2025, Vol. 14, Issue 1

Piotr Czepulonis

Cardinal Stefan Wyszyński University in Warsaw

https://doi.org/10.21697/2025.14.1.03

DISINFORMATION ONLINE AND THE PRINCIPLE OF NON-INTERVENTION

Abstract: Disinformation is as old as communication. Yet, its latest reincarnation in the form of so-called fake or misleading news distributed by social media provokes new questions under international law. Due to its qualitative and quantitative characteristics, modern disinformation can have a debilitating impact on election processes, social order, and even national security. Its growing importance from the perspective of international law has been reflected in the adoption of relevant resolutions by the UN General Assembly and the Human Rights Council as well as in initiatives undertaken by states and regional organisations to address the problem of foreign disinformation campaigns. The crucial question for an international lawyer is whether a disinformation campaign violates international law and if so which norms or principles thereof. This article will focus on the principle which is of particular importance in the context of disinformation, namely the principle of non-intervention. While considering the latest developments in the field, the article will try to clarify whether and if so, under what circumstances a disinformation campaign may violate the principle. The affirmative view has been expressed by several states in their national positions on application of international law to cyberspace. The COVID-19 pandemic during which disinformation exacerbated public health crises, clearly played a role in forming at least some of these positions. The text will separately tackle two elements forming the principle of non-intervention: a) interference with a state's internal or external affairs; and b) coercion. It will pay particular attention to the scope of the term "coercion" in the context of information domain. Since coercion may be understood as either taking control over sovereign decisions or "extorting" expected behaviour from another state, the article will tackle both meanings of the term.

Keywords: non-intervention, coercion, disinformation, cyberspace

1. Introduction

Cyberspace has radically changed how information is generated, distributed and consumed. In 2024 users spent on average over 6 hours online per day,[1] of which over 2 hours on social media,[2] which are increasingly used to promote political and social narratives. At the same time, the consumption of so-called traditional media has been steadily decreasing over the last two decades.[3] Undoubtedly, the new information landscape privileges the spread of news online over traditional means.

This creates huge opportunities for actors aiming at influencing public discourse, including in foreign states. In fact, few have been relations as consequential for international relations as between disinformation and the cyberspace. Ever a useful political tool, disinformation campaigns have grown into prominence in recent years thanks to the global reach of the cyberspace. In the past, in order to reach a foreign population, states had to rely on techniques of limited effectiveness such as dropping leaflets or using radio. Nowadays, states have at their disposal cyberspace which allows disinformation campaigns to become faster, more invasive, and widespread. Geographical distances are no longer a barrier for effective information operations and states can directly or indirectly influence foreign infospheres[4] with unprecedented ease.[5]

The watershed year for public awareness about the impact of disinformation was 2016. Then, disinformation campaigns allegedly orchestrated by Russia significantly influenced the US presidential elections[6] and the UK

1 Average daily time spent using the internet by online users worldwide from 3rd quarter 2015 to 3rd quarter 2024, Statista, accessed 30 May 2025, https://www.statista.com/statistics/1380282/daily-time-spent-online-global/.

2 Daily time spent on social networking by internet users worldwide from 2012 to 2024, Statista, accessed 30 May 2025, https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide.

3 For the readership of newspapers in the US see: Newspapers Fact Sheet, Fact Sheets: State of the News Media, accessed 30 May 2025, https://www.pewresearch.org/journalism/fact-sheet/newspapers/.

4 Floridi, *The fourth revolution: how the infosphere is reshaping human reality.*

5 Kahler, Foreign Influence and Democratic Governance, 2024, Council on Foreign Relations, https://www.cfr.org/report/foreign-influence-and-democratic-governance.

6 Press Release, White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity. For a detailed analysis of Russian interference into American presidential elections see:

Brexit referendum.[7] Since that point, we have witnessed numerous information operations, including disinformation and misinformation, related to COVID-19, migration, and armed conflicts. Some of those campaigns resulted in political instability, others have caused death and injury[8].

It has become significantly easier to become an actor manufacturing or spreading disinformation also. Today, it is not only states or their intelligence agencies who can conduct sophisticated information operations abroad. The pool of disinformation creators and peddlers includes politicians, extremist groups, companies, NGOs, and individuals.[9]

The growing use of disinformation online translates into greater effects on political, economic, or social aspects of public life. It may lead to detrimental effects on individuals, groups of people, organisations, or whole states. At the same time, the causal link between disinformation and the harm caused is not always clear.[10]

Due to its global relevance, disinformation has become a subject of interest of international law and states increasingly refer to it in their positions on application of international law to cyberspace. The issue of interstate disinformation may be analysed from different legal perspectives such as international human rights law (especially in the context of the right to freedom of expression and opinion) or the principle of sovereignty. One principle, however, is particularly relevant in the context of interstate disinformation campaign: the principle of non-intervention.

In this article I will analyse how the prohibition on intervention into internal or external affairs of another state applies to the phenomenon of online disinformation. In the second section, I will focus on the meaning of disinformation itself, and I will try to delineate the difference between it and other types of information operations such as misinformation, propaganda and hate speech. In the third section, I will move to the principle of non-intervention. I will dissect two elements that constitute this principle, namely:

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

7 Marshall and Drieschova, "Post-Truth Politics in the UK's Brexit Referendum", 89-106.

8 Caceres et. al., "The impact of misinformation on the COVID-19 pandemic", 262-277.

9 Hamm, "The Few Faces of Disinformation", EU Disnfo Lab, 11 May 2020, https://www.disinfo.eu/publications/the-few-faces-of-disinformation/#:~:text=With%20the%20use%20of%20fake%20identities%2C%20online%20profiles%20and%20websites,of%20undermining%20climate%20protection%20measures.

10 Dias, *Study on International Norms for Foreign Information Manipulation and Interference*, 6.

coercion and *domaine réservé*. Moreover, I will analyse different concepts of coercion, focusing on coercion understood as extortion and coercion understood as control. In the fourth section, I will focus on application of the non-intervention principle in the cyber context. I will examine whether specific traits of cyberspace affect how the principle of non-intervention is understood and applied. In the fifth section, I will refer to specific scenarios where disinformation campaigns can be treated as violations of the non-intervention principle, analysing them through the prism of two elements of the non-intervention principle. I will analyse disinformation campaigns conducted in the context of elections (in the wake thereof and thereafter), aiming at undermining public health policies, causing civil unrest and supporting insurgent groups. In the last section, I will present the summary of the article.

2. What is Disinformation?

Before we move into the legal analysis it is important to clarify what we mean by the term 'disinformation'. In the public discourse 'disinformation' is often used interchangeably with expressions such as 'misinformation', 'fake news', 'information operations' or Foreign Information Manipulation and Interference (FIMI).

