Law*, Clarendon Law Series (Oxford: OUP Oxford, 2007). p. 103.

37 The incorporation of the prohibition of the use of force into the non-intervention principle was underscored in the *Corfu Channel* Case: 'the alleged right of intervention, as the manipulation of a policy of force (...) cannot (...) find a place in international law' Corfu Channel Case (merits) - Judgment of 9 April 1949, ICJ Reports (1949). p. 35. and was later reiterated in the *Nicaragua* Case, Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 106.

38 Philip Kunig, "Prohibition of Intervention," *Max Planck Encyclopedia of Public International Law*, no. April (2008). Para A.1 (b); Chatham House, "The Principle of Non-Intervention in Contemporary International Law: Non-Interference in a State's Internal Affairs Used to Be a Rule of International Law: Is It Still?," no. February 2007 (2007): 1–8. p. 2; Apart from being recognised in art 2(4) UN Charter, the prohibition of the use of force is customary international law, having the character of jus cogens. See: Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. para 188-190, pp. 99-101; Helal calls this the coercion continuum, meaning that force is an extreme form of coercion, see Mohamed Helal, "On Coercion in International Law," *SSRN Electronic Journal*, no. 475 (2019). pp. 53 ff.

39 United Nations, "Article 52: Resolution Relating To The Declaration On The Prohibition Of Military, Political Or Economic Coercion In The Conclusion Of Treaties," Commentary on the 1969 Vienna Convention on the Law of Treaties § (1969).; Cassese, *International Law in a Divided World*. p. 147.

40 Which also applies to cyberspace. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66(22) p. 319 states that cyber use of force by one State against another is always coercive and therefore constitutes intervention.

41 Rosalyn Higgins, "Intervention and International Law," in *Intervention and International Law*, ed. Hedley Bull (Clarendon Press Oxford, 1984), 272–83. p. 281; See also: Antonios Tzanakopoulos, "The Right to Be Free from Economic Coercion," *Cambridge Journal of International and Comparative Law* 4, no. 3 (2015): 616–33. p. 622; Helal, "On Coercion in International Law." pp. 53 ff; Allison Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign," *Boston University International Law Journal* 37, no. 171 (2019): 183–210. pp. 195-201.

42 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. para 251, p. 128.

43 Jennings and Watts, *Oppenheim's International Law*. Para 119, pp. 385-390.

for redress. The lawful response to an armed attack differs fundamentally from response options related to a violation of territorial integrity.[44]

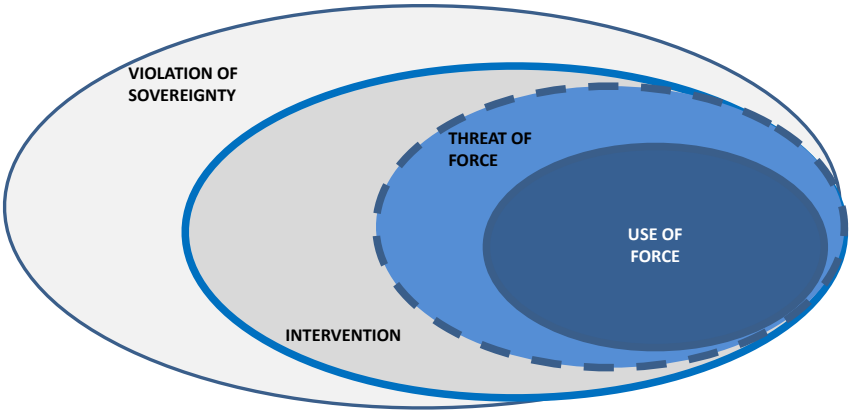

Figure 3 - 1 Degrees of infringement

Cognizant of the intertwined nature of the relations, the intent of a conceptual categorization of the range of infringements is to be able to single out the specific characteristics of violations of sovereignty and non-interventions respectively, away from the severest forms of infringements that include the threat or use of force.[45]

The main thresholds for demarcation are the use of force[46] and the use of coercive means (short of the use of force),[47] based on which several categories can be made.[48] The most severe infringements use, or threaten with, armed force. These infringements may even amount to an armed attack. Economic or political means are excluded from the notion of use of force.[49] An intervention, shown in figure 3.1., is an infringement by (non-military) coercive means

44 Paul A.L. Ducheine and Peter B.M.J. Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in *Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans P.B. Osinga and Tim Sweijs (Springer, 2021), 475–500. pp. 488-495.

45 See also: Helal, "On Coercion in International Law." pp. 54-56.

46 Damrosch alludes to the difference between the use of force versus an intervention which is a 'nonforcible efforts to influence another state's internal politics'. Lori F. Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs," *The American Journal of International Law* 83, no. 1 (1989): 1–50. p. 1.

47 Steven Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion,'" *Duke Journal of Comparative and International Law* 30, no. 3 (2020). p. 20.

48 See also: Nicholas Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace," *European Society of International Law Reflections Series* 9, no. 4 (2020). p. 4; Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, 2013. pp. 199-200.

49 United Nations Information Organization (UNIO), "United Nations Conference on International Organization (UNCIO)-Volume VI," 1945. The Brazilian proposal to include 'mesure d'ordre économique' on p. 609 and the rejection of it on p. 334.

which is invasive in the reserved domain of a State. The final category is the violation of sovereignty, i.e. an infringement without the use of coercive means.

Section 3.3.: Violation of Sovereignty

"Sovereignty is a funny thing. It is allegedly the foundation of the Westphalian order, but its exact contours are frustratingly indeterminate."[50]

3.3.1. The legal basis of the rule on sovereignty

The legal basis for the principle of sovereignty as a primary rule of customary international law is found in State practice and *opinio iuris*, reflected in decisions of international courts and tribunals,[51] multilateral conventions and other international instruments such as the Helsinki Final Act and certain resolutions of the UN General Assembly.[52]

The UN Charter safeguards several aspects of sovereignty: the sovereign equality of States is referred to in Articles 2(1) and 78; and the territorial integrity and political independence in Article 2(4).[53] Also the regional Organisation of American States refers to sovereignty, territorial integrity and independence in the first article of its Charter.[54] Likewise, the Helsinki Final Act speaks about juridical equality, territorial integrity, freedom and political independence as attributes inherent to sovereignty.[55]

Case law on sovereignty is substantial. The 1927 *Lotus* Case argues that, if there are no permissive rules, a State 'may not exercise its power in any form in the territory of another State' alluding to the territorial integrity, the political independence and sovereign equality of States[56] which are elements most prominently articulated in the 1928 *Island of Palmas* Arbitral

50 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?," *Texas Law Review* 95 (2017): 1579–98. p. 1579.

51 Michael N. Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95 (2017): 1639–70. pp. 1650 ff.

52 CSCE, "Helsinki Final Act" (1975).; United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)," 1970.

53 United Nations, "Charter of the United Nations" (1945).

54 OAS, "Charter of the Organization of American States" (1948). Article 1. See also Article 1 of the ICAO, "Convention on International Civil Aviation" (1944).; Article 2 of the "United Nations Convention on the Law of the Sea" (1982).

55 CSCE, Helsinki Final Act. Article 1. Note that the Helsinki Final Act is a political rather than a legal convention, see Terry D. Gill, "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace*, 2013, 217–38. p. 220.

56 PCIJ, The Case of the S.S. Lotus (France v. Turkey) - Judgment, Series A Collection of Judgments 1–79 (1927). p. 18.

Award: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[57]

The 1949 *Corfu Channel* Case is important for two reasons. First of all, the ICJ states that '(b) etween independent States, respect for territorial sovereignty is an essential foundation of international relations'.[58] Second, the ICJ queries whether the sovereignty of *in casu* Albania was violated by the United Kingdom (UK). Irrespective of the assessment of the ICJ, deliberations on the violation of sovereignty during litigation gives prominence to the notion that respect for sovereignty is a binding rule of law. This is underlined by the UK invoking exemptions to the obligation to respect the sovereignty of other States. Invoking the exemptions again does not weaken but underlines the principle of sovereignty. Later, in the 1986 *Nicaragua* Case, a similar rationale is used by the United States (US) invoking the right of (collective) self-defence to use force against Nicaragua. Invoking this right underlines the binding nature of the prohibition of the use of force.[59]

In the 1974 *Nuclear Test* Case (Australia vs France), Australia claimed that the radioactive fall-out from French atmospheric nuclear testing landed on Australian soil, violating its territorial integrity and, hence breaching international law. France acknowledged the fall-out and did not dispute its French origin, but claimed that deposits were negligible and constituted no danger to the health of the population.[60] Though the ICJ refrained from commenting on the merits of the case, and decided not to pursue litigation once France pledged not to continue with atmospheric testing, thereby removing the legal interest of Australia, the case indicates the existence of the notion of territorial integrity of a State as a legal obligation that can be violated.[61]

The 1986 *Nicaragua* Case referred to territorial integrity and sovereignty numerous times,[62] including the obligation under customary international law not to violate these norms. Though the violation of sovereignty is often a consequence of a breach of the prohibition of intervention or a use of force, sovereignty is also breached as a stand-alone legal obligation

57 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards 829–71 (1928). p. 838.

58 Corfu Channel Case (merits) - Judgment of 9 April 1949, ICJ Reports. p. 35.

59 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 193 & 211, pp. 102 & 110-111.

60 Nuclear Tests (Austl. v. Fr.) - Judgment, ICJ Reports 253 (1974). Para 18, p. 258.

61 Nuclear Tests (Austl. v. Fr.) - Judgment, ICJ Reports. pp. 271-272.

62 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 212, when referring to the laying of mines, p. 111.

in the case of laying mines in Nicaraguan territorial waters,[63] and in relation to unauthorised overflights by US military aircraft in Nicaraguan airspace.[64]

In the 1988 *Nicaragua- Honduras Border* Case, Nicaragua referred to obligations of customary international law 'not to intervene in the affairs of another State, not to use force against another State, and not to violate the sovereignty of another State'.[65] Honduras objected to the Nicaraguan claims and, though they were rejected by the ICJ, the fact that two States and the ICJ contemplated the violation of sovereignty, highlights its existence as a distinct rule.[66]

Violations of sovereignty are often intrinsically related to breaches in the prohibition of intervention or the use of force. A case where the violation of sovereignty is a not consequence of a coercive or forceful infringement is the 1990 *Rainbow Warrior* Arbitration Case.[67] In this case France violated New Zealand sovereignty by sinking the Greenpeace ship Rainbow Warrior in Auckland harbour. Two French secret service officers were tried and incarcerated at Hao Island in French Polynesia after a bilateral agreement was agreed upon. However, France 'repatriated' the two officers to mainland France before the end of the sentence, violating an international obligation stemming from the bilateral agreement. Though force was used to sink the Rainbow Warrior, the prohibition of threat or use of force was not invoked in this case. This 'low level use of force'[68] was first and foremost a violation of the dignity of a sovereign State after which France was summoned to pay reparations. The amount did not only cover material damage but also non-material i.e. moral and legal damage,[69] alluding to the specific position of the principle of sovereignty. In a second iteration, related to the violation of the bilateral agreement, the declaration of the arbitrator constituted in itself appropriate satisfaction, in analogy to the 1949 *Corfu Channel* Case.

Respect for sovereignty and territorial integrity are also core elements in the 2005 *Armed Activities* Case (DRC v. Uganda).[70] As in previous cases, by mentioning the principles, the

63 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 111, para 213. The prohibited use of force regarding the laying of mines is discussed in para 227 on p. 118.

64 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 128, para 251. Phil Spector, "In Defense of Sovereignty, in the Wake of Tallinn 2.0," *AJIL Unbound* 111 (2017): 219–23. p. 222.

65 Case Concerning Border and Transborder Armed Actions (Nicaragua v. Honduras) - Judgment of 20 December 1988, ICJ Reports (1988). Paras 50-57, pp. 90-92.

66 The substance in this case relates to the existence of armed bands (contra forces) that operating from Honduras, carrying out armed attacks on Nicaraguan territory, hence falling within the realm of threat or use of force rather than sovereignty proper. Case Concerning Border and Transborder Armed Actions (Nicaragua v. Honduras) - Judgment of 20 December 1988, ICJ Reports. Para 50, p. 90. The substance in this case relates to the existence of armed bands (contra forces) that operating from Honduras, carrying out armed attacks on Nicaraguan territory, hence given the categorisation in § 3.2 would be a threat or use of force rather than sovereignty proper.

67 RIIA, Rainbow Warrior (New Zealand v France) (1990).

68 Michael Pugh, "Legal Aspects of the Rainbow Warrior Affair," *British Institute of International and Comparative Law* 36, no. 3 (1987): 655–69. p. 658.

69 RIIA, Rainbow Warrior (New Zealand v France), 20. p. 272.

70 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports. Para 165, p. 227.

ICJ recognises their obligatory nature. However, the activity employed by Uganda was a military intervention, breaching Article 2(4) of the UN Charter and consequently violating the sovereignty of the DRC. When elaborating this argument, the grave violation of the prohibition of the use of force appears to be the material breach, without further referral to violation of sovereignty as the basis of a breach of the legal obligation.[71] In this case sovereignty is violated via a breach of the prohibition of the use of force.

In the 2015 Case on *Certain Activities Carried out by Nicaragua* (Costa Rica – Nicaragua) the ICJ held that Nicaragua had violated the territorial sovereignty of Costa Rica,[72] which is an independent legal obligation and the violation thereof constitutes a breach of international law. There are several references to territorial sovereignty as an independent rule in this case.[73] Similar to earlier cases, the 'declaration by the Court that Nicaragua breached the territorial sovereignty of Costa Rica (...) provides adequate satisfaction for the non-material injury suffered on this account'.[74]

The legal obligation of respect for the sovereignty of States in customary international law is echoed in numerous declarations of the UN. The 1970 UN General Assembly (UNGA) Declaration on Friendly Relations emphasises the importance of sovereign equality of States.[75] The sovereign equality entails not only the judicial equality of States, but also highlights the inviolability of territorial integrity and political independence of States and their right to freely choose and develop political, social, economic and cultural systems. The latter had already been stated in the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs,[76] and was confirmed by the 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, though without making a clear distinction between interference and intervention.[77]

71 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports. Paras 160-165, pp. 226-227.