According to the High-Level Expert Group on Fake News and Online Disinformation of the European Commission: 'Disinformation (...) includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'.[11] In the 1st EEAS Report on Foreign Information Manipulation and Interference Threats disinformation is defined as

> Verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security.[12]

11 Final report of the High Level Expert Group on Fake News and Online Disinformation, 12 March 2018, accessed 20 May 2025, https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation.

12 1st EEAS Report on Foreign Information Manipulation and Interference Threats, 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf.

In short, disinformation is equivalent to intentional promotion of 'claim(s) that contradicts or distorts common understanding of veritable facts'.[13]

The definitions indicate that disinformation does not need to be based solely on outright lies. It is sufficient that the content is misleading which may be achieved also by presenting facts in a distorting way leading the target audience to false conclusions.[14] By doing so the authors of disinformation campaigns use small truths to build big lies (e.g. 'all immigrants are criminals'). In addition, disinformation may be used to undermine trust in truthful information by labelling them as fake news.[15]

Disinformation can be treated as part of a broader category of information operations which aim at influencing infosphere of another country regardless of whether the information used in these operations are true, misleading, or false.

Disinformation must be differentiated from misinformation. The latter is unintentional, i.e. those who engage in it are not aware that they are distributing a deceitful material.[16] The former is shared with an intent to manipulate the target audience, the latter with a simple intent to inform. Disinformation is also different from malinformation that is 'the intentional dissemination of accurate information, usually obtained by illegal means, such as doxing'.[17]

Disinformation, misinformation, and malinformation are distinct from rumours, unverifiable claims, propaganda or hate speech even though they all fall into the category of so-called information operations and/or FIMI. According to the authors of the Oxford Statement 'information operation[s] and activities encompasses any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience'.[18]

13 Guess and Lyons, "Misinformation, Disinformation and Online Propaganda", 10-33.

14 Baade, "Fake News and International Law".

15 Disinformation and freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, 2021, A/HRC/47/25.

16 Guess, "Misinformation, Disinformation and Online Propaganda", 10-33.

17 Dias, *Study on International Norms for Foreign Information Manipulation and Interference*. See also: Wardle and Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking", 5.

18 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities, 2023, accessed 30 May

Propaganda can be defined as information that may be true but 'is used to disparage opposing viewpoints'[19] or as 'the selective presentation of information, facts or views to emotionally influence and manipulate audiences'.[20] Hate speech, as observed by the UN General Assembly in the resolution entitled Countering disinformation for the promotion and protection of human rights and fundamental freedoms, may overlap in some cases with disinformation.[21] Both phenomena may lead to vilification of vulnerable groups or even to violence against them. Hate speech uses pejorative or discriminatory language with reference to a person based on their identities such as religion, ethnicity, nationality, or race.[22]

The precise boundaries between various kinds of information operations may not always be clear[23] and the same behaviour may sometimes fall in distinct categories. However, it is fair to say that all of them can be treated as cognitive operations since their main goal is to exert influence over what the target audience thinks and, in consequence, how it acts.[24]

3. Non-intervention Principle: Introduction

The principle of non-intervention forbids one to intervene in matters within the domestic jurisdiction of other states. It is linked to the broader principle of sovereignty[25] which it protects, and to the prohibition on the use of force[26]. The principle protects only states.[27] Thus, interventions against non-state

2025, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities.

19 Guess, "Misinformation, Disinformation and Online Propaganda," 10-33.

20 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, 2024, accessed 15 May 2025, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

21 A/RES/76/227.

22 "What is hate speech?" United Nations, accessed 15 May 2025, https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech.

23 The Special on the promotion and protection of the right to freedom of opinion and expression correctly observed that difficulty in defining the concept of disinformation partially 'lies in the impossibility of drawing clear lines between fact and falsehood and between the absence and presence of intent to cause harm'. See: Disinformation and freedom of opinion and expression, 3.

24 Wanyana, "Cognitive Warfare: Does it Constitute Prohibited Force?".

25 Jennings and Watts eds., *Oppenheim's International Law – Vol. 1: Peace*, 428.

26 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para 205.

27 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", 253.

actors are beyond its scope unless their consequences indirectly impact on sovereign functions of a state.

The principle is regulated by both the UN Charter and customary international law. It has been referred to in regional agreements such as the Charter of the Organization of American States,[28] the Charter of Organization of African Unity,[29] and the Charter of ASEAN.[30] It is also reflected in The Final Act of the Conference on Security and Co-operation in Europe.[31] Moreover, it has been dealt with in the ICJ jurisdiction[32] and UNGA resolutions.[33]

The UN Charter in Article 2(7) forbids the UN from intervening into 'matters which are essentially within the domestic jurisdiction of any state'.[34] Even though the article does not regulate the interstate relations its impact on understanding of the non-intervention principle under customary international law has been significant.[35]

There is no provision in the UN Charter that would explicitly prohibit the intervention conducted by a state. Yet, the non-intervention principle among states can be deducted from Articles 2(1) and 2(4) of the Charter and customary international law.[36] Given the subject matter of this article I will focus on the non-intervention principle as applied between states.

Article 2(1) refers to the principle of sovereign equality of states. One of the core elements of this principle is the right of each State to freely choose

28 Article 3.

29 Article III(2).

30 Article 2(2)(e)(f).

31 Principle VI.

32 *The Corfu Channel Case*, Merits, ICJ judgment of 9 April 1949, I.C.J. Rep 1949, paras. 34-35; *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 202; *Armed activities on the territory of the Congo (Democratic Republic of the Congo v. Ruanda)*, Merits, ICJ judgment of 3 February 2006, I.C.J. Rep 2006, paras. 161-163.

33 Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations (GA Res. 2625(XXV)), 1970; Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (A/RES/20/2131).

34 Nothing contained in the present Charter shall authorise the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.

35 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", 253.

36 Nolte, "Article 2(7)", 284; Kułaga, „Działania w cyberprzestrzeni wpływające na wybory w innym państwie a zasada nieinterwencji".

and develop its political, social, economic, and cultural systems.[37] Thus, the principle of sovereign equality must be protected from unlawful foreign interventions that would deprive a State from the right to decide on the matter of its internal affairs. Article 2(4) prohibits the threat and the use of force in interstate relations. The use of force is an example of flagrant violation of the non-intervention principle. As noted by the ICJ in the *Nicaragua case*

> the element of coercion (...) is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[38]

The principle of sovereign equality, the principle of non-intervention and the prohibition on the use of force are all closely linked. The same acts that violate the principle of non-intervention may also violate either of two other principles.[39]

The ICJ observed that the principle of non-intervention is part of customary international law.[40] The expression of customary international law regarding the principle of non-intervention according to the Court can be found in the 1970 Friendly Relations Declaration.[41] In its preamble the Declaration provides that intervening in the affairs of any other State 'violates the spirit and letter of the Charter' and 'leads to the creation of situations which threaten the international peace and security'. The inclusion of international peace and security suggests a broader interest of international community in upholding this principle. The Declaration also indicates that 'any attempt aimed at the partial or total disruption

37 GA Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).

38 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 205.