72 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015, ICJ Reports (2015). Para 93, p. 703.

73 The case dealt with a misunderstanding to whom certain pieces of terrain belonged. By declaring that the disputed area belongs to Costa Rica, Nicaragua consequently breaches sovereignty Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015, ICJ Reports. pp. 740 ff., para 229. See also: Crawford, *Brownlie's Principles of Public International Law.* p. 200, related to the title, in the sense in the concept of ownership, of the territory.

74 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015, ICJ Reports. Para 139, p. 717.

75 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)." Under 'the principle of sovereign equality of States'.

76 United Nations General Assembly, "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty - Resolution 2131 (XX)," 1965. Bullet 5: "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State."

77 United Nations General Assembly, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States - A/Res/36/103," 1981. In bullets 1 and 2 under a, b and c.

In sum, sovereignty as a primary rule of law has a firm foundation in international law. Respect for sovereignty is a primary rule of law, a breach of which constitutes a violation of international law. If there is no further justification, and the violation can be attributed to a State, the violation is an internationally wrongful act and open to redress.

3.3.2. The characteristics of violations of sovereignty

Oppenheim states that 'interference pure and simple is not intervention'.[78] To define interference in the sovereignty of a State, away from coercive intervention (discussed in the next section) or an infringement based on the use of force, sovereignty as such needs to be addressed.

Sovereignty cannot easily be summarised;[79] it is a 'catch-all' term, with a lengthy and troubled history.[80] Sovereignty can be categorised in several ways referring to the dichotomy between independence and equality or between domestic and international. Sovereignty can both be internal and external,[81] or as Crawford argues, there is sovereignty between States and within States.[82]

The sovereignty of a State can be violated if one of the core elements of sovereignty - territorial integrity and political independence - is infringed.[83] The interrelatedness between these concepts is illustrated in the earlier mentioned 1928 *Island of Palmas* Case, in which Judge Huber stated that,[84] 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[85] Sovereignty among States refers to the legal equality of States – sovereignty in the relation between States signifies independence

78 Jennings and Watts, *Oppenheim's International Law*. p. 432.

79 See i.a. James Crawford, "Sovereignty as a Legal Value," in *The Cambridge Companion to International Law*, 2012, 117–33. pp. 117-119.

80 Crawford, *Brownlie's Principles of Public International Law*. p. 432; for a concise overview of the origins of modern international law, see Gleider Hernandez, *International Law* (Oxford, United Kingdom: Oxford University Press, 2019). Chapter 1, pp. 3-29.

81 See e.g. Samantha Besson, "Sovereignty," *Max Planck Encyclopedia of International Law*, no. April (2011).; Jennings and Watts, *Oppenheim's International Law*. pp. 382 ff.

82 Crawford, "Sovereignty as a Legal Value." pp. 120-123.

83 Quincy Wright, "Subversive Intervention," *The American Journal of International Law* 54, no. 3 (1960): 521–35. p. 522; Samuel K N Blay, "Territorial Integrity and Political Independence," *Max Planck Encyclopedia of International Law*, no. March (2010). Para1; See also: Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 38; Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1648; Marko Milanovic and Michael N. Schmitt, "Cyber Attacks and Cyber (Mis) Information Operations During a Pandemic," *Journal of National Security Law & Policy* 11 (2020): 247–84. p. 6.

84 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards. p. 838.

85 PCA, II Reports of International Arbitral Awards. p. 838.

- while sovereignty within States refers to the right to exercise the functions of the State, within a portion of the globe.[86]

In the context of international law States are sovereign within the State and equal among other States.[87] States are juridically equal in international law, regardless of size or composition, based on the principle of *par in parem non habet imperium*.[88] The sovereignty equality is one of the cornerstones of the system of international law and is recognised in Article 2(1) of the UN Charter.[89]

Apart from referring to juridical equality, sovereignty within the State can be categorised according to a territorial (the portion of the globe) and a political element (the functions of the State),[90] referred to as territorial integrity and political independence.[91]

Territorial integrity signifies exclusive authority and power the State has over its territory and its appurtenances,[92] which includes the inviolability of, and respect for the territorial boundaries and connected territorial sea and airspace. Crawford argues that sovereignty is the independence of territory and authority over that territory and those residing upon it, public and private.[93]

Political independence relates to the autonomy of States and enables them to execute the functions of the State.[94] States can 'freely pursue a path to economic, social and cultural

86 Crawford, "Sovereignty as a Legal Value." pp 120-121; See also Harriet Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention," 2019. Para 30, p. 11.

87 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."

88 Eric Jensen, "Cyber Sovereignty: The Way Ahead," *Texas International Law Journal* 50, no. 2 (2015): 275–304. p. 285 – an equal has no power over an equal.

89 Bardo Fassbender, "Purposes and Principles, Article 2 (1)," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma et al., 3rd ed., vol. I, 2014. Para 73, p. 164.

90 Though the elements of sovereignty can be categorised, they are inter-linked. See also: Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 21.

91 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."; United Nations General Assembly, "Definition of Aggression - Resolution 3314 (XXIX)," 1974.; Oliver Dörr and Albrecht Randelzhofer, "Purposes and Principles, Article 2 (4)," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma et al., 3rd ed., vol. I (Oxford University Press, 2014). pp. 215-217. See also Article 2(4) of the United Nations, Charter of the United Nations.; United Nations Information Organization (UNIO), "United Nations Conference on International Organization (UNCIO)- Volume VI." pp. 334-335; Crawford, *Brownlie's Principles of Public International Law*. p. 200.

92 Crawford, *Brownlie's Principles of Public International Law*. p. 192.

93 Crawford, "Sovereignty as a Legal Value." pp. 131-132, which is in line with the wording used in the iterations of the Tallinn Manual, when related to cyberspace See e.g. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *Cambridge University Press*, 2013. Rule 1, pp. 15-18; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 1, pp. 11-13.

94 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards. p. 838; Higgins, "Interv. Int. Law." p. 274.

development of its choice',[95] which remit coalesces with the inherently governmental functions.[96] Political independence also means that States have the authority and capability to engage with, and enter into relations with, other sovereign States.[97]

Sovereignty entails a constellation of rights and obligations of the State.[98] States are entitled to exercise jurisdiction over objects and persons within their territory. Obligations of the State include the principle of due diligence but first and foremost the duty to avoid interfering with the sovereignty of other States. Conversely derived from the principle of their sovereign equality, States are protected from undue infringements by other States.

A violation of sovereignty, away from an intervention, is a non-coercive infringement that may be unlawful. However, not all these infringements are unlawful; dialogues and interaction between States or moderate persuasions could be unwelcome but are not unlawful. Consensual agreements in treaties can provide justifications for intrusions. On the other hand, if the interference is conducted in a way that violates a legal obligation in the relation vis-a-vis States or to the international community at large, it is unlawful.

To assess the characteristics of a non-coercive violation of sovereignty, an analogy is made to the 'domain' and 'nature' of an intervention in other words the *domaine réservé* and coercion.[99] Below, the domain of a violation of sovereignty of the State as well as its nature will be described. Since the domain and nature for a breach of territorial integrity differ from a violation of political independence, these will be dealt with separately.

95 Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." p. 191.

96 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.; Schmitt, "Grey Zones in the International Law of Cyberspace." pp. 5-6.

97 An if they enter into relations with other States, this is on equal footing, reflecting the principle of the sovereign equality of States In this sense political independence and equality are different attributes of a State. See also: United Nations, Charter of the United Nations. Preamble and Article 2 (1).

98 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards. p. 839. See also: Corfu Channel (U.K v. Alb.), 1949 I.C.J. (Opinion of Judge Alvarez), ICJ Reports 43 (1949). p. 43., who states that 'sovereignty confers rights upon a State and imposes obligations on them'; Crawford, *Brownlie's Principles of Public International Law*. p. 432.

99 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020. p. 48. Other dichotomies are end (domain) versus means (nature/ tools), see e.g. Helal, "On Coercion in International Law." p. 4.

3.3.2.1. Territorial integrity

The domain of territorial integrity is the territory of the State, including the adjacent territorial sea[100] and airspace above and the population and materiel located there; a spatial recognition, but also limitation, of the supreme territorial authority of the State.[101]

The nature of the incursion is related to the State's control of access to and egress from the territory, but also with the authority and protection of persons, materiel and infrastructure in the territory of the State.[102] The obligation to respect the territory of another State is related to the obligation to abstain from aggression and subversive intervention.[103] Other injurious activities refer to the principle of *sic utere tuo ut non alienum laedas*,[104] urging States not to harm other States territory e.g. by refraining from polluting rivers that flow from one territory into another, preventing the laying of mines in maritime straits or launching missiles whose debris might land on, and could impact, other States.

Although the use of territory is regulated in many conventions including EU- treaties,[105] violations of sovereignty in case law are still most frequently related to the territorial integrity of sovereignty (compared to breaches of political independence), as illustrated with the unauthorised overflight and mining in the territorial waters in the 1986 *Nicaragua* Case, or the excavation of *caños* (channels) in contested terrain in the 2015 *Certain Activities Carried out by Nicaragua* Case.[106]

3.3.2.2. Political independence

The second aspect is political independence of the State, meaning that the State is an independent political entity that has full authority over the functions of the State.[107] The

100 North Sea Continental Shelf Cases, ICJ Reports (1969). Para 59, p 37. The 1969 North Sea Shelf case confirms not only the land territory but also seabed and the territorial sea adjacent to it falls under the full sovereignty and hence sovereign jurisdiction of that State.

101 Arthur Watts, "Sovereignty," *Encyclopedia Princetoniensis*, 2019. p. 5.

102 Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *U.S. Naval War College International Law Studies* 89 (2013): 123–56. pp. 124- 134.

103 Wright, "Subversive Intervention." p. 528.

104 *Sic utere sic tuo ut non alienum laedas* is a Latin maxim meaning use your own property in such a way that you do not injure other people's, see: Wright. p. 528.

105 The free movement of persons is regulated via Article 3(2) of the Treaty on European Union (TEU); Article 21 of the Treaty on the Functioning of the European Union (TFEU); Titles IV and V TFEU; Article 45 of the Charter of Fundamental Rights of the European Union. See also: Besson, "Sovereignty." Para 42-44.

106 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 111, para 213 & p. 128, para 251; Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015, ICJ Reports. para 139, p. 717.

107 Crawford, *Brownlie's Principles of Public International Law*. pp. 470- 474; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. note 26, p. 22.

authority of the State is related to competences inherent to the State and includes authority to collect taxes, defend the State, hold elections, conduct diplomacy and enforce the law. These are functions of the State that only the State can do, and which can be referred to as inherently governmental functions.[108] These functions must not be confused with the jurisdiction the State has. The functions of the State, together with the territorial integrity form the basis of sovereignty while jurisdiction is a corollary from sovereignty. Jurisdiction is related to how the State executes and implements the functions of the State and the control of its territory.

Inherently governmental functions are the domain of political independence. The nature of the incursion is an interference with these functions by another State or – more severely - taking over (usurping) these functions.

This difference in domains between territorial integrity and political independence comes to the fore regarding infringements of private property in a State.[109] When an agent of a foreign State infringes and damages non-vital commercial infrastructure, the political independence, or inherently governmental function is not violated, but the territorial integrity probably is. Related to case law, it may be argued that in the 1974 *Nuclear Test* Case, Australian sovereignty was violated due to a breach of territorial integrity rather than its political independence.

3.3.3. Scope and intent of violations of sovereignty in cyberspace

Respect for sovereignty is a well-recognised principle of international law with the corollary legal obligation not to violate the sovereignty of another State.[110] A breach of both territorial integrity and political independence may constitute a violation of sovereignty of the State.

This would also account for sovereignty in cyberspace. During the two iterations of the Tallinn Manual this was confirmed - or rather not disputed - by academics, with Schmitt as their most active proponent.[111] Schmitt's position along with that of a significant number of jurists and a number of States is that 'sovereignty constitutes both an international law principle from

108 Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018). p. 45; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. p. 20 rule 4(10, 16, 17).

109 A purely commercial activity is beyond the domain of inherently governmental functions, see: Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 47.

110 See e.g. United Nations, Charter of the United Nations.; CSCE, Helsinki Final Act.

111 See i.a. Schmitt and Vihul, "Respect for Sovereignty in Cyberspace."; Jeffrey Biller and Michael N. Schmitt, "Un-Caging the Bear ? A Case Study in Cyber Opinio Juris and Unintended Consequences," *EJIL*, 2018.; Schmitt, "Grey Zones in the International Law of Cyberspace."; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law."

which various rules derive (such as the prohibitions on coercive intervention and the use of force) and a primary rule in its own right capable of being violated."[112]

However, since mid-2016 a discussion between legal scholars has been ongoing in which some challenge the concept of sovereignty as a rule in cyberspace.[113] The challengers recognise that sovereignty is a non-binding principle, but no legal rights and obligations can be derived from it when operating in cyberspace, partially due to the lack of State practice.

Is sovereignty a principle or a rule in cyberspace, or both? The issue is relevant for two reasons. First, if sovereignty is not a rule of international law, interferences of a non-coercive nature would not be unlawful. Second, a violation of international law, in the sense of an internationally wrongful act, implies the breach of a primary rule of law and not of non-obligatory principles. Perceiving sovereignty as a non-binding principle purports that it cannot constitute an independent international obligation and, even if the act can be attributed, the injured state cannot invoke an internationally wrongful act and consequently demand reparation including a reset of the system of international law.[114]

Though discourses on sovereignty are not new,[115] the emergence of cyberspace appears to have reopened the discussion urging Fischerkeller to state that no concept of cyberspace sovereignty currently exists.[116] Others have joined the academic discourse,[117] but the most authoritative articulation came from the UK.[118]

The idea that sovereignty is a principle but not a rule in cyberspace, is the position currently held in the UK.[119] In 2016 UK Attorney General Wright stated that the emergence of cyberspace has posed questions regarding the applicability of international law.[120] Wright argues that it

112 Michael N. Schmitt, "France's Major Statement on International Law and Cyber: An Assessment," *Just Security*, no. 2 (2019). p. 2.

113 See e.g. Michael N. Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace," *Just Security*, 2020.; Przemysław Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach," in *Governing Cyberspace*, ed. Dennis Broeders and Bibi van den Berg, 2020, 65–84. pp. 67-69.

114 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 41.

115 Jensen, "Cyber Sovereignty: The Way Ahead." p. 282; Louis Henkin, "That 'S' Word: Sovereignty, and Globalization, and Human Rights, et Cetera," *Fordham Law Review* 68, no. 1 (1999): 1–13. p. 1, calling it *'the 'S' word, an illegitimate child that did not age well'*.; Winston P. Nagan and Craig Hammer, "The Changing Character of Sovereignty in International Law and International Relations," *Columbia Journal of Transnational Law* 43, no. 1 (2004): 141–87. pp. 143-144.

116 Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93. p. 386.

117 See e.g. Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *AJIL Unbound* 111 (2017): 207–12.

118 Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace." p. 4.

119 The 2016 legal statement by Wright show some disparity with the 2020 political communique of the UK government condemning Russia of undermining the sovereignty of Georgia via cyberspace. See: UK Government, "UK Condemns Russia's GRU over Georgia Cyber-Attacks," 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

120 Jeremy Wright, "Cyber and International Law in the 21st Century," 2018.

is the responsibility of the international community of States to clarify what is meant in this regard. The UK argues that the prohibition of intervention, and of the threat or use of force against the territorial independence or political integrity of any State are valid in cyberspace.[121] Violations constitute an internationally wrongful act, also in cyberspace, after which redress is possible. The challenges are related to cyber activities in peacetime, especially below a coercive intervention. Though sovereignty is fundamental to the international rules-based system, Wright is 'not persuaded' to 'extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention."[122] The UK Government have made an explicit statement that they do not accept that sovereignty is a binding rule of current international law in cyberspace.[123]

In a similar vein to the UK public statement, US scholars Corn and Tayler state that cyberspace offers 'a broad array of targets, free from the physical constraints of geography and territorial boundaries."[124] Though there are sufficient proscriptions against unlawful uses of force and interventions in treaty law and customary international law, 'below these thresholds, there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace."[125] Furthermore, Corn et al. mentions that, based on the law and State practice, 'sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law"[126]. Sovereignty, according to the authors, is therefore not an 'absolute bar' for operations in cyberspace against another state as long as the operation does not use force or constitutes a coercive intervention.[127]

Of relevance is that Corn and Taylor do not express the official US position on this topic; moreover, other legal US commentators hold more restrained, or nuanced, views.[128] In 2012, Koh argued that 'states conducting activities in cyberspace must take into account

121 The transcript of the speech of Attorney- General Wright mentions 'territorial independence and political integrity' while refering to Article 2(4) of the UN Charter. The latter however states: territorial integrity and political independence.

122 Both citations from: Wright, "Cyber and International Law in the 21st Century." "Cyber and International Law in the 21st Century".

123 Furthermore, the UK does not agree that it has to give prior notification to countermeasures after a cyber related breach of international law. Nor does it feel obligated to provide information underlying a decision to publicly attribute a violation. See: Wright.

124 Corn and Taylor, "Sovereignty in the Age of Cyber." p. 207.

125 Corn and Taylor. p. 208.

126 Corn and Taylor. p. 208.

127 Corn and Taylor. p. 208.

128 Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace."; Robert Chesney, "The Pentagon's General Counsel on the Law of Military Operations in Cyberspace," *Lawfare*, 2020, 1–5.; Duncan B. Hollis, "Improving Transparency International Law and State Cyber Operations (OAS - Fourth Report)," vol. 19, 2020. p. 20 arguing that the current US position is 'murkier'; Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace."

the sovereignty of other States, including outside the context of armed conflict."[129] While confirming Koh's statement in November 2016, Egan does not deny the existence of sovereignty as a legal obligation. He states that '(p)recisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that will ultimately be resolved through the practice and *opinio juris* of States."[130] In his opinion there is no absolute threshold in international law for the violation of sovereignty by remote cyber operations, especially if the activity has 'no effects or de minimis effects' in the other State's territory.[131] In 2020, DoD General Counsel Ney stated that the prohibition of the use of force and of intervention applies to cyberspace,[132] but that '(f)or cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory.'[133] Though this view is more aligned with the UK opinion,[134] it must be argued that the US, similar to Israel,[135] is still 'on the fence'.[136]

Though many States still remain silent on the topic,[137] and State practice regarding whether sovereignty is a rule or a principle in cyberspace is meagre,[138] a growing number of States including Australia,[139] Estonia,[140] France,[141] the Netherlands,[142] New Zealand,[143] and Germany

129 Koh, "International Law in Cyberspace." p. 6.

130 Brian Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35, no. 1 (2016). p. 174.

131 Egan. "International Law and Stability in Cyberspace," p. 174.

132 See also Chesney, "The Pentagon's General Counsel on the Law of Military Operations in Cyberspace." Under 4 c -d.

133 Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," 2020. Under B. International law.

134 Chesney, "The Pentagon's General Counsel on the Law of Military Operations in Cyberspace." Under 4. f.

135 Roy Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *EJIL*, 2020, 1–9.

136 Michael N. Schmitt, "Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)," *Just Security*, 2020.

137 Which can very well be a calculated decision, see: Ronald Alcala, "Opinio Juris and the Essential Role of States," *Articles of War*, 2021.

138 In the sense that there are not overt activities nor is there official documentation on the cyber activities of the state. See also: Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention."p. 9; Hollis, "Improving Transparency International Law and State Cyber Operations (OAS - Fourth Report)." pp. 2-3.

139 Australian Government Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, *Department of Foreign Affairs and Trade*, 2017.

140 Kristi Sits, "President of Estonia : International Law Applies Also in Cyber Space," in *CyCon 2019*, 2019, 1–2.

141 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace."; See also Michael N. Schmitt, "France Speaks Out on IHL and Cyber Operations : Part I," *EJIL*, 2019, 1–4.; Przemysław Roguski, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I," *OpinioJuris*, 2019, 1–5.

142 Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace.; See also: Michael N. Schmitt, "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis," *Just Security*, 2019.

143 New Zealand Ministry of Foreign Affairs & Trade, "The Application of International Law to State Activity in Cyberspace," 2020. pp. 2-3, New Zealand leans towards accepting sovereignty as a rule, stating that in the physical realm the principle of sovereignty has effect via the standalone rule of territorial sovereignty, but in the cyber realm New Zealand 'considers that

have given their legal opinion on the applicability of international law in cyberspace including reference to sovereignty.[144]

For France sovereignty is a rule, also in cyberspace,[145] stating that it will protect its sovereignty over the information systems located on its territory and implements the means necessary to protect this sovereignty[146] and reserves the right to respond to any cyberattack of which it has been the victim.[147] France argues that a violation of sovereignty is not only related to rules regarding the prohibition of intervention or use of force, but also to political independence and territorial integrity over its territory and the people and objects within that territory.[148] Cyber operations executed by another State on French digital infrastructure will violate sovereignty and international law.[149]

The Netherlands hold a more explicit legal opinion than France. Similar to France, the Netherlands argues that the rules stemming from the principle of sovereignty are not merely the right of self-defence, the principle of non-intervention and the prohibition of force,[150] but also the territorial integrity and the inherently governmental functions of a State, thereby following the rationale of the Tallinn Manual.[151] The Netherlands states that the principle of sovereignty is an independently binding rule of international law and its violation constitutes an internationally wrongful act.[152]

---

the standalone rule of territorial sovereignty also applies in the cyber context but acknowledges that further state practice is required for the precise boundaries of its application to crystallise.'

144 The discussion is not confined to Europe and the US. Iran has provided a statement for the OEWG, see: Iran Minstry of Foreign Affairs, "Intervention by Delegation of the Islamic Republic of Iran on International Law." And also in the Organisation of American States silence is broken. Bolivia, Guatemala and Guyana argue that sovereignty is a stand-alone rule that can be breached in cyberspace. Other are less outspoken and some suggest it only a principle. See: Duncan B Hollis, Ben Vila, and Daniela Rakhlina-Powsner, "Elaborating International Law for Cyberspace," *Directions Cyber Digital Europe*, 2020.; Hollis, "Improving Transparency International Law and State Cyber Operations (OAS - Fourth Report)." Para 52, p. 19.

145 Schmitt, "France's Major Statement on International Law and Cyber: An Assessment."

146 SGDSN, "Revue Stratégique de Cyberdéfense," 2018. p. 82.

147 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace." p. 6 'La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire et met en œuvre les moyens nécessaires à la protection de cette souveraineté.'

148 Ministère des Armées. p. 7: "Les violations les plus graves de souveraineté, notamment celles qui portent atteinte à l'intégrité territoriale ou à l'indépendance politique de la France, peuvent constituer une violation du principe d'interdiction de recours à la menace ou à l'emploi de la force, lequel s'applique à tout emploi de la force indépendamment de l'arme employée"; SGDSN, "Revue Stratégique de Cyberdéfense.", p. 82 reads that: 'le principe de souveraineté s'applique au cyberespace. A ce titre, la France réaffirme, qu'elle exercise sa souveraineté sur le systeme d'information, les personnes, les activités cyber sur son territoire (...)'.

149 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace." p. 7.

150 Ministry of Foreign Affairs, "Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace" (2019). p. 1.

151 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4, p. 20.

152 Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace. p. 2.

The German position paper on the application of international law to cyberspace argues that sovereignty is both a principle and a rule of international law,[153] thereby providing a more elaborate distinctive interpretation of political interdependence and territorial integrity related to different layers of cyberspace.

Switzerland, Austria, the Czech Republic and Finland similarly support the view that sovereignty is a rule of international law.[154] Other countries are less outspoken. Australia concurs that for cyber activities below the threshold of the use of force, general principles of international law, the principle of due diligence and the customary international law on State responsibility as laid down in the Responsibility of States for Internationally Wrongful Acts, apply.[155] Estonia, similar to Australia, circumvents wording on the appreciation of sovereignty as a principle or primary rule in cyberspace.[156] In this regard, Estonia does not elaborate any further than affirming that international law applies to cyberspace, and that States must refrain from the threat of or use of force against the territorial integrity and political independence of other States.[157] Also China states that 'the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace."[158] This is a view echoing the Joint Statement by China and the Russian Federation on cooperation in Information Space Development, in which they strongly support the principle of national sovereignty within the UN framework.[159] This statement confirms an earlier declaration of six members of the Shanghai Cooperation Organisation sent to the UN Secretary General in January 2015.[160] The language used is neutral and restates the text of the UN Charter when referring to sovereignty, hence not confirming but also not denying the existence of the rule of sovereignty in cyberspace.

153 German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace." pp. 2-4; Michael N. Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law," *Just Security*, 2021.

154 Swiss Ministry of Foreign Affairs, "Position Paper on Switzerland's Participation in the UN OEWG and UNGGE," (2020).; Austrian Ministry of Foreign Affairs, "Pre-Draft Report of the OEWG - ICT," (2020).; Czech Republic Ministery of Foreign Affairs, "Comments Submitted by the Czech Republic in Reaction to the Initial 'Pre-Draft' Report of the OEWG," (2020).; Finland Ministry of Foreign Affairs, "Finland Published Its Positions on Public International Law in Cyberspace," 2020, https://um.fi/current-affairs.

155 Australian Government Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*. Annex A, p. 91.

156 Also the 2019 supplement to the Australian Cyber Strategy stay silent on the topic. Australian Government Department of Foreign Affairs and Trade, "2019 International Law Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace," 2019.

157 Sits, "President of Estonia : International Law Applies Also in Cyber Space." First and fifth point.

158 Ministery of foreign affairs of the people's republic of China, "International Strategy of Cooperation on Cyberspace," 2017. Chapter II para 2.

159 "Joint Statement Between the People's Republic of China and the Russian Federation on Cooperation in Information Space Development," 2016.

160 United Nations General Assembly, "A/69/723 Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General," *UN Doc. A/69/723* 00392, no. January (2015). p. 4.