39 *Armed activities on the territory of the Congo (Democratic Republic of the Congo v. Ruanda)*, Merits, ICJ judgment of 3 February 2006, I.C.J. Rep 2006, para. 164. See also Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 608.

40 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para 202.

41 Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion of 22 July 2010, I.C.J. Rep. 403, para. 80. See also Keller, "Friendly Relations Declaration (1970)".

of the national unity and territorial integrity of a State or country (...) is incompatible with the purposes and principles of the Charter.'

From the operative part of the Declaration the three following paragraphs are of particular importance for our further deliberations:

> No State or group of States has a right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other state. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic, and cultural elements, are in violation of international law.
> No state may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign right and to secure from its advantages of any kind. Also, no State shall organise, 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.
> Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State.

The language used in these paragraphs ('for any reason whatever', 'or any other type of measures', 'advantages of any kind') indicates at the broad scope of the prohibition on intervention.

The principle of non-intervention was extensively covered in the UN General Assembly's Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States. Yet, it cannot be said that the document reflects customary international law since a number of states opposed it.[42]

The principle was also subject of work by the International Law Commission which concluded that 'Every State has the right to independence and hence to exercise freely, without dictation by any other State, all its legal powers, including the choice of its own form of government'.[43]

42 Kunig, "Prohibition of Intervention".

43 Article 1, International Law Commission, Draft Declaration on Rights and Duties of States, reprinted in General Assembly resolution 375(IV), "Draft Declaration on Rights and Duties of States", adopted 6 December 1949.

3.1. Two Elements of the Principle of Non-intervention

As indicated in the Article 2(7) of the UN Charter the principle of non-intervention consists of two basic elements: intervention, and matters which are essentially within the domestic jurisdiction of any state. That is, the means and the object against which the means can be used.[44] Both elements need to be analysed separately.

The notion of intervention is not defined in international law and has been a subject of many discussions, with significant differences among states on types of behaviours that would fall into this category, especially regarding those involving economic instruments.[45] Looking at the state practice we can point at two basic ways of understanding the term.

The broad understanding encompasses critical views on actions or omissions of states as well as recommendations to undertake a given course of action. This understanding is sometimes proposed by states to counter any unacceptable – in their view – criticism directed at them. From this perspective, intervention can include pointing at the human rights violations or recommending internal reforms, including amendments of national law. Illustrative in this regard is the reaction of Saudi Arabia to Canada's post on Twitter, in which Canada requested the Saudi Arabia authorities to release blogger Raif Badawi and his sister Samara Badawi from prison. The Saudi Arabia treated the publication of the post as unacceptable interference into its internal affairs and responded by recalling the Canadian ambassador as well as by suspending trade agreements, flights and students exchange programs between the two countries.[46] Another example is China's response to the assessment (*de facto* report) prepared by the Office of the United Nations High Commissioner for Human Rights regarding the human rights situation in Xinjiang. The report published on 31 August 2022 included numerous allegations of human rights violations committed by the Chinese government.[47] In the note verbale China described the report as interfering in its internal affairs even though it stopped short from saying that it violated the principle

44 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 609.

45 Helal, "On Coercion in International Law".

46 Samuel, *The Two Words That Made Saudi Arabia Furious at Canada*.

47 Office of the United Nations High Commissioner for Human Rights, Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, 2022.

of non-intervention.[48] At the same time, one needs to be aware that it is not always clear whether aggressive responses to perceived interventions are rooted in international law analysis or rather in purely political calculations based on projecting sovereigntist posture.[49] It is sometimes argued that the broader understanding of intervention (i.e. encompassing recommendations, criticism etc.) is used in the Article 2(7) of the Charter[50].

The approach presented above is problematic principally because if conflates intervention with mere interference while the exact goal of the principle of non-intervention is to differ between these two types of behaviour. As noted by Czechia in its statement on the application of international law to cyberspace, prohibited intervention must be differentiated from 'mere influencing, criticism or persuasion'.[51] Austria distinguishes between disinformation campaigns violating non-intervention principle and 'lawful public relations activities of state representatives including e.g. by openly criticising the human rights situation in another state on social media accounts or websites'.[52] Canada has endorsed a similar position[53] as well as Denmark,[54] Norway,[55] Sweden,[56] and

48 Note verbale of the Permanent Mission of the People's Republic of China to the United Nations Office at Geneva and Other International Organisations in Switzerland, 31 August 2022, https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/ANNEX_A.pdf.

49 Kułaga, „Działania w cyberprzestrzeni wpływające na wybory w innym państwie a zasada nieinterwencji", 161.

50 Nolte, "Article 2(7)", 280, 285.

51 Czech Republic Position paper on the application of international law in cyberspace, February 2024, accessed 13.07.2025, https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf, [hereinafter Position of Czech Republic].

52 Position Paper of the Republic of Austria: Cyber Activities and International Law, April 2024, accessed 13.07.2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf, [hereinafter Position of Austria].

53 International Law applicable in cyberspace, April 2022, accessed 13.07.2025, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, [hereinafter Position of Canada].

54 Kjelgaard, "Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction", 446-455.

55 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, 68-69, [hereinafter Position of Norway].

56 Engdahl, "Sweden's Position Paper on the Application of International Law in Cyberspace: Introduction", 489-497.

Switzerland.[57] Also, the authors of the Tallinn Manual distinguished between coercion and 'persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like' stressing the difference between, on the one hand, influencing the target State and, on the other, compelling it to act or not to act in a demanded fashion.[58]

In fact, criticising and influencing other states is part of interacting in international relations and without its foreign policy would not be possible.[59] Moreover, as we will see a decision whether to violate or not obligations deriving from international law (e.g. international human rights law) does not belong to 'matters which are essentially within the domestic jurisdiction of any state' and it is not protected from criticism and, as a matter of fact, from other means aiming at ending the violations. Hence, in the abovementioned cases neither the means applied (criticism, recommendations) nor the object of these means (violations of international law committed by another state) are covered by the principle of non-intervention.

This leaves us with the narrower or traditional understanding of the term intervention. Under this approach intervention to breach international law must involve coercion and it must aim at impacting on the areas in which another State should be allowed to decide freely.[60] Beyond the scope of the prohibition are 'discussion, study, enquiry and recommendation'[61] and activities enumerated already above by Czechia, Austria, and others.