Though the UK's legal opinion regarding sovereignty in cyberspace should be taken into account, the status of sovereignty as a binding rule of customary international law should not, on balance, be rejected. The determination flows from the longstanding recognition of sovereignty as a rule of customary international law and the considerable body of opinion expressed by States, as well as in much of the academic world, which accepts both its status as a rule and its applicability to cyberspace.[161] Moreover, the mere emergence of a new domain to engage in is scarcely enough to change a legal regime. After all, sovereignty is and has been a legal obligation, and it is legally consequential,[162] in all other domains of engagement[163] and no State has so far openly and consistently rejected its application in cyberspace or in any other domain. Finally, the argument that sovereignty is not or cannot yet be a legal obligation in cyberspace due to the lack of State practice is not persuasive. It might be true that there is a lack of State practice, but this rationale would also apply to cases related to intervention and the use of force in cyberspace[164] which clearly constitute rules of international law.[165]

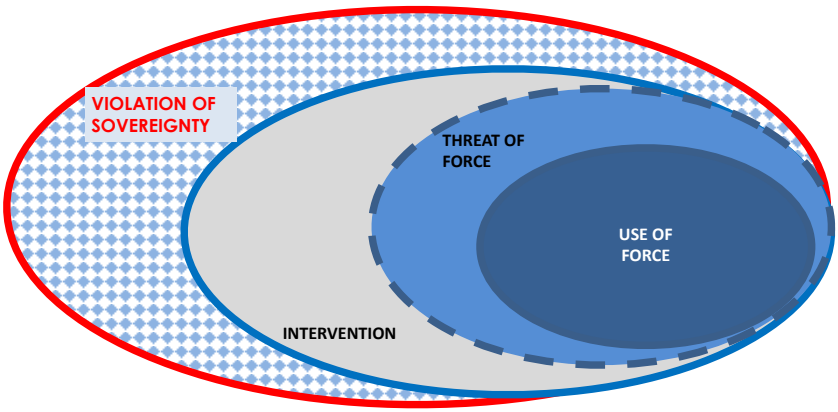

Figure 3 - 2 Violation of sovereignty

161 Also NATO states that cyber operations may constitute a violation of international law including a breach of sovereignty or other international wrongful acts. Of note, the UK has made a reservation related to this topic, see NATO, "Allied Joint Doctrine for Cyberspace Operations - AJP-3.20," *Nato Standardization Office*, 2020. pp. v & 20 (footnote 26).

162 Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace." p. 5.

163 See e.g. Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1649; Corfu Channel Case (merits) - Judgment of 9 April 1949, ICJ Reports. p. 35; Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 106, para. 202 & p. 111 para 213. In the latter the Court quotes the Corfu Channel Judgment in stating that '"Between independent States, respect for territorial sovereignty is an essential foundation of international relations", and international law requires political integrity also to be respected.'

164 Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare* 19, no. 4 (2020): 1–16. p. 6.

165 Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion.'" p. 11.

Sovereignty is a legal rule in all domains of engagement, including cyberspace,[166] not least since there is neither a consistent refutation nor State practice to conclude differently.[167] This, however, does not preclude the underlying arguments regarding the discourse on how sovereignty should be applied as a rule in cyberspace. To elaborate on the discourse, an assessment is made on the basic elements of sovereignty - territorial integrity and political independence - in cyberspace, and the violation thereof. The paragraphs below refer to the violation of sovereignty away from coercive intervention, the threat or use of force, or armed attack – hence solely the chequered area of the outer rim in figure 3-2.

3.3.3.1. Territorial integrity

The authority over territory includes the adjacent territorial sea[168] and airspace above it. Cyberspace, consisting of a physical network layer, logical software layer and virtual personal layer, is partially linked to that territory. The physical network layer, the ICT infrastructure, which supports the Internet and activities in cyberspace, is generally located on the sovereign soil of a State and falls within the domain of its territory.[169]

An infringement damaging the computers and networks (the cyber infrastructure), whether these are in public of private hands,[170] could constitute a violation of territorial integrity,[171] since sovereignty 'protects all infrastructure within a state'.[172] Based on this, the UN GGE has concluded that 'States have jurisdiction over the ICT infrastructure located within their territory'.[173]

166 See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Pp 11-13. But also the UN GGE reports, e.g. the United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174.".

167 Spector, "In Defense of Sovereignty, in the Wake of Tallinn 2.0." pp. 219-223.

168 North Sea Continental Shelf Cases, ICJ Reports. Para 59, p 37. The 1969 North Sea Shelf case confirms not only the land territory but also the territorial sea adjacent to it falls under the full sovereignty and hence sovereign jurisdiction of that State; See also: United Nations Convention on the Law of the Sea. Article 2; Hernandez, *Int. Law*. pp. 474-475.

169 Jensen, "Cyber Sovereignty: The Way Ahead." pp. 277 & 296; Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." pp. 194-196.

170 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (5), p. 18.

171 Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace." p. 129. See also: Michael N. Schmitt and Liis Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?," *AJIL Unbound* 111 (2017): 213–18. p. 216. If attributed to a State, the 2014 Sony Picture hack could have amounted to a violation of sovereignty due to the breach of territorial integrity. Regarding the Sony Picture Hack see also: Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired*, 2014, 2014.

172 Duncan B Hollis and Jan Neutze, "Defending Democracies via Cybernorms," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Duncan B. Hollis and Jens D. Ohlin (Oxford University Press, 2021). p. 321.

173 United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174." Para 27/28, p. 12; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 40; Koh, "International Law in Cyberspace." Question 9, p. 6; United Kingdom Ministery of Defense, "Cyber Primer (2nd Edition)," 2016. p. 4.

The challenge is how to apply the notion of territorial integrity to the virtual dimension of cyberspace[174] with its dematerialised, detemporalised and deterritorialised[175] characteristics, which is different from other domains (land, sea, air) in scale, reach and effect.[176] Activities in cyberspace can be executed from within the territory of the targeted State in which case the violation of sovereignty can be breached.[177] Cyber activities can also be executed remotely, from abroad in which case no physical border will be crossed[178] and a the violation of territorial integrity is more difficult to substantiate.

The specific characteristics of cyberspace raise the question on whether any remotely executed cyber intrusion from abroad into the territory of another State should be classed as a violation, especially if there is no tangible impact.[179]

Violation of territorial integrity is traditionally related to physical incursions into the territory of the State.[180] The approach is also the basis of the French legal opinion related to activities in cyberspace.[181] France argues that *every* cyberattack by another State on the cyber infrastructure or the exploitation thereof on French territory is a violation of sovereignty. Roguski has called this view the penetration-based approach.[182] The advantage of this approach is that all activities conducted within the cyber infrastructure located on the territory of other States without the latter's consent violate territorial integrity.

This 'purist'[183] penetration-based approach is difficult to uphold. Though a remote cyberattack from abroad could cause physical damage or injury and subsequently violate the territorial integrity (and sovereignty) of the State,[184] most cyber intrusions are difficult to

174 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." pp. 13-14.

175 Jackson Adams and Mohamad Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies* 4, no. 6 (2016): 256–65. p. 256; Tsagourias, "The Legal Status of Cyberspace." p. 21.

176 Determining when activities or effects in cyberspace reach the threshold of violating the sovereignty of a State is challenging not least due to the lack of State practice and limited *opinio iuris*.

177 See the 'analogue' parallel with the Israeli Secret Service operators in Argentina in the 1960 Eichmann abduction, Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1659; or the Russian attempt to hack the OPCW from within Netherlands territory, see: Government of the Netherlands, "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW," News item, 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

178 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (5),(10),(21) pp 18, 20 & 23.

179 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." pp. 21-24.

180 Spector, "In Defense of Sovereignty, in the Wake of Tallinn 2.0." p. 222.

181 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace." pp. 6-7. 'Les cyberattaques peuvent être constitutives d'une violation de souveraineté'.

182 Przemysław Roguski, "Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views," *The Hague Program for Cyber Norms Policy*, 2020. pp. 5-6; Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 75. Roguski proposes the intrusion-approach as a way to bridge the gap between the non-sovereignty position of the UK (Wright) and the sovereignty-as-a-rule advocates.

183 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention."

184 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 253.

detect and seldom cause functional let alone physical damage.[185] Moreover, the injured State is often not aware the remote cyber operation is taking place. The State will become aware when the impact takes shape and is tangible on its territory. Schmitt argues, in this sense that it is 'the effect of a cyber operation, not the target, that usually determines whether a territorial sovereignty violation has occurred'. [186] An alternative interpretation of the penetration-based approach is one that requires at least a minimum impact. Contrary to the French stance on this matter,[187] Roguski's introduces the intrusion-based approach, arguing that not all infringements are a violation of sovereignty. Regular use of ICT infrastructure located on other States would not be an unlawful intrusion, neither would unauthorised access. Roguski argues that if the integrity of the data is violated – rather than the availability or confidentiality – a breach would take place.[188] This interpretation is in essence a minimum impact-threshold and the introduction of qualified threshold to assess a violation of sovereignty in cyberspace. Also, the European Union has embraced the qualified threshold approach of the 2019 EU Council Decision on measures against cyberattacks,[189] providing a list in support of determining whether a cyberattack has had a significant effect.

The most prominent scholarly work qualifying the impact on sovereignty by a remote cyberattack from abroad is the second iteration of the Tallinn Manual (*Tallinn Manual 2.0*).[190] The *Tallinn Manual 2.0* lists three criteria in which case a remotely executed cyber operation could violate of the territorial integrity – physical damage, functional damage (the loss of functionality of cyber infrastructure), and infringements falling below the threshold of functional damage. The thresholds are based on the impact of a remote cyber operation rather than on the act itself.[191]

Physical damage or injury can result from the malfunctioning of systems due to malware. Causing physical damage by remote means from abroad may qualify as a violation of sovereignty, also if the impact is indirect.[192] However, as mentioned in the *Tallinn Manual 2.0* itself, it could also amount to a violation of the prohibition of intervention and even the use

185 So far, only France has taken this position, which to other State would rather de defined as espionage, see: Schmitt, "Foreign Cyber Interference in Elections." p. 753; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 254.

186 Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law." Under 'sovereignty'.

187 And providing an alternative view to the effect-based approach of the *Tallinn Manual 2.0*. See: Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." pp. 79-80.

188 Roguski. p. 79.

189 Council of the European Union, "Council Decision Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States," *CFSP*, 2019.

190 Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 76.

191 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention."

192 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 7. See also: Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, pp. 107-108.

of force,[193] especially if damage to the infrastructure in the territory of the State could reach a certain magnitude.[194] However, physical damage does not necessarily invoke the prohibited use of force. The latter is related to the notion that States should solve their conflicts in a peaceful manner. Therefore, damage away from the actual use of interstate force can still be a breach of sovereignty of the State as was the case in the *Rainbow Warrior* Arbitration.[195] Damage to the physical network layer of public or private ICT infrastructure via remote cyber operations (malign software) from abroad can amount to a violation of territorial integrity.

Functional damage could also qualify as a violation of sovereignty.[196] Where physical damage is related to the physical network layer, the loss of functionality relates to the logical and the virtual persona layers of cyberspace.[197] Although the experts of the *Tallinn Manual 2.0* could not agree on exact thresholds, the subject of 'loss of functionality' is at the core of the cyber-related interference with sovereignty. Loss of functionality stems from the degradation, destruction, disruption of data and is an infringement of the confidentiality, integrity or availability (CIA) of the data or the system as a whole.[198]

Activities that do not result in physical or (permanent) functional damage of a system in cyberspace are difficult to grasp not least since there is no definition of functional damage given. The examples used in the *Tallinn Manual 2.0* or by other scholars fall within the logical or virtual persona layers of cyberspace,[199] e.g. the temporary loss of functionality, the data theft, port scanning (reconnaissance) with malicious intent,[200] or the creation of a backdoor preparing for future cyberattacks. Damage caused by soft-cyber or influence operations that use cyberspace as a vector to target the cognitive dimension is also difficult to establish.

Though these activities could violate territorial integrity based on the penetration-approach, the actual penetration or unauthorised access will difficult to demonstrate due to manner in

193 Schmitt uses the example of Stuxnet in this case, which has been assessed as a use of force by the experts of the Tallinn Manual, see: Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p 43; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 71 (10) p. 342; Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?," *Journal of Conflict and Security Law* 17, no. 2 (2012): 212–27. pp. 220-221. The Stuxnet attack was a cyber-related activity resulting in damage. The experts of the Tallinn Manual unanimously considered it a use of force. See: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 71 (10), p. 342.

194 Heintschel von Heinegg states that it is generally accepted that damages to cyberinfrastructure constitutes a violation of sovereignty, though others argue that this only applies beyond a certain magnitude. Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace." pp. 128-129.

195 RIIA, Rainbow Warrior (New Zealand v France), 20.

196 The German opinio iuris speaks about 'functional impairment', see: German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace." p. 4.

197 The so-called Hard-Cyber Operations, in contrast to Soft-Cyber Operations that use cyberspace as a vector to gain effects in the cognitive dimension. See Chapter 2, § 2.2.3.

198 See also: Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 79.

199 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 4(14), p. 21; Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 21.

200 Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 79.

which data is transferred in cyberspace – related to the technical design of TCP/IP protocols of Internet.[201] Messages via the Internet are sent in packets that do not follow the same route. Moreover, digital communication in general is permitted by existing treaties including the international telecommunication law.[202] Activities below the level of functional damage could even fall below the *de minimis non curat lex*-maxim (i.e. 'the law is not concerned with trivial things'),[203] if they do not reach a certain magnitude,[204] or they could be classed as activities of cyber-espionage.[205] Activities that do not result in physical or permanent functional damage can breach sovereignty, though there is no generic set of criteria, and the legality of these activities should be assessed on a case-by-case basis.[206]

3.3.3.2. Political independence

States enjoy the exclusive right to perform inherently governmental functions on their territory, and to freely develop political, economic and social systems.[207] Activities such as law enforcement, national defence, or conducting elections fall in this remit. The inherently governmental functions are related to the authority the State has but not related to the jurisdiction on how to implement these functions.

Related to cyberspace, the *Tallinn Manual 2.0* distinguishes two ways in which the political independence of a State can be violated: first by the usurpation of and, second, by interference with, the inherently governmental functions.[208]

201 Transmission Control Protocol/ Internet Protocol, see: Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (2018). pp. 129-136.

202 As also mentioned by Roguski, see: Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 79,but also Ian Walden, "International Telecommunications Law, the Internet and the Regulation of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski, 2013. pp. 266 ff.

203 E.S. Roscoe, "The Future of International Law," *The North American Review* 207, no. 749 (1918): 558–63. p. 561. See also: Roguski, "Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views." p. 4; Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 21; Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace." p. 129. Activities in this area could still violate national (penal/cybercrime) legislation.

204 Roguski, "Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views." p. 4; Jensen, "Cyber Sovereignty: The Way Ahead." pp. 302-303.

205 Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart, 2019). pp. 17-18; Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." pp. 201-202; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 4 (7-9) pp. 19-20.

206 Theft of data is not a legitimate act, it is merely that these acts are not covered by public international law, but by national criminal law, see e.g.: Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 193; United States District Court, Indictment (United States v Netyksho) (2018).

207 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."

208 The experts of the Tallinn Manual process could not define the inherently governmental functions, and (subsequently) expressed caution in the test regarding interference and usurpation. See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. para 16-17, p. 22.

Usurpation is the notion of taking over and performing governmental functions which inherently belong to another State. Usurpation could be argued to be a restriction articulated in the otherwise permissive tenure of the 1927 Lotus Case, in which the Permanent Court of Justice (PCIJ) stated that 'failing the existence of a permissive rule to the contrary, it [a State] may not exercise its power in any form in the territory of another State'.[209] An example of the unlawful seizure of sovereign power in derogation of the constitution of the proper ruler is extraterritorial law enforcement.[210] Usurpation of inherently governmental functions is ambivalent. Efrony and Shany argue that usurpation is a violation of the prohibition of intervention in the absence of coercion,[211] with interventions in elections as the pivotal example. De facto, these authors argue that inherently governmental functions equal the reserved domain (a notion related to the principle of non-intervention), which is not aligned with the delineation used in this research. [212]

Interference with the inherently governmental functions means tampering with or frustrating the State's functions including the ability to hold elections, collect taxes, manage crises[213] or establish a system of social welfare.[214] Manipulating the registration system for voters, disrupting the websites used for fiscal revenue services, or launching a foreign influence operation dissuading voters to cast their ballots could amount to an interference. Not every infringement of the State functions will amount to an unlawful interference, but only those interferences that undermine the ability of the State to perform its functions. Disrupting a State function, e.g. conducting an election, is an interference in this sense, though persuading a foreign government to change its view on a specific topic is not.[215] While the State functions are generic and universal in nature, the tasks a government performs are not. The latter depend on the governmental structure of the State under threat. In the UK, the National Health Service is a task performed by the government, but not necessarily a State function.[216] Conversely State functions could also be privatised.[217]

209 PCIJ, The Case of the S.S. Lotus (France v. Turkey) - Judgment, Series A Collection of Judgments. p. 18.

210 Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1660.

211 Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice," *The American Society of International Law* 112, no. 4 (2018): 583–657. p. 642.

212 See § 3.3.4.1. and for the difference between State functions and reserved domain, see also: Michael N. Schmitt, "Foreign Cyber Interference in Elections: An International Law Primer, Part I," *EJIL*, 2020, 1–6. p. 2; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 9.

213 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 255.

214 But also other political roles of the State such as the task of crisis management or official and public communication (e.g. on Covid-19), what Almond calls 'political communication', see Gabriel A. Almond, "Comparative Political Systems," *The Journal of Politics* 18, no. 3 (1956): 391–409. pp. 395 ff.

215 In that vein: interfering with the State's task to perform its task in crisis management such as during the Covid-19 pandemic is an inherently governmental task. How the State choses to tackle the crisis is a matter of policy and hence part of the reserved domain of the State. See also: Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 254-256.

216 Milanovic and Schmitt. pp. 254-255.

217 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (16), p. 22. E.g. private military contractors. Despite the privatised execution of the task, it remains a State function.

A violation of political independence in cyberspace does not require physical or functional damage, contrary to a violation of territorial integrity. The majority of experts of the *Tallinn Manual 2.0* argued that political independence is breached 'irrespective of where the cyber operation occurs or manifests' itself.[218] A minority argued that the operation must manifest on the territory of a sovereign State. However, this view must not be looked upon as opposing the majority view, but as stemming from a different perception of cyberspace, i.e. one focusing on the physical network layer. All experts agree that a violation of a purely virtual nature could violate the political independence if it usurps or interferes with the inherently governmental functions.[219]

3.3.4. Core elements of violations of sovereignty

Sovereignty, traditionally based on territoriality, entails territorial integrity and political independence. Without justification, a violation of sovereignty of a State is unlawful. Applying international law, including the respect of sovereignty, to cyberspace can be challenging due to the boundless, a-territorial and ubiquitous characteristics of the virtual dimension of cyberspace (logical and virtual persona layer).[220] The virtual dimension does not fit well with the notion of territoriality.[221]

But these difficulties do not render the rule of sovereignty inapplicable in cyberspace. Activities in cyberspace that cause physical or functional damage, or non-consensual activities in cyberspace carried out by foreign agents on the territory of the targeted State can still violate territorial integrity. Conversely, remote cyber activities, e.g. foreign influence operations aimed to alter the cognitive dimension of a targeted audience causing little or no physical impact, would be less likely to violate the territorial integrity of another State. Apart from violating territorial integrity, activities in cyberspace can also breach the political independence of a State.

Since damage is not a requirement for a violation of political independence in cyberspace, remote cyber-related activities may violate the sovereignty of a State if they interfere with or usurp the State functions.

218 Schmitt. Rule 4 (19), p. 23.

219 Schmitt. Rule 4 (21), p. 23.

220 Stephens, "Influence Operations & International Law." p. 9. Stephens argues that the legal regimes related to use of force, intervention and the violation of sovereignty were developed in the context of physical geo-political activities.

221 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 21, note 102; Schmitt and Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?" p. 218.

The main conclusion is that States enjoy sovereignty over cyber infrastructure, persons and cyber activities on their territory,[222] based on territorial integrity and political independence. Though remotely conducted cyber operations, especially foreign influence operations, are less likely to affect the territorial integrity of a State when executed from abroad, remote cyber operations could violate the political independence of the State.[223] Based on the notion that political independence can be violated in cyberspace, it can be concluded that sovereignty is a binding rule of customary international law in cyberspace,[224] as it is in other (physical) domains.

Section 3.4.: Intervention

'Cuius regio, eius religio'[225]

3.4.1. The legal basis for the prohibition of intervention

The prohibition of intervention is widely considered to be both a principle and a rule of customary international law.[226] The legal basis for this primary rule between States vis-à-vis each other[227] can be found in treaties and foremost in customary international law.

UN Charter, Article 2(7),[228] contains an element of non-intervention stipulating that the UN – not States - should refrain from any form of interference in matters which are essentially within the domestic jurisdiction of the States.[229] Though there is no universal codification of the prohibition of interventions in treaty law, regional treaties have adopted prohibitions

222 Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1647.

223 Peter B.M.J. Pijpers and Bart G.L.C. Van Den Bosch, "The 'Virtual Eichmann': On Sovereignty in Cyberspace," *ACIL Research Paper 2020-65*, 2020. pp. 19-20; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (21), p. 23.

224 See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. pp. 11-13. But also the UN GGE reports, e.g. the United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174.".

225 'Whose realm, his religion', the central idea in the Treaty on the Peace of Augsburg 1555. Despite the wording the principle did not prelude religious freedom or absolute prohibition of religious interventions, but merely allowed the co-existence of two forms of religion: Roman Catholicism and Lutheranism.

226 Jennings and Watts, *Oppenheim's International Law*. pp. 428-430; "Case Concerning Military and Paramilitary Activities in and against Nicaragua - Dissenting Opinion of Judge Jennings," *ICJ*, 1986. p. 524.

227 Gill, "Non-Intervention in the Cyber Context." p. 223.

228 Gill. pp. 219-220.

229 Kunig, "Prohibition of Intervention." Paras 11-12, pp. 3-4; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 67(1) p. 325.

of intervention,[230] e.g. the 1933 Montevideo Convention,[231] the 1948 Charter of the Organisation of American States,[232] the 1961 Vienna Convention on Diplomatic Relations,[233] or the Constitutive Act of the African Union.[234]

Non-intervention as a customary rule is reflected in case law. Numerous judgments and deliberations on the prohibition of intervention in another State refer directly or indirectly to the general practice and its acceptance as a rule of customary international law.[235] In the 1949 *Corfu Channel* Case, the ICJ rejected the alleged right to intervene, especially emphasising that intervening as a 'policy of force'[236] has no place in international law. The 1986 *Nicaragua* Case is a seminal judgment related to the legal interpretation of non-intervention. The ICJ stated that the prohibition of intervention is 'part and parcel' of customary international law,[237] and contended, in line with the Montevideo Convention and UNGA Declaration on Friendly Relations, that the principle forbids States to intervene in the internal affairs of other States.[238] The ICJ thereby argued explicitly that the principle of non-intervention forbids States to intervene directly or indirectly in internal or external affairs of other States.[239] In the 2005 *Armed Activities* Case, the ICJ again indicated that the provisions as mentioned in the UNGA Declaration on Friendly Relations are expressions of customary international law referring to the prohibition of intervention,[240] though actually addressing the prohibition of the use of force.[241]

230 Though the articles in the regional treaties might deviate from the the principle of non-intervention in customary international law, see: Schmitt, "Foreign Cyber Interference in Elections." p. 744.

231 Articles 3 and 8 of the International Conference of American States, "Montevideo Convention on the Rights and Duties of States" (1933). Article 8 was affirmed in the Additional Protocol Relative to Non-Intervention in 1936.

232 OAS, Charter of the Organization of American States. Articles 9 and 13.

233 "Vienna Convention on Diplomatic Relations" (1961). Article 41.

234 African Union, "Constitutive Act" (2000). But see also art 2 of the ASEAN, "Treaty of Amity and Cooperation in Southeast Asia" (1976).

235 Crawford, *Brownlie's Principles of Public International Law*. p. 21.

236 Corfu Channel Case (merits) - Judgment of 9 April 1949, ICJ Reports. p. 35.

237 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. p. 106.

238 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."

239 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, pp. 107-108.

240 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports. Para 165, p. 227.

241 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports. pp. 226-227 & para 266, p. 259.

The UNGA has issued several resolutions[242] related to sovereignty and non-intervention,[243] most importantly the 1970 Declaration on Friendly Relations.[244] The Declaration on Friendly Relations emphasises that States should refrain from the threat or use of force, highlighting the essence of the *jus cogens* nature of the prohibition of the use of force as recognised in Article 2(4) of the UN Charter, but it also highlights the 'duty to refrain from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any other state', and warns 'not to intervene in matters within the domestic jurisdiction of any State',[245] as breaching these elements constitutes a violation of international law.[246] UNGA resolutions are generally considered to be non-binding and cannot be assumed to validate or affirm customary law in general. However, in some cases a resolution can be seen as a confirmation of customary international law,[247] though not all resolutions regarding non-intervention reflect a universal acceptance of law. In general resolutions express a majority view.[248]

3.4.2. The characteristics of interventions

The prohibition of intervention is a corollary to every State's right to sovereignty, territorial integrity and political independence.[249] Non-intervention not only safeguards States from unlawful interference, but also gives substance to the concept of sovereign equality

242 But also regional organisations such as the CSCE, Helsinki Final Act. Item 1 (a) VI under chapter regarding questions related to security in Europe.

243 Starting with the 1949 International Law Commission, Draft Declaration on Rights and Duties of States.; the 1965 United Nations General Assembly, "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty - Resolution 2131 (XX)."; United Nations General Assembly, "Charter of Economic Rights and Duties of States - Resolution 3281 (XXIX)," 1974.; United Nations General Assembly, "Definition of Aggression - Resolution 3314 (XXIX)."; United Nations General Assembly, "Declaration on Non-Interference in the Internal Affairs of States - A/Res/31/91," 1976.; 1981 United Nations General Assembly, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States - A/Res/36/103." See also the post-WWII discourse in Wright, "Subversive Intervention."

244 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."

245 United Nations General Assembly. Preamble and third principle.

246 United Nations General Assembly. Third principle, which uses similar language as earlier stated in art 8 of the 1933/1936 Montevideo Convention.

247 Maziar Jamnejad and Michael Wood, "The Principle of Non-Intervention," *Leiden Journal of International Law* 22, no. 2 (2009): 345–81. p. 352.

248 The 1986 Resolution (36/103) was adopted with 102 against 22 votes, endorsed by then Warsaw pact and non-aligned States and objected by the majority of Western States, see: Kunig, "Prohibition of Intervention." Para 20; Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. p. 196.

249 Jennings and Watts, *Oppenheim's International Law*. p. 428.

among States.[250] An unlawful intervention breaches a legal obligation and constitutes an internationally wrongful act if the intervention is attributable to a State.[251]

An intervention contains two elements:[252] the interference impacts upon the domestic jurisdiction - *domaine réservé* - of another State, and it is coercive in nature.[253] Deriving from sovereignty, States are entitled to exercise jurisdiction 'by subjecting objects and persons within their territory to domestic legislation and to enforce these rules.'[254] Jurisdiction can be described as the legislative (or prescriptive), enforcement and adjudicatory authority of the State over infrastructure, persons, materiel and activities within its territory.[255] Coercion may entail an armed element, but this will be regarded as a special kind of intervention,[256] as mentioned in § 3.2. Nonetheless, interventions that fall short of the use of force can still be coercive in nature,[257] based on diplomatic or economic threats.[258]

3.3.4.1. Domaine réservé

The *domaine réservé*, or reserved domain,[259] is the area 'in which each State is permitted, by the principle of State sovereignty to decide freely. This area is the choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[260]

250 As mentioned in: United Nations, Charter of the United Nations. Art 2(1); See also art 52 of the "Vienna Convention on the Law of Treaties" (1969).; Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," in *Cyber War: Law and Ethics for Virtual Conflicts*, 2015. p. 250; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66(1), p. 312.