This approach is broadly supported by states who refer to coercion in their official positions regarding the principle of non-intervention.[62] It is also

57 Switzerland's position paper on the application of international law in cyberspace, May 2021, accessed 13.07.2025, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf, [hereinafter Position of Switzerland].

58 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 317.

59 Kranz, *Pojęcie suwerenności we współczesnym prawie międzynarodowym*, 142.

60 Nolte, "Article 2(7)", 285

61 Lauterpacht, "The International Protection of Human Rights", 19.

62 Positions of Canada and Switzerland as well as African Union Peace and Security Council, the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 1.2024, accessed 10.07.2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/CAP_Communiques_FULL_0e34eb5799.pdf, [hereinafter Common African Position]; Council of the European Union, Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace, 11.2024, accessed 10.07.2025, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf, [hereinafter Position of the European Union]; Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and

confirmed by the ICJ jurisdiction. In the Nicaragua case, the Court stated that: 'Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones'.[63]

3.1.1. Coercion

The term coercion is used in the treaty law[64] and the law on state responsibility.[65] The Vienna Convention on the Law of the Treaties (VCLT) refers to coercion used both against a state and its representative. Article 52 thereof provides a narrow understanding of coercion by stipulating that '(a) treaty is void if its conclusion has been procured by the threat or use of force in violation of the principles of international law embodied in the Charter of the United Nations'. Article 51 of the VCLT in turn provides that coercion of a State's representative may take place through acts or threats, which is a significantly broader concept of coercion. Article 18(2) of Draft Articles on Responsibility of States for Internationally Wrongful Acts states as follows

> A State which coerces another State to commit an act is internationally responsible for that act if: (a) the act would, but for the coercion, be

communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, 18-19, [hereinafter Position of Brazil]; Costa Rica's Position on the Application of International Law in Cyberspace, 7.2023, accessed 10.07.2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf, [hereinafter Position of Costa Rica]; Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 5.2021, accessed 10.07.2025, https://www.mofa.go.jp/files/100200935.pdf, [hereinafter Position of Japan]; The Application of International Law to State Activity in Cyberspace, 12.2020, accessed 10.07.2025, https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf, [hereinafter Position of New Zealand]; Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 83, [hereinafter Position of Singapore]; Attorney General, Suella Braverman, International Law in Future Frontiers, 5.2022, accessed 10.07.2025, https://www.gov.uk/government/speeches/international-law-in-future-frontiers, [hereinafter Position of the United Kingdom].

63 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 205.

64 Vienna Convention on the Law of Treaties.

65 Article 18(2), ILC Articles on State Responsibility.

> an internationally wrongful act of the coerced State; and (b) the coercing State does so with knowledge of the circumstances of the act.

The use of force is an obvious example of intervention because it is undoubtedly coercive. The ICJ observed that:

> The presence of the element of coercion, which forms the very essence of prohibited intervention is evident in the case of an intervention which includes a use of force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[66]

This does not mean, however, that actions below the threshold of force are not prohibited under this principle. This was also indicated by the ICJ which referred to interventions 'with or without armed forces'.[67] The term coercion is not defined in international law nor has it been defined by the Court and the exact contours of the principle below the threshold of the use of force have been a subject of intensive debate among states and scholars, including whether it should encompass activities in political and economic realms.[68]

We can look at the activities aimed at influencing another state's behaviour as belonging to a spectrum where the use of force is an extreme example of coercion and activities belonging, for example, to public diplomacy or mere persuasion are evidently not coercive. The key difficulty is to draw a line between those behaviours that are coercive and those that are not when they do not belong to either of the two extremes. It should not come as a surprise that many States believe that identifying coercion should be undertaken on a case-by-case basis.[69]

Some authors suggest that the amount of pressure applied should be a decisive criterion. Jamnejad and Wood argue for instance that 'if the pressure is such that it could be reasonably resisted, the sovereign will

66 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 205.

67 Ibid., para. 206.

68 Lowe, *International Law*; Jamnejad and Wood, *The Principle of Non-intervention*.

69 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 77, [hereinafter Position of Romania] as well as positions of Austria, Canada, Czech Republic, Sweden, and Switzerland.

of the target state has not been subordinated' and (o)nly acts of a certain magnitude are likely to qualify as coercive'.[70] This would mean that there is a certain threshold of pressure to be met that leaves the target state with no other reasonable option than to succumb to the will of the intervening state. This threshold would be by no means set in stone since the ability to resist the same actions would widely differ between different states depending on their potential, interdependence, specific vulnerabilities etc. Let us imagine that State A change the course of action of State B threatening the latter with a suspension of bilateral trade. If trade with State A forms 30% of all State's B trade it will be more difficult to resist such pressure than if it forms only 1% of its overall trade. What follows is that the threshold of coercion needs to be established on a case-by-case basis.

Wheatley reconstructs the notion of coercion by building on research conducted in other fields of humanities such as philosophy or ethics that deal with the problem of coercion applied against individuals.[71] Similarly, as above, coercion is perceived as actions leaving the target with no tolerable alternative option or no other option whatsoever. The actions analysed in the context of coercion may include several types of behaviour such as compulsion, coercion or manipulation. Compulsion will involve physically forcing someone to do something by e.g. grabbing his hand to sign a contract; in this scenario it can be said that the object of coercion was indeed deprived of his or her freedom to act. Coercion as a threat (do it or else) will impact on someone decision process by presenting the object with additional costs. The gravity of the threat (do it or I will kill you vs. do it or I will not go out with you) clearly impacts on whether the pressure is resistible. Coercive manipulation distorts the target's process of taking decisions.[72] It may be conducted either by providing the target with false information or by changing his perception of facts. Other kinds of manipulation (non-coercive), enticements or simple requests evidently do not fall into the category of coercion.

Analysing coercion at the interpersonal level may provide us with some useful insights yet one needs to be careful when transferring these findings

70 Jamnejad and Wood, *The Principle of Non-intervention*, 348.

71 Wheatley, "Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion"".

72 See also: Roscini, *The Principle of Non-Intervention in the Information Age: Cyber Operations as a New Means of Coercion in the Domestic Affairs of States'*, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, 399.

into the field of international law. After all, the non-intervention principle protects States and not individuals. The dynamics of exerting pressure over a political entity and individuals are no doubt different even though at the end of the day individuals act on behalf of states. It is also different how they respond to pressure and what can be perceived as tolerable alternative options.