251 Gill, "Non-Intervention in the Cyber Context." pp. 226-228.

252 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 48; Steven J Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion," *Just Security*, 2017. 3rd paragraph; Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 27.

253 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. para 205, pp. 107-108; Jennings and Watts, *Oppenheim's International Law*. p. 430.

254 Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace." p. 124.

255 Jennings and Watts, *Oppenheim's International Law*. p. 456; Cedric Ryngaert, "The Concept of Jurisdiction in International Law," in *Research Handbook on Jurisdiction and Immunities in International Law*, ed. Alexander Orakhelashvili (Edward Elgar, 2015), 50–75. Section 2.

256 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." p. 258. Watts argues that "it may be appropriate to understand the principle of non-use of force as a form of *lex specialis* with respect to intervention, particularly with respect to acts simultaneously constituting direct uses of force." See in that context also the Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports. Para 164, p. 227; Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 209, pp. 109-110.

257 Gill, "Non-Intervention in the Cyber Context." p. 218.

258 Jamnejad and Wood, "The Principle of Non-Intervention." pp. 367-377.

259 PCIJ, Nationality Decrees in Tunis and Morocco - Advisory Opinion, Series B PCIJ Reports (1923). p. 24.

260 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205 p. 108; Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." p. 191. See also: United Nations General Assembly, "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty - Resolution 2131 (XX)."; United Nations General Assembly, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States - A/Res/36/103."Corn and Taylor, "Sovereignty in the Age of Cyber." p. 208.

The *domaine réservé* relates to the internal or domestic jurisdiction of a sovereign State,[261] and has an internal and external aspect.[262] The Montevideo Convention mentions that 'every recognised state has the right to (...) organise itself as it sees fit, to legislate upon its interest, administer its services and to define the jurisdiction, and competences of its courts.'[263] The internal aspect reflects the right of peoples or population to self-determination once they have achieved statehood.[264] The external aspect of State jurisdiction refers to the sovereign State's formulation of foreign policy, the prerogative to choose with whom to enter into diplomatic relations, to conduct a foreign economic support programme,[265] or enter into membership of an international organisation or the formation and abrogation of treaties.[266] The sovereign jurisdiction of the State is not unrestricted.[267] The jurisdiction of the State must comply with, and can be limited by, international law both via customary international law and (bi- and multilateral) treaties,[268] such as international human rights law. Also, UN Security Council resolutions or unilateral declarations can limit the domestic jurisdiction of a State.

The limitations of the jurisdiction of the State are not involuntary, but stem from increased cooperation of States or otherwise voluntary acceptance of international legal obligations.[269]

261 Gill, "Non-Intervention in the Cyber Context." p. 217; Kunig, "Prohibition of Intervention." Para 3; Katja S Ziegler, "Domaine Réservé," *Max Planck Encyclopedia of International Law*, no. April (2013). Para 1; It can be argued that this notion coalesces with internal self-determination: the right to freely choose their own political, economic, and social system. See: Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." p. 265.

262 Jennings and Watts, *Oppenheim's International Law*. pp 430-431. Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace." Under the header 'Intervention'; Jennings and Watts, *Oppenheim's International Law*. p. 430; Schmitt, "Foreign Cyber Interference in Elections." p. 745.

263 International Conference of American States, Montevideo Convention on the Rights and Duties of States. Article 3.

264 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020. pp. 51-52; United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."; Salvatore Senese, "External and Internal Self-Determination," *Social Justice* 16, no. 1 (1989): 19–25. p. 19.

265 In the Nicaragua case the ICJ assessed the claim of Nicaragua whether a change in the economic policy termination of aid) of the US breached the prohibition of intervention. But the US aid was does not fall within the reserved domain of Nicaragua and can be seen as an expression of economic foreign policy. Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. paras 123-125, 244-245 & 276; See also: Baade, "Fake News and International Law." p. 1363. A similar rationale can be followed with 1973 reduction in oil production of the oil production Arab states, Jamnejad and Wood, "The Principle of Non-Intervention." p. 370.

266 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." pp. 267-268.

267 Crawford, *Brownlie's Principles of Public International Law*. pp. 191-200 arguing that the power of disposition of a State can be limited by treaties leaving the title unaffected; Or as the Netherlands government stated in that context: 'The Netherlands' decision to accede to the Convention on Cybercrime of the Council of Europe is an example of the exercise of Dutch sovereignty.', Netherlands Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace. p. 2; In a similar vein Crawford states that 'human rights standards qualify, but do not displace, the sovereignty of states'. Crawford, "Sovereignty as a Legal Value." p. 122. Other restrictive obligations relate to international human rights law, respect for the immunity of other States' diplomats, or the international protection of minorities Kunig, "Prohibition of Intervention." Para 3, p. 1; ICAO, Convention on International Civil Aviation. Articles 1 & 3 (c).

268 PCIJ, Case of the SS Wimbledon (Great Britain v. Germany) - Judgment (1923). p. 25; Ziegler, "Domaine Réservé." Para 2.

269 Corfu Channel (U.K v. Alb.), 1949 I.C.J. (Opinion of Judge Alvarez), ICJ Reports. p. 43. Judge Alvarez argues that 'we can no longer regard sovereignty as an absolute and individual right of every State', instead sovereignty of the State is bound not solely by their free will but also due to social interdependence and the predominance of the general interest;

Regarding the prohibition of intervention Higgins argues: 'The purpose of the international law doctrine of intervention is (...) to provide an acceptable balance between the sovereign equality and independence of states on the one hand and the reality of an interdependent world and the international law commitment to human dignity on the other'.[270]

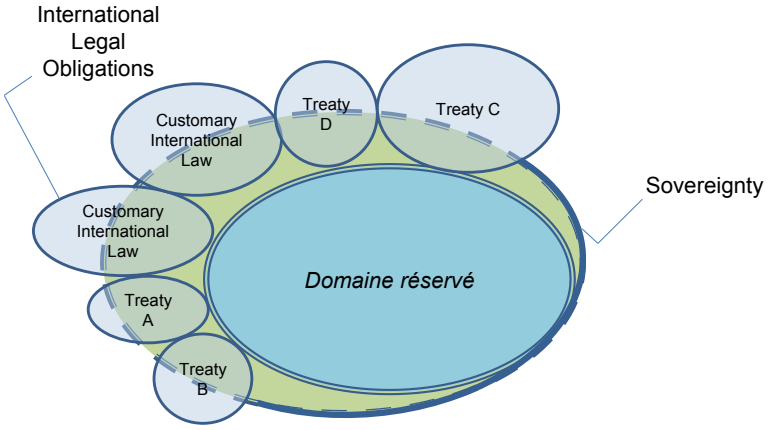

Figure 3 - 3 Domaine réservé

The size of the reserved domain of the State is 'a relative question',[271] as alluded in the 1923 *Nationality Decrees* Case, and dependent on the number and density of the international obligations of the State.[272] Within this (decreasing) domain,[273] any intrusion which does not find justification in international law, violates the right of the State to conduct its foreign relations and domestic affairs without outside interference. The object of an intervention in the reserved domain is related to undermining the State's ability to make free choices in the political system and its organisation.[274]

Ziegler mentions three dimension which reduces the *domaine réservé*: the increase in interdependence; development of international law; and increase in international integration (e.g. EU), Ziegler, "Domaine Réservé." Para 8.

270 Higgins, "Interv. Int. Law." p. 273.

271 PCIJ, Nationality Decrees in Tunis and Morocco - Advisory Opinion, Series B PCIJ Reports. p. 24.; Kunig, "Prohibition of Intervention." Para 3, p. 1; Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace*, *International Law*, 2013. p. 164.

272 PCIJ, Case of the SS Wimbledon (Great Britain v. Germany) - Judgment, Series A. p. 30. In which Germany is required to have a treaty article prevail over an invoked element of sovereignty (neutrality). See also: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 p. 316; Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?" p. 1588.; Koh, "International Law in Cyberspace." Mentioning "[t]he exercise of jurisdiction by the territorial State, however, is not unlimited; it must be consistent with applicable international law, including international human rights obligations."

273 Besson, "Sovereignty." Para 122.

274 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020. P. 48; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (10-11), pp. 315-316.

The relation between international conventions and the reserved domain is also referred to in the 1923 *Wimbledon* Case, which made clear that any treaty (or other international legal) obligation consented to by a sovereign State or binding on a State prevails over the inherent or original sovereignty of that State.[275]

The reserved domain is a notion distinct from the inherently governmental function of the State.[276] Though the domains 'overlap to a degree (they) are not identical'.[277] The topics covered including law enforcement or conducting election intersect, but the two notions have a different base.[278] Inherently governmental functions are particular functions only States can perform including administering justice or conduct elections. The domaine réservé is the domain of domestic jurisdiction of a State activity that is not governed by international law. [279] The jurisdiction of the State encompasses activities in the public and private sphere, but is limited by international law.[280] Defending national borders, conducting war, or enforcing the law are State functions, whereas the manner in which prisoners of war or suspects are treated is subject to international law and beyond the domaine réservé. Conversely modern States perform tasks that are neither functions of the State nor covered by international law.[281]

Conducting elections is an inherently governmental function, while 'how' the State conducts them is based on national legislation and restricted by international obligations. Depending on the execution of the cyber-related influence activity, meddling in foreign elections could both be an interference in the governmental functions and invasive in the reserved domain, the latter being an intervention only if the act is coercive in nature.[282]

3.3.4.2. Coercion

Intervention is perceived to be wrongful when it 'uses methods of coercion in regard to such choices, which must remain free ones'.[283] Interference as such, lacking the element of

275 PCIJ, Case of the SS Wimbledon (Great Britain v. Germany) - Judgment, Series A. pp. 30 & 33. In this case Germany refused the treaty-based free passage to belligerent States based on the fact that Germany itself claimed neutrality.

276 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 48-49.

277 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (22), p. 24; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 256.

278 Overthrowing a government will primarily violate the state functions but will also (indirectly) undermine the State's authority to make free choices. See: Gill, "Non-Intervention in the Cyber Context." p. 222.

279 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (7), p. 314.

280 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 255-257.

281 Purely commercial activities, or activities between private actors, are not covered in this domain. See: Schmitt, "Grey Zones in the International Law of Cyberspace." p. 7; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 255-257.

282 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (10), p. 315.

283 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

coercion, does not constitute an intervention.[284] Coercion is therefore 'the very essence of prohibited intervention'.[285]

Coercion means applying unwanted pressure upon another actor ranging from non-kinetic threats to the use of armed force, thereby compelling the targeted State to subordinate to the coercive State.[286] Or as Joyner states: 'Coercion in inter-State relations involves the government of one State compelling the government of another State to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force'.[287] The result of coercion is to effectuate change in the attitude or behaviour of the target State. Coercion has been described in different ways in legal writing and case law and,[288] though it 'has not yet fully crystallised in international law',[289] it has legal consequences.[290] The ICJ mentioned in the *Nicaragua* Case that coercion 'is particularly obvious in the case of an intervention which uses force in the direct form of military action'.[291] Coercion in the *Nicaragua* Case could coalesce with customary law on the prohibition of the use of force as recognised in Article 2(4) UN Charter,[292] as is echoed by the Netherlands government stating that 'although there is no clear definition of the element of coercion, it should be noted that the use of force will always meet the definition of coercion. Use of force against another state is always a form of intervention.'[293] Aside from the coercive use of force, coercion can be described as being dictatorial. According to Oppenheim, 'to constitute intervention the interference must therefore be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question',[294] which broadens the concept to diplomacy, economy and other means if they are coercive in nature. But coercion can also have a more subtle and psychological dimension, manipulating the opponent's choices and reducing the number of options to choose from, applying subversive, psychological, covert

284 Jennings and Watts, *Oppenheim's International Law*. p. 432.

285 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

286 Stephens, "Influence Operations & International Law." p. 7.

287 Christopher C Joyner, "Coercion," *Max Planck Encyclopedia of International Law*, 2006. Para A; see also Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 66 (18) p 317 with a similar definition.

288 See also Gill, "Non-Intervention in the Cyber Context." Note 4 on p. 219, providing an outline of the different forms of coercion.

289 Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace. p. 3.

290 Kunig, "Prohibition of Intervention." Para A.1.(b); Tzanakopoulos, "The Right to Be Free from Economic Coercion." p. 623; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (18) p. 317.

291 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. para 205, p. 108.

292 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020. pp. 52-53.

293 Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace. p. 3; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis) Information Operations During a Pandemic." p. 255.

294 Jennings and Watts, *Oppenheim's International Law*. p. 432.

manipulative means.[295] In general, coercion includes forceful means, but building on the limitation as alluded to in Chapter 1, coercion in this thesis excludes the use of force or threat of force i.e. military coercion.[296]

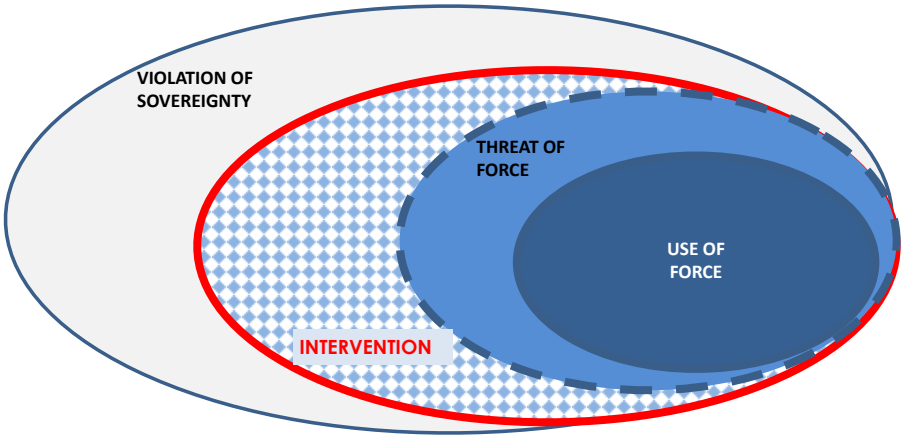

Figure 3 - 4 Intervention

Coercive interventions, (the chequered area within the red circle in figure 3-4) include economic, diplomatic, informational or any other form of subversive measures,[297] as long as they have the 'necessary coercive effect'.[298] These intervention are wrongful,[299] if intended to undermine the control of the State and prevent the State from exercising its free will, or sovereign rights,[300] on matters which fall within its reserved domain.[301] In the 1986 *Nicaragua* Case the ICJ determined that arming and training the Contras would amount to threat or use of force against Nicaragua, while this would not necessarily be so for mere financial

295 Steven Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber," in *New Technologies: New Challenges for Democracy and International Law*, 2019, 1–27. pp. 6-7; Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020., p. 53; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (18), p. 317.

296 See § 1.2.4.

297 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."; Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

298 Jennings and Watts, *Oppenheim's International Law*. p. 434; See also United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)." Stating that '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, or interfere in civil strife in another State.'

299 Kunig, "Prohibition of Intervention." Paras 24-27; Jamnejad and Wood, "The Principle of Non-Intervention." pp. 368-377.

300 Gill, "Non-Intervention in the Cyber Context." p. 221.

301 Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs." p. 31.

assistance. In the view of the ICJ supplying funds is not a threat or use of armed force, but it is 'an act of intervention in the internal affairs of Nicaragua'.[302]

The compelling elements of coercion are the deliberate undermining of the ability and will of the targeted State to autonomously make decisions, as the aim of the coercer is to effectuate a change in policy.[303] The legal appreciation of coercion is related to control, or the lack of control,[304] to make decision freely and autonomously. With reference to the *Nicaragua* Case, intervention is wrongful if it uses methods of coercion regarding the choices that should be to the State's own make, such as the choice of 'a political, economic, social and cultural system, and the formulation of foreign policy.'[305] The Declaration of Friendly Relations also reflects the lack of control when it uses the wording 'the subordination of the exercise of its sovereign rights'[306] to express the prerogative of control and autonomous decision making of the state.

The coercer pursues a change of policy of the State,[307] or intends to effectuate a particular course of action. The intent of the coercer is pivotal,[308] as it objectifies the purpose of a change the policy. Or, as Stern mentions, 'unilateral economic sanctions are not unlawful in themselves, but can become unlawful if the intention of the State which adopts them is to override the sovereign will of another State and to intervene in its domestic affairs'.[309]

302 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 228, p. 119.

303 Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" p. 224; Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." pp. 2 & 29-30. This could also be referred to as undermining the self-determination of a State, see: Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 10.

304 Jennings and Watts, *Oppenheim's International Law*. p. 432. Oppenheim mentions that 'in effect' coercion means 'depriving the state intervened against of control over the matter in question'; See also: Gill, "Non-Intervention in the Cyber Context." p. 222.

305 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205 p. 108; Stephens, "Influence Operations & International Law." p. 7.

306 United Nations General Assembly, "Declaration on Principles of International Law Concerning Friendly Relations and Co Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)."

307 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (19) p. 318; Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 5. Arguing that coercive threat result in a change of behaviour of others.

308 Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." Wheatley considers the intent as the crucial element in coercion when stating that "Where an outside power intends to determine the outcome of the political processes of another state, and acts on that intention, that behaviour is 'coercive' in nature." p. 18; see also Jamnejad and Wood, "The Principle of Non-Intervention." p. 381; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 51; Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law." under 'Intervention'.

309 Brigitte Stern, "The Elements of An Internationally Wrongful Act - Part III The Sources of International Responsibility," in *The Law of International Responsibility*, ed. James Crawford, Alain Pellet, and Simon Olleson (OUP, 2010). p. 210.

Coercive interference, constituting an intervention that fails to reach a desired outcome still breaches the prohibition of intervention.[310] An attempt does not need to succeed,[311] as the primary requisite is the deliberate intent of the coercer to undermine the control and decision-making processes of the other State (related to the choice of a political, economic, social and cultural system and the formulation of foreign policy) with the aim to pursue a change in policy.[312]

The question whether a State is aware of an intervention is relevant as it uncovers the difference between compellence as a strategic term and coercion as a legal one.[313] Borghard and Lonergan argue that clear communication is a precondition for compellence, if that condition is not met, the targeted audience will be unaware of behaviour to be displayed.[314]

This dialectic analysis is also found in the deliberations in the *Tallinn Manual 2.0*. On the one hand, under the header of Rule 70, the definition of threat of force i.e. military coercion, the *Tallinn Manual 2.0* argues that a threat, which is usually intended to be coercive in nature, 'must be communicative in nature', must be 'conveyed to the target State.'[315] Within the *Tallinn Manual 2.0* remit of intervention (Rule 66), this is also the position of a minority of experts who argue that if a State is 'unaware of the coercive act, its will has not been coerced'.[316] Hence, in strategic studies, knowledge is a precondition for a compelling intervention. On the other hand, awareness of the coercive act is irrelevant for the legality of the act, which is the majority view of the *Tallinn Manual 2.0* experts.[317] The lack of knowledge as such does not preclude the wrongfulness of an intervention.[318] Whether the injured State is aware of the intervention or not is relevant for appealing for redress, but not for the violation as such.

310 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (29) p. 322; Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 18; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 52.

311 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 241, p. 124.

312 Also the 1986 Nicaragua Case mentions the intent, when it argues that 'if one State, *with a view to* the coercion of another State, (...) that amounts to an intervention (...). (Italics added). See Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 241, p 124.

313 Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." pp. 4-9; See also Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020. p. 56.

314 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81. p. 455, this based on the work of Schelling, see: Thomas C. Schelling, *The Strategy of Conflict*, *Harvard University Press*, 1980 ed (Cambridge, Mass: Harvard University Press, 1960). pp 187-188. On the notion of coercion in legal and international relation literature see also: Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020). pp. 79-85.

315 Both cititions: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 70 (4) p. 338.

316 Schmitt. Rule 66 (25) p. 320. Also other scholars take this position: e.g. Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 83-85; Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?" pp. 1591-1594.

317 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (25) pp. 320-321.

318 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," 2020., pp. 55-56.

In line with the majority view, Baade argues that it is not necessary for an intervention to be prohibited when a State does not know it is being compelled to act in a certain manner,[319] not least since the most effective means of intervention are the ones in which the injured State is unaware that its 'decisions are being affected by manipulation, disruption, or disinformation.'[320] The lack of knowledge therefore exacerbates the subversive nature of cyber-related coercive acts and does not disavow it.

An interference is unlawful if it violates the sovereignty of another State, and if no justification for the activity is provided. The justification can be an explicit invitation of the State,[321] an admissible countermeasure or a collective intervention based on Chapter VII of the UN Charter.[322] The unlawful interference constitutes an intervention if it is coercive in nature and invasive in the reserved domain of another State.

3.4.3. Scope and intent of intervention in cyberspace

In general terms, the rule of customary international law regarding the prohibition of intervention is accepted in cyberspace.[323] Though State practice is lacking (similarly to the lack of State practice related to the respect for sovereignty in cyberspace), numerous States, including the UK,[324] have expressed their legal opinions, affirming the existence of the rule of non-intervention in cyberspace. Conceptually, there is no difference in the application of non-intervention to cyberspace; however, in practical terms there are.[325]

In concept, the principle of non-intervention in cyberspace retains the same criteria as in other domains; the act must relate to the *domaine réservé* of a target State and must be coercive in nature. The criteria for coercion also apply in cyberspace i.e. the intent of the coercer to effectuate a change in policy by undermining the targeted State's ability to autonomously

319 Baade, "Fake News and International Law." p. 1364.

320 Ido Kilovaty, "The Elephant in the Room: Coercion," *AJIL Unbound* 113, no. June 27 (2019): 87–91. pp. 88-89.

321 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Rule 66 (32), p. 323.

322 Kunig, "Prohibition of Intervention." Paras 28-33 Under sub D: Justification of interventions. Kunig mentions more justifications which including the so-called Bush Doctrine and the Humanitarian Intervention, which lack universal consensus. See also: Joyner, "Coercion." Para B.

323 Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" p. 221; Schmitt, "Foreign Cyber Interference in Elections." p. 744; Hollis and Neutze, "Defending Democracies via Cybernorms." p. 317.

324 Wright, "Cyber and International Law in the 21st Century." Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace.; Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace."; Sits, "President of Estonia : International Law Applies Also in Cyber Space."

325 Though the exact content can change over time, see: Kunig, "Prohibition of Intervention." Para 2.; Higgins, "Interv. Int. Law." pp. 272-273.

make decisions.[326] The Tallinn Manual Group of Experts argued – with a majority of views - that mere coercion, i.e. an aggressive act, will not amount to an intervention. The 'coercive efforts must be designed to influence outcomes in (...) matters reserved to a target State',[327] alluding to the notion that coercion relates to the elements of intent and change of policy.

In practical terms, the main difference is that the attributes of cyberspace change the nature of coercion and coercive behaviour. Given the characteristics of cyberspace, it is challenging to ascertain coercion below the threat or use of force. Only when (kinetic) force is used, or physical damage is the effect of a cyber operation, are the results tangible, such as the use of the Stuxnet virus to sabotage an Iranian nuclear facility.[328] Furthermore, cyberspace widens the range of instruments. Hard-cyber operations, as examined by Efrony and Shany,[329] can be used to destroy or disable the hardware of the ICT infrastructure or change and disrupt the software and data. If coercive in nature,[330] hard-cyber operations will provide an additional layer in coercive instruments. More fundamental is the potential to compellingly influence the cognitive dimension of persons and groups directly via soft-cyber operations, using cyberspace as a vector.

3.4.3.1. Domaine réservé

The reserved domain is linked to the State's authority to exercise domestic jurisdiction in those internal and external areas that are not governed by obligations of international law, and 'the matter most clearly within a State's *domaine réservé* appears to be the choice of both the political system and its organisations'.[331]

Though there is no fundamental difference between the physical and the 'cyber' notion of the reserved domain,[332] it stands to reason that the characteristics of cyberspace have increased the possibilities to access the reserved domain.[333] Due to social media platforms but also to publicly accessible information via internet, domestic aspects of State policies

326 Biller and Schmitt, "Un-Caging the Bear ? A Case Study in Cyber Opinio Juris and Unintended Consequences."; WannaCry (though not necessarily a State-control act) is an exemplary coercive cyber operation changing behaviour; Kilovaty highlight the 'intent' (and the intrusiveness) of interventions in cyberspace when describing his 'intervention 2.0'. See: Kilovaty, "The Democratic National Committee Hack: Information as Interference."

327 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (19) p. 318.

328 Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Rule 10(9), p. 45.

329 Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." pp. 598-631. All cases chosen are hard-cyber operations, even the cases related to the 2016 US election only focuses on the DNC hack.

330 Not all 11 cases of Efrony & Shany are assessed to be coercive. See: Kilovaty, "The Elephant in the Room: Coercion." p. 87.

331 Ziegler, "Domaine Réservé." Para 5(f); Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (10) p. 315.

332 Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." pp. 40-41.

333 Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion.'" p. 7.

are no longer confined to national stakeholders but reach a global audience. Cyberspace provides a 'facilitative environment' for foreign agents to reach out to citizens and not solely to the political elites of the other State.[334]

3.4.3.2. Coercion

Coercion is traditionally related to the application of force.[335] Though where forceful coercion is obvious in the physical realm,[336] in cyberspace, coercive behaviour will most likely take the shape as informational threats or other subversive methods.

This leads to an interesting dilemma. While the accessibility of the reserved domain has increased significantly, the intangible nature of the virtual dimension evades straightforward coerciveness. The experts of the Tallinn Manual also struggled with this topic.[337] Foreign influence in or via cyberspace can take the shape of executing an informational or propaganda campaign during elections or a referendum in another State. The dissemination of propaganda and potential disinformation, has the purpose to alter or manipulate the perceptions and beliefs of the audience in another State.[338] Based on pre-cyberspace State practice, Schmitt argues that propaganda during elections is not a violation of sovereignty,[339] let alone an intervention, it does affect the domestic policy and surges the information environment of another State.[340]

The first edition of the Tallinn Manual was inclined to suggest that 'manipulation by cyber-means of elections or of public opinion on the eve of elections, as when online news services are altered in favour of a particular party, false news is spread, or the online services of one party are shut off',[341] could constitute prohibited intervention.[342] But not every form

334 Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," *EJIL*, 2019.; Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion.'" p. 7.

335 Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion."

336 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

337 As do other academics, see: Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention."; Ohlin, *Election Interference: International Law and the Future of Democracy.*; Stephen Barela, "Zero Shades of Grey: Russian-Ops Violate International Law," *Just Security*, 2018.

338 Anna Reynolds, *Social Media As a Tool of Hybrid Warfare*, *NATO Strategic Communication Centre of Exellence*, 2014. p. 8.

339 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 46.

340 Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs." p. 6. Cuba on the other hand argues that US television transmission, and radio broadcasts into Cube without the latter's consent does violate territorial sovereignty and treaty obligations. See: United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security A/64/129 (Add 1)," 2009. pp. 2-5.

341 Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Rule 10(10), p. 45.