Milanović convincingly argues that there are in fact two models of coercion: the extortion model and control model.[73] In the first, one State makes a demand regarding affairs the target State should be allowed to decide freely which is accompanied by a threat of negative consequences in case the demand is not met. If the target State resists the extortion attempt, the threatening State may make good on its threat and inflict costs on it. The goal of the threat and/or threatened actions it is to change the victim State's calculus by threatening to impose or in fact imposing such high costs that bearing them would not be reasonable. For classifying the behaviour of the threatening State as a prohibited intervention, it does not matter whether the threatened behaviour was eventually carried out or whether it was successful in changing the target State's position. What is important in this model is that the target State is left with a freedom of choice and it may well decide to bear the high costs imposed by another State even if such a decision seems unreasonable. Since the whole concept of coercion as extortion hinges on the decision of the target State whether to succumb or not to the applied pressure, it must be aware that coercion is being used against it and that it is subject of a demand formulated by another state.[74] The extorting State in turn *must* intend to change the behaviour of the target State.

In the control model, coercion means depriving the target State of control over choices belonging to its *domaine reserve*.[75] This can be

73 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 626-647. Roscini also referring to two models of coercion uses the following terms: dictatorial and forcible coercion. Roscini, *The Principle of Non-Intervention in the Information Age: Cyber Operations as a New Means of Coercion in the Domestic Affairs of States', International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, 382-385.

74 The importance of will of the victim State was stressed in the definition of coercion proposed in the Tallinn Manual which reads as follows: 'coercion is not limited to physical force, but rather refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way', Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 317.

75 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 640-7.

undertaken either by taking direct control over a matter belonging to another State's reserved domain by e.g. changing the voting result, or by depriving that State of control without taking it over by e.g. causing societal upheaval. In this scenario, the calculus of the victim State does not need to be changed. The target State does not need to take any decision; it does not even need to be aware of the activities undertaken by another State. The decisions of the intervening State are being imposed directly on the victim State. At the same time, the intervening State does not need to have any specific demand. This model resembles to some extent coercion as compulsion and as manipulation that were mentioned previously in the interpersonal context.

Regardless of the model adopted there is a certain threshold of intensity that must be met to classify a given behaviour as coercion. This is a position adopted by Canada, Czechia, Israel, Poland, and Switzerland.[76] Germany and the UK in their official statements referred to the scale and effects standard when assessing which interferences are coercive.[77] The activities forming coercion must be intentional too[78] which was raised in the statements of Czechia,[79] New Zealand,[80] and Norway.[81]

The actions forming coercion may be internationally wrongful acts when the interviewing State either threatens to violate the victim State's rights in the coercion model or simply does it in the control model. Yet, in

76 Schöndorf, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations; The Republic of Poland's position on the application of international law in cyberspace, Ministry of Foreign Affairs of Poland, 12.2022, 4, accessed 10.07.2025, https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131, [hereinafter Position of Poland]; as well as positions of Canada, Czech Republic, and Switzerland.

77 On the Application of International Law in Cyberspace, 3.2021, accessed 10.07.2025, https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf, [hereinafter Position of Germany] as well as position of the United Kingdom.

78 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, paras. 19 and 27.

79 'There is a certain similarity between the terms internal and external affairs and inherently governmental affairs, which is one of the defining elements of violation of sovereignty. The difference between actions that violate sovereignty and actions that violate the prohibition of intervention is that the latter is coercive, i.e., intentionally aims to influence the State's free will and choice'.

80 'While the coercive intention of the state actor is a critical element of the rule, intention may in some circumstances be inferred from the effects of cyber activity'.

81 'Thus, carrying out cyber operations with the intent of altering election results in another State, for example by manipulating election systems or unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak'), would be in violation of the prohibition of intervention'.

some circumstances acts that otherwise would be lawful can be also treated as coercive. If these acts are coupled with the intent to limit the victim State's freedom in its *domaine réservé*, they may violate the principle of non-intervention. It is precisely the intent that changes legal qualification of the act.[82]

The Declaration on Friendly Relations states that interventions into internal and external affairs of another State is prohibited regardless of the particular motive ('for any reason whatsoever').[83] It is nevertheless worth looking at potential goals behind coercive behaviours because they may impact on what type of coercion is chosen by the intervening State. In the extortion model coercion typically will aim at changing the policy of the target State by forcing it to adopt or forego specific policies within its *domaine réservé*. Hence, the demand should be concrete enough to make it possible for the target State to accept or reject it. It is worth stressing that the pressure does not need to be applied in the area that the intervening State seeks to impact upon. In the control model the goal will be to undermine the target State's 'ability to exercise its state powers in some way'.[84] The intervening State's goal may be to either debilitate the target State or to undermine its government. In the latter case, the general direction of the country or its political system are the real purposes, and the government of the target State cannot satisfy the intervening State's demands unless it decides to give away the power to political forces favoured by the latter.[85] Actions of the intervening State may involve a plethora of activities ranging from 'supporting and assisting armed bands whose purpose is to overthrow the government',[86] targeting the critical infrastructure or undermining the trust of the population regarding the ruling class or political institutions. Many actions conducted by Russia against Ukraine since at least the so-called

82 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 634.

83 Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations (GA Res. 2625(XXV)), 1970.

84 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 31.

85 Of course, the intervening State may pursue more than one goal simultaneously looking for both specific concessions and weakening of the target State.

86 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 241.

Orange Revolution in 2004 would fall into the category of coercion in this sense.[87]

It is generally accepted that intervention, to be illegal does not need to be successful,[88] i.e. it does not need to change the target State behaviour in the desired direction or effectively deprive it of control over matters belonging to its *domaine réservé*. The bare intention to change the behaviour of a state accompanied by coercive actions in areas belonging to its reserved domain is sufficient. This is why some authors prefer to talk about coercive behaviour rather than coercion.[89]

Act that otherwise could violate the principle of non-intervention may not be wrongful if they are conducted as retorsions or countermeasures in response to hostile or illegal behaviours – yet only if these responses are within the limits allowed by international law.[90]

It is worth noting that intervention may be direct, when conducted by a State, or indirect, when committed by non-states actors acting under instructions or control of a State.[91]

3.1.2. Domaine Réservé

The second component of the principle of non-intervention are 'matters which are essentially within the domestic jurisdiction of any state' or the so-called *domaine réservé*. Coercive interference only into this protected area of competences can violate the prohibition on intervention.

Historically, the concept of *domaine réservé* was understood as matters that are not regulated by international law. The Permanent Court of International Justice in the *Nationality Decrees* advisory opinion stated that matters belonging to *domaine réservé* are 'not, in principle, regulated

87 Buchan and Tsagourias, "The Crisis in Crimea and the Principle of Non-Intervention", 165-193.

88 Common African Position, Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 323; Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 3, Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 646.

89 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 34.

90 Kranz, *Pojęcie suwerenności we współczesnym prawie międzynarodowym*, 142.

91 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 206.

by international law'. [92] This meant that only those issues that international law did not speak about were protected by the principle of non-intervention. Nowadays *domaine réservé* is understood as 'matters which are *essentially* within the domestic jurisdiction'.[93]

The catalogue of *domaine réservé* is not permanent and it varies between states. The developments in conventional and customary international law impact on matters that are essentially within domestic jurisdiction.[94] The more international obligations a state has accepted, the narrower is its *domaine reserve*.[95] It has been noted that globalisation and integrative tendencies in recent decades have significantly limited the matters belonging to the domestic jurisdiction of states.[96] In this regard the development of international human rights law and its impact on reducing States' freedom of action toward individuals falling into their jurisdiction has been of particular importance.[97] Yet, the opposite process of expanding one's *domaine réservé* by limiting one's international obligations (e.g. by withdrawing from international agreements) is also possible. It is worth noting that obligations deriving from treaties are owed only to other parties, hence matters regulated in a treaty may still belong to *domaine réservé vis-à-vis* non-parties.[98] Moreover, even if a matter is regulated by international law, states may still be left with a certain amount of freedom to act and to choose between different lawful options regarding that manner.[99] There is no reason to assume that this kind of freedom should not be protected from foreign interventions.

Domaine réservé is something that a state can decide upon freely because its course of action is not predetermined by its obligations under international law. Yet, the notion can also be defined in a positive way. The Declaration on Friendly Relations clearly says that any coercion against political independence or territorial integrity is not allowed under

92 *Nationality Decrees Issued in Tunis and Morocco*, Advisory Opinion, 1923 P.C.I.J. Rep Ser. B No. 4, at 22- (7 Feb.).

93 UN Charter Article 2(7).

94 Ziegler, "Domaine Réservé", para. 5.

95 Article 15(8) of the Covenant of the League of Nations referred to 'a matter which by international law is solely within the domestic jurisdiction'.

96 Mik, *Fenomenologia regionalnej integracji państw. Studium prawa międzynarodowego, t. 2: Regionalne organizacje integracyjne z perspektywy analitycznej prawa międzynarodowego*, 314-315.

97 Ziegler, "Domaine Réservé", para. 5.

98 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 316.

99 Mik, *Fenomenologia regionalnej integracji państw. Studium prawa międzynarodowego, t. 2: Regionalne organizacje integracyjne z perspektywy analitycznej prawa międzynarodowego*.

international law. Moreover, the Declaration provides that 'Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another state'.[100] *Domaine réservé* also includes the conduct of foreign policy.[101]

Those areas that do not belong to *domaine* réservé are not protected by the non-intervention principle. For instance, if a state owes an obligation to another state deriving from a treaty to which both are parties the latter state can resolve to coercive measures in case of a breach of this obligation because the breaching state cannot decide freely on this matter *vis-à-vis* this State. Depending on the circumstances, a reaction to a breach of international obligations may take the form of retorsions or countermeasures.[102]

4. Non-intervention Principle in the Cyber Context

It is widely recognised that the principle of non-intervention applies to actions in cyberspace. This is a position expressed by a number of states individually,[103] the European Union,[104] the African Union,[105] and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[106] This position has also been widely adopted by academia, including by the authors of the Tallinn Manual.[107]

Some authors argue that the principle of non-intervention should be understood differently in the cyber context because the requirement

100 A/RES/25/2625.

101 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, para. 205.

102 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 317.

103 See for example: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 139-140, [hereinafter Position of the United States], as well as positions of Australia, Brazil, Canada, Israel, Germany, Norway, New Zealand, Singapore, Switzerland, Sweden, and the United Kingdom.

104 Position of the European Union.

105 Common African Position.

106 UN Doc. A/68/98 and UN Doc. A/70/174.

107 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 312. See also: Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", 211, 221; Roscini, *The Principle of Non-Intervention in the Information Age: Cyber Operations as a New Means of Coercion in the Domestic Affairs of States', International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, 377.

of coercion is generally inadequate for activities in cyberspace.[108] In this view, interferences in cyberspace will virtually never be coercive. This in turn requires the reformulation of the principle of non-intervention in such a way that it would also encompass activities of a non-coercive nature such as 'manipulation, deception, disruption, and disinformation'.[109] To others, the perceived difficulty of reaching the threshold of intervention in cyberspace makes the sovereignty principle more attractive as a legal basis on which one should analyse malicious cyber operations.[110]

The problems with applying the principle of non-intervention to malicious cyber operations derive from a restrictive understanding of the term coercion. Coercion can and has been, as we saw in the previous section, interpreted in a broader or flexible way. It can encompass demands accompanied by threats as well as depriving another state of control over matters that it should decide on freely. Both outcomes can clearly be achieved by cyber means. Thus, there is no need to resign from this element when analysing states' behaviour from the principle of non-intervention perspective. A broader interpretation of coercion has been embraced in the cyber context by a number of states including Austria, Costa Rica, Germany, Iran, New Zealand, and Poland[111] as well as scholars such as Gill,[112] Moynihan,[113] Milanović,[114] and Watts.[115]

Also, the narrow interpretation of "coercion" is incompatible with the meaning of the term used in the Declaration on Friendly Relations which provides that:

> No state may use or encourage the use of economic, political or *any other type of measures* to coerce another State in order to obtain from it the subordination

108 Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", 641-43; Kilovaty, "The Elephant in the Room: Coercion", 89-90.

109 Ibid.

110 Schmitt and Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?".

111 Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, 08, 2020, accessed 10.07.2025, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Iran_(2020), [hereinafter Position of Iran] as well as positions of Austria, Costa Rica, Germany, New Zealand, and Poland.

112 Gill, "Non-Intervention in the Cyber Context", 222.

113 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 32.

114 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 605.

115 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", 256.

> of the exercise of its sovereign right and to secure from its advantages of any kind.[116]

Any other type of measures can include both cyber operation and information operations including disinformation.

5. Non-intervention Principle in Context of Disinformation Campaigns

The growing number of states have referred to disinformation in their statements on the application of international law to cyberspace.

According to Austria '(l)arge-scale cyber activities, including disinformation campaigns, conducted by or attributable to a state may also constitute, if undertaken to compel another state to involuntarily change its behaviour, a violation of the prohibition on intervention'.[117] A disinformation campaign that could violate the non-intervention principle is exemplified by a case where State A spreads disinformation about the corruption of State B's government. In result the government of State B resigns.

To Costa Rica '(c)oercion may occur when a State (...) engages in or supports subversive or hostile propaganda or the dissemination of false news that interfere in the internal or external affairs of another State'.[118] Moreover, it refers to electoral disinformation campaigns aimed at distorting the results, disinformation affecting a public health, war-mongering and posts that 'disrupt or subvert the internal order of another State'.[119]

Germany considers that disinformation inciting 'violent political upheaval, riots and/or civil strife in a foreign country' that undermines electoral process 'may be comparable in scale and effect to the support of insurgents and may hence be akin to coercion in the above-mentioned sense'.[120] Moreover, it notes the following

> cyber activities targeting elections may be comparable in scale and effect to coercion if they aim at and result in a substantive disturbance or even

116 Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations (GA Res. 2625(XXV)), 1970.
117 Position of Austria.
118 Position of Costa Rica.
119 Ibid.
120 Position of Germany.

> permanent change of the political system of the targeted State, i.e. by significantly eroding public trust in a State's political organs and processes, by seriously impeding important State organs in the fulfilment of their functions or by dissuading significant groups of citizens from voting, thereby undermining the meaningfulness of an election[121].

At the same time Germany observes that

> (e)ven harsher forms of communication such as pointed commentary and sharp criticism as well as (persistent) attempts to obtain, through discussion, a certain reaction or the performance of a certain measure from another State do not as such qualify as coercion.[122]

Iran as violations of the non-intervention principle classifies engineering the public opinions on the eve of the elections as well as sending mass messages in a widespread manner to the voters to affect the result of the election. It highlights that '(e)very state enjoys the inherent right to the full development of information system and mass media and their employment, without intervention, to advance their own political, social, economic, and cultural interests and aspirations'.[123]

New Zealand believes that the prohibition of non-intervention may be violated by 'a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic'.[124]

According to Poland, 'a wide-scale and targeted disinformation campaign may also contravene the principle of non-intervention, in particular when it results in civil unrest that requires specific responses on the part of the state'.[125]

Other states, such as Canada, Czechia, Denmark, Norway, and Sweden,[126] without specifically mentioning disinformation enumerated activities that would not violate non-intervention principle. This included public diplomacy, criticism, influencing, persuasion, and propaganda. Notably, none of them included disinformation into this category of non-coercive activities.

121 Ibid.
122 Ibid.
123 Position of Iran.
124 Position of New Zealand.
125 Position of Poland.
126 Positions of Canada, Czech Republic, Denmark, Norway, and Sweden.

The African Union referred to a broader concept of instruments of information which if used 'by a State for the purposes of intervening in the internal or external affairs of a foreign State'[127] would violate the prohibition on intervention. It is sensible to assume that instruments of information include disinformation campaigns.

These positions will help us identify areas of *domaine réservé* which can be affected by disinformation campaigns and then to apply the concept of coercion in each of them.

5.1. Disinformation and *Domaine R*éservé

The analysis of states' views indicates certain areas belonging to *domaine réservé* that can be potentially affected by disinformation to such an extent that the prohibition on intervention may be violated. These include electoral processes, public health, as well as public safety and order. I will discuss these cases below.

The application of the non-intervention principle in the context of democratic elections has been one of the most relevant topics in the context of cyberspace and there has been quite some literature on the impact of cyber influence operations, including disinformation campaigns, on elections.[128] The issue of electoral interferences has been raised by states too. Costa Rica believes that the principle of non-intervention may be violated by 'electoral disinformation campaigns seeking to mislead the electorate about the vote itself, candidates, electoral polls or results'.[129] Germany refers to the non-intervention principle in the context of online disinformation leading to 'violent political upheaval, riots and/or civil strife in a foreign country' which significantly impede ' the orderly conduct of an election and the casting of ballots'.[130] Iran as violations of the non-intervention principle classifies 'engineering the public opinions on the eve of the elections' as well as 'sending mass messages in a widespread manner to the voters to affect the result of the election'.[131]

127 Common African Position.

128 See for example: Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law"; Wheatley, "Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion""; Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?".

129 Position of Costa Rica.

130 Position of Germany.

131 Position of Iran.

The focus on electoral interference is understandable. Influencing voters' preferences during an electoral campaign may change the political course of the targeted country for years to come. Undermining the public opinion's trust in politicians and the political system can destabilise and debilitate the target State. The negative impact of disinformation on the democratic process was recognised by the Human Rights Council in Resolution 49/21 which described disinformation as a 'threat to democracy that can suppress political engagement, engender or deepen distrust towards democratic institutions and processes, and hinder the realisation of informed participation in political and public affairs'.[132] The Council observed that this phenomenon 'may be used by States and State-sponsored actors as part of hybrid influence operations that exploit and undermine the freedom of societies and can accompany serious violations of international law'.[133] In Resolution 55/10, the Council urged States and other relevant stakeholders to recognise the risk 'that disinformation could introduce to electoral and other democratic processes'.[134]

In principle, it seems uncontroversial that the freedom to conduct elections of representatives belong to *domaine réservé* and as such it should be protected from coercive interference.[135] To target this freedom is to target the choice of political system which is the sovereign right of every state.

Another area belonging to *domaine réservé* which is prone to be negatively affected by disinformation is public health. Both Costa Rica and New Zealand referred to disinformation affecting public health in their national positions on the application of international law to cyberspace.[136] The damaging impact of disinformation in the public health sphere was particularly evident during the COVID-19 pandemic.[137] The spread of lies or misleading information about vaccines[138] which turned large parts of the populations sceptical about this form of protection against the virus

132 PP 9, A/HRC/RES/49/21.

133 PP 20, A/HRC/RES/49/21.

134 OP 8, A/HRC/RES/55/10.

135 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace".

136 Positions of Costa Rica and New Zealand.

137 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities, accessed 25.05.2025, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/.

138 Skafle et. al., "Misinformation About COVID-19 Vaccines on Social Media: Rapid Review".

was no less of a challenge to states' responses to the pandemic than, for example, cyberattacks against medical facilities or vaccine distribution systems.

Disinformation campaigns may also lead to civil unrest, political upheaval etc. and undermine public safety and/or order of the target State. Germany,[139] Poland, and Costa Rica[140] touched upon disinformation causing political and civil disorder in their national positions. Poland for example noted that 'a wide-scale and targeted disinformation campaign may also contravene the principle of non-intervention, in particular when it results in civil unrest that requires specific responses on the part of the state'.[141]

The political or social turmoil can be achieved by spreading false and misleading information, hate speech and propaganda. Goals of authors of these kinds of operations may be to increase political polarisation or to stoke religious, ethnical, or racial tensions. In extreme cases, disinformation may lead to violence, sometimes directed against the government. Notably the Human Rights Council in Resolution 55/10 observed that: 'disinformation campaigns can be used to vilify individuals and groups, to exacerbate social divisions, to sow discord, to polarise societies, to spread hatred' while 'expressing particular concern at instances of incitement to crimes against humanity and other violations or abuses of human rights'.[142] In Resolution 49/21 the Human Rights Council stressed that disinformation can be used to spread hate speech and to exacerbate social division.[143]

5.2. Disinformation and Coercion

In the previous subsection, I argued that electoral processes, public health, as well as public safety and order are particularly vulnerable to disinformation. The question is whether and if when disinformation campaigns interfering into these areas can be treated as coercive either under coercion-as-extortion or coercion-as-control model.

In the context of elections, the following actions are sometimes raised as examples of violations of the principle of non-intervention: changing the result of elections through cyber means; blocking voters' access to online

139 Position of Germany.
140 Position of Costa Rica.
141 Position of Poland.
142 A/HRC/RES/55/10.
143 A/HRC/RES/49/21.

voting platforms; or disabling machinery necessary to count the votes.[144] All the above-mentioned cases include an element of coercion-as-control since a foreign state takes over or tries to take over control of the electoral process. Disinformation, however, works in more subtle and indirect ways as was already discussed in the previous sections. Its impact on the outcome of elections is indirect. It may influence the views of the voters, yet they remain those who ultimately decide on whom to cast their ballots even if their freedom of will was somehow restricted.[145] In addition, it is extremely difficult to know to what extent voters' views are the result of influence operations, including disinformation. Similarly, it is difficult to determine to what extent disinformation campaigns were decisive in the outcome of elections. We should not forget that voters may also be influenced by opinions of experts which are neither true nor false but may be misleading anyway.[146] Yet, the abovementioned doubts do not mean that disinformation campaigns cannot be qualified as prohibited intervention.

We can consider two basic scenarios of foreign intervention into electoral processes which differ in their ultimate goals. In the first, the foreign power has a specific candidate or political party it supports because it believes that a victory of this candidate or party would be beneficial for its interests (e.g. the Party of Regions in Ukraine supported by Russia in the 2010s). Here disinformation aims at changing the political chances of candidates by weakening the frontrunner and/or strengthening the underdog.[147] In the second scenario, the foreign power's goal is to disrupt the election process to undermine the trust of the population in the political system as a whole and, as a result to weaken the target State. Here disinformation may be used to stoke polarisation and present all main political forces as corrupt or untrustworthy. The means used may range from false or misleading information, trolling, deep fakes attributing certain statements to political actors,[148] overwhelming the public opinion with one narrative and leaving voters with limited meaningful alternative, etc.[149]

144 See e.g.: positions of Australia, Canada, and Germany.

145 Yaffe, "Indoctrination, Coercion, and Freedom of Will", 335, 342.

146 Similar doubts apply to disinformation used in different areas of *domaine réservé* also.

147 Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", 51.

148 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 129.

149 Wheatley, "Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion"", 24.

In both scenarios disinformation clearly aims at manipulating voters, and as we saw before manipulation can be a form of coercion. Individuals are not protected by the non-intervention principle; however, voters constitute the electoral base that through the elections conduct a sovereign function of a state, which is to elect its representatives. By doing so the population exercises its right to self-determination.[150] If the impact of the disinformation campaign reaches a certain threshold[151] it may be argued that the decision process of the electing population was undermined and its right to elect its representatives challenged.

The difference between the two scenarios is that only in the first the foreign power formulates, even if implicitly, a demand, which is elect my candidate. Yet, the demand is not communicated to the target audience so it cannot be aware thereof. In addition, there is no threat that would accompany this implicit demand. In the second scenario there is no demand altogether. Therefore, coercion-as-extortion model is not applicable to either of the two scenarios.

The control model seems to be more fitting to the problem of using disinformation in electoral processes. If a disinformation campaign distorts the electoral process by changing voters' political decisions to the extent that it significantly influences the election result, the electing population loses its control over the political path and by extension over the political system of the state.

Even though the control model seems to be more appropriate, hypothetically, we can imagine the application of the extortion model in electoral scenario also. This could take place if a foreign power used disinformation campaign not as a means of taking control over the decision process of the voting population but as a threat directed at the government of the target State. In this scenario the intervening State formulates demand regarding *domaine réservé* of the target State and threatens that unless the demand is met it will use a means of disinformation to support opponents of the government during the electoral process or to destabilise the elections altogether. However, such a demand would allow the target State to prepare itself and the population against disinformation operations so it could prove self-defeating. The victim's awareness of a planned attempt to manipulate

150 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace".

151 I will discuss the issue of threshold later in this subsection.

the electoral process would blunt its potential effects. It is not surprising that states hid their involvement in disinformation campaigns.[152]

Importantly, disinformation campaigns may also take place after voting. Such operations may try to convince the target audience that the results of the voting were fabricated or that significant electoral irregularities took place. Here the goal may be either to overturn the election results or to undermine the political system of the target State. Had the assault on the Capitol in 2021 in the aftermath of the US presidential elections been instigated by foreign disinformation campaign it would have been a clear-cut case of prohibited intervention into *domaine réservé* of another state even though eventually it proved unsuccessful in overturning the result of the election.[153]

Any involvement of another State into electoral process of another interferes with the *domaine réservé* of the latter and even if it does not violate the principle of non-intervention (because it does not reach the threshold of coercion) it can still be unlawful under the principle of sovereignty or under international human rights law.[154]

The coercion-as-control model will also apply to disinformation targeting other areas belonging to *domaine réservé* such as public health, public order, and public safety. Disinformation campaigns spreading falsehoods about vaccines or public health measures could thwart governments' efforts to protect their population which would be tantamount to depriving it of control over their sovereign prerogative. This could result in many more otherwise avoidable deaths and huge economic losses, which should bear on a legal analysis of disinformation. Under certain circumstances disinformation campaigns could be treated as fomenting or inciting subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another state or interfering in civil strife in another State, i.e. the activities which according to the Declaration on Friendly

152 1st EEAS Report on Foreign Information Manipulation and Interference Threats, 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf; Roberts, China's Disinformation Strategy, Its Dimensions and Future, Atlantic Council, 2020.

153 January 6 U.S. Capitol attack summary, Britannica, accessed 29.05.2025, https://www.britannica.com/summary/January-6-U-S-Capitol-attack

154 In turn, a foreign State threatening to use military force in case of unwelcomed election result would violate the non-intervention principle, yet these kind of actions are beyond the scope of this article.

Relations would violate the principle of non-intervention.[155] Similarly, as with a public health, one could argue that disinformation campaigns deprive the target State of control over its public order and public safety and by doing so violate the prohibition on intervention.

Another, even if not raised so far by states scenario is supporting insurgents engaged in a military struggle against the government by means of disinformation. A foreign State could directly engage in spreading disinformation that either undermines support for the government or strengthen