342 Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion." Under: The Russian Activities Report; Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 200.

of political or economic interference violates the non-intervention principle, since not all interferences are coercive.[343]

Non-intervention is elaborated on more widely in *Tallinn Manual 2.0*, illustrating how the domain reserve and, first and foremost the notion of coercion can be applied to cyberspace.[344] Though the international group of experts of the *Tallinn Manual 2.0* agreed that the choice of political system and its organisation is part of the reserved domain, the spreading of foreign propaganda, white lies or even fabricated news during elections will not immediately qualify as an intervention since the act is not coercive per se. However, manipulation of facts via a sustained targeted campaign to undermine faith in the integrity of the electoral process, directly impacts on voters' choices or induces persons to forgo making use of their voting rights, thus might well qualify as an intervention.

The question that remains is, when is a cyber operation, below the level of the use of force, coercive? Based on the assessment in Chapter 2, cyber operations can try to influence the position of another State in three manners: persuasive, compelling, and manipulative. Although persuasive, compelling and manipulative cyber operations, including influence operations in cyberspace, all have the deliberate aim to change the policy of the other State, not all are coercive in nature.

Persuasive and compelling cyber operations are overt, rational and conscious activities. Persuasive activities are not coercive since they do not undermine the deliberate understanding and autonomous decision-making process but allow actors to make a deliberate (willing) choice.[345] Propaganda from abroad, day-to-day practices of diplomacy or verbal criticism of another State's policies are, in general, examples of persuasive influence operations.[346] During these influence activities the State tries to persuade the targeted audiences of another State to change the weighing of the options to choose from, but the target State 'retains the ability to choose'.[347] If, however, the audiences' options of choice are severely restricted, the propaganda could become coercive.

Compelling activities in cyberspace, as in any other domain, force an unwilling act which undermines the autonomous ability to make a decision. Installing and executing ransomware such as NotPetya or WannaCry are compelling (hard-cyber) operations since they reduce the options to choose from to one, thus eliminating the autonomous decision-

343 Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Rule 10(10), p. 45.

344 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (9), p. 315.

345 Schmitt. pp. 318-319.

346 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." pp. 261 & 268; Gill, "Non-Intervention in the Cyber Context." p. 223; Jamnejad and Wood, "The Principle of Non-Intervention." pp. 374-375.

347 Schmitt, "Grey Zones in the International Law of Cyberspace." p. 8.

making of the other actor.[348] In the Nicaragua Case, financial support to opposing forces of the incumbent government was recognised as a violation of the prohibition of intervention, based on a coercive economic act. A diplomatic or economic act (economic sanctions or countermeasures)[349] of that magnitude in cyberspace would similarly breach the prohibition of intervention.[350]

Manipulative cyber activities, especially manipulative influence operations in cyberspace are often covert and invoke subconscious judgments based on heuristics, meaning that the autonomous decision-making process of the targeted audience is not just undermined but circumvented altogether.[351] Manipulative influence operations could deprive the audiences of the targeted State of their free choice. The audiences are often not aware that they are being influenced. Manipulative influence operations exploit subconscious heuristics and biases of the targeted audience. Though these operations are not new and find their origin in doctrine such as Russian Reflexive Control and Active Measures,[352] cyberspace is an accelerator in the use, exploitation and effectiveness of these techniques.

Manipulation is not coercive per se. But if coercion can be defined as having the intent of changing the policy of another State and deny the target State the ability of deliberate understanding and autonomous decision-making, then some manipulative influence operations, achieving the same effect are coercive in nature. The coercive element of manipulative influence operations stems from the ability to subconsciously target the biases and heuristics of audiences by making use of the informational instrument of power via cyberspace.

348 Using malware including NotPetya is coercive but does not necessarily constitute a violation of intervention, not least since it is unclear whether the perpetrator was a State actor and whether the reserved domain was invaded. If the target was a commercial actor this might possibly not be the case.

349 Tzanakopoulos, "The Right to Be Free from Economic Coercion." pp. 623-629.

350 If the NotPetya malware (sent by a State actor) would have been intended to attack the port of Rotterdam it would be a form of economic cyber coercion. See also the deliberation in Jamnejad and Wood, "The Principle of Non-Intervention." pp. 369-372.

351 See also Kilovaty, "The Elephant in the Room: Coercion." pp. 90-91.

352 Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," *Select Committee on Intelligence United States Senate*, (2017). pp. 1-6.

3.4.4. Core elements of interventions

Infringements will constitute an intervention if two conditions are fulfilled: infringements need to be coercive and invasive in the reserved domain of another State.

An intervention is an intrusion in the reserved domain of a State, the area of domestic jurisdiction that is not regulated by international legal obligations. The size of the reserved domain depends on the nature of the international obligations of the State and is therefore inherently relative. A mere infringement in the reserved domain does not qualify as an intervention, whereas an infringement in the *domaine réservé*, executed in a coercive way, is an intervention. An intervention that fails to reach the desired outcome is still unlawful. If there is no justification to intervene, the coercive infringement in the reserved domain is an unlawful intervention.

Coercion is the core element of intervention. Based on literature and the assessment above a conceptual tool can be distilled for which the elements of coercion are a) the deliberate intent, b) to subordinate the State's capacity for deliberate understanding and autonomous decision making, c) with the aim to force the target State to a change of policy on a matter which the State is free to decide. All three elements are required to constitute coercion.[353] Though the principle of non-intervention is a legal obligation of customary international law between States, which undisputedly applies to cyberspace, the characteristics of cyberspace do affect the nature of coercion. Not only are compelling cyber operations likely to breach the prohibition of intervention if targeting the reserved domain, the characteristics of cyberspace are also conducive to manipulative (influence) operations, relying on subconscious techniques to be coercive in nature.[354]

353 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." pp. 268-269.

354 See also Schmitt's deliberation in: Schmitt, "Foreign Cyber Interference in Elections." pp. 747-750.

Section 3.5.: Key findings

"Einer kann sich nicht beweisen:
aber Zweie kann man bereits nicht widerlegen."[355]

In this section the key findings are presented as an answer to the second sub-question of this research: *"Identify how rules and principles of international law, related to sovereignty and (non) intervention apply in cyberspace to States in their conduct with other States or political systems?"*

Though the State's sovereignty is absolute, its autonomy and domestic jurisdiction can be limited by international legal obligations stemming from treaties and customary international law. States cooperate in nearly all domains of society and, therefore, not all infringements are per se unlawful.

A categorisation by infringements is made to assess the criteria of, on the one hand, an intervention below the use of force and, on the other, a breach of sovereignty as a separate infringement away from intervention and the threat or use of force. The thresholds for marking the categories of infringements are coercion and the use of force.

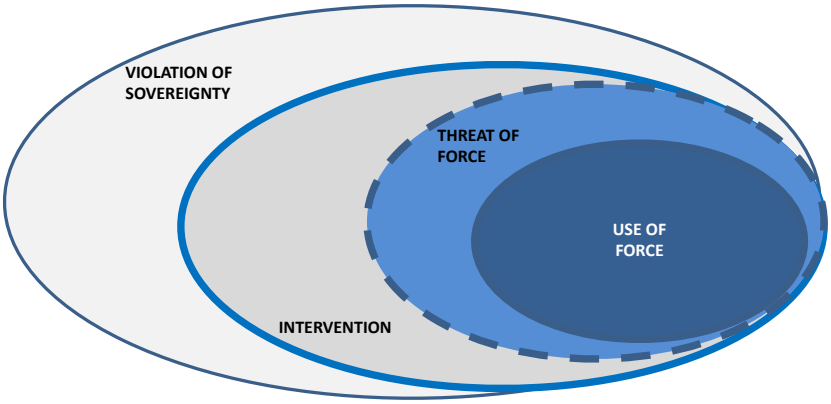

Figure 3 - 5 Degrees of infringement

355 Friedrich Nietzsche, *Die Fröhliche Wissenschaft*, Ungekürzte, Gesammelte Werke in 11 Bänden ; Bd. 6 (München: Goldmann, 1959).

The following assessment provides a reflection on how the rules and principles of sovereignty and non-intervention apply to State conduct in cyberspace.

3.5.1. Violations of sovereignty

Sovereignty in this research is based on territorial integrity and political independence. Though international law applies to cyberspace, the a-territorial virtual dimension of cyberspace (the virtual persona, software and data) does not fit well with the notion of respect for sovereignty, which is traditionally based on the territory of a State. While the physical layer of cyberspace is well within the territory of a sovereign State, the question 'how' the notion of sovereignty applies to cyberspace, especially the virtual dimension, has fuelled a discourse on whether sovereignty is a rule or a principle of international law in cyberspace. This discourse is far from just being semantic, since internationally wrongful acts can only be invoked if a primary rule of law is violated.

Violation of the territorial integrity of the State is an intrusion of the territory as the domain of territorial integrity. The domain includes the persons and materiel on the territory of the State, public and private. Where in the physical world the territory is violated after unwanted access, this act of unwanted penetration is challenging in cyberspace, especially where it concerns remotely executed cyber operations that do not physically cross borders. Still, the impact of remote cyber operations may cause damage to another State. In the *Tallinn Manual 2.0* thresholds on physical and functional damage are introduced, encapsulating violations of territorial integrity.

Criteria for violations of the sovereignty of a State are:

- Violation of territorial integrity
  - Domain – territory (public and private)
  - Nature –
    - Physical damage
    - Functional damage
    - Below functional damage
- Violation of political independence
  - Domain – inherently governmental functions
  - Nature – (no damage required)
    - Interference
    - Usurpation

Figure 3 - 6 Violation of sovereignty

Based in the interpretation of the *Tallinn Manual 2.0*, cyber-related operations violate territorial integrity if physical or functional damage is caused. Cyber operations executed from within the targeted State by foreign agents that have entered the targeted State without proper authorisation can violate the territorial integrity of the targeted State. Remote cyber activities executed from abroad will not violate the territorial integrity of the targeted State since no borders are physically crossed. If these remote cyber operations executed from abroad cause damage, they can violate the territorial integrity of the targeted State. Often, however, remote cyber operations do not have the intent to cause harm in the physical layer of cyberspace, but rather intend to affect the virtual layers in which case the infliction of damage is less obvious. Remote cyber operations targeting the virtual dimension of cyberspace are less likely to affect the territorial integrity of another State.

However, these predicaments do not render the rule of sovereignty inapplicable. While territorial integrity is difficult to align with activities in the virtual dimension of cyberspace, infringement of the political independence of another State is not necessarily dependent on the territoriality and no damage is needed to constitute a breach of political independence in cyberspace. Activities in cyberspace may interfere with or usurp the inherently governmental

functions – the core functions of the State such as the ability to conduct elections - thereby violating the political independence and hence the sovereignty of a State, in a way similar to infringements in the land, sea or air domain.

Based on the notion that political independence can be violated in cyberspace, the conclusion is that sovereignty is a binding rule of customary international law in cyberspace,[356] as it is in the land, sea or air domain. States enjoy sovereignty over cyber infrastructure, persons on their territory and activities in cyberspace.[357] The question related to sovereignty in cyberspace should therefore not be 'if' a rule of international law is violated, but rather 'when' the rule of sovereignty in cyberspace is violated and the infringement is unlawful.[358]

3.5.2. Intervention

An intervention is a non-consensual coercive infringement of the reserved domain of another State. *Domaine réservé* denotes an area of activity that is, as a general matter, left to State by international law. An intervention that fails to reach the desired outcome is still unlawful.

Coercion is the core element of intervention. An intervention is coercive if it deliberately intends to undermine the autonomous decision-making process of another State, and if it aims to change the policy of the other State on a matter which the State is free to decide.

356 See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. pp. 11-13. But also the UN GGE reports, e.g. the United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174.".

357 Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." p. 1647.

358 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." pp. 17-18. Which is in line with Egan's referral to the 'de minimis' activities, and Corn's argument that 'whether and precisely when non-consensual cyber operations below the threshold of a prohibited intervention violate international law is a question that must be resolved through the practice and *opinio juris* of states'. See: Egan, "International Law and Stability in Cyberspace." p. 174; Corn and Taylor, "Sovereignty in the Age of Cyber." pp. 210-211; Michael N. Schmitt, "International Cyber Norms: Reflections on the Path Ahead," *Militair Rechtelijk Tijdschrift*, 2018. p. 17.

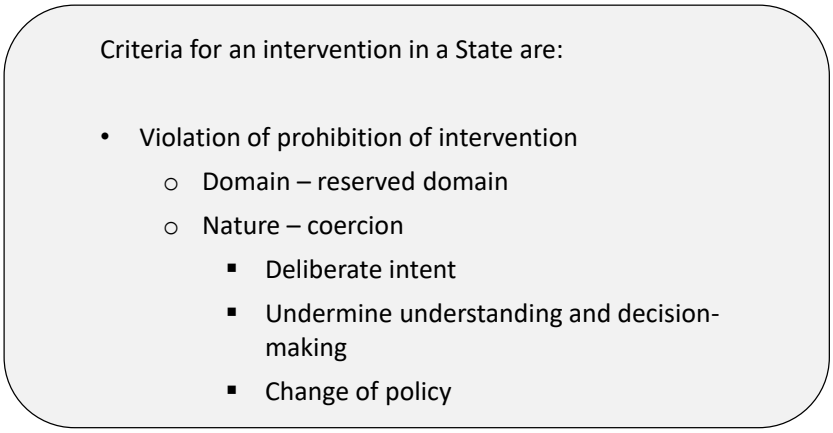

Figure 3 - 7 Intervention

The prohibition of intervention is a legal obligation of customary international law, which undisputedly applies to cyberspace. The characteristics of cyberspace do not change the nature of coercion as such, but they increase the coercive possibilities. Apart from persuasive and compelling cyber operations which are intended to overtly change of the policies (within the reserved domain) of the State, influence operations in cyberspace can also apply subconscious techniques which are often covert. These (often) covert manipulative operations deny the target State the ability of deliberate understanding and autonomous decision-making and can therefore also be coercive in nature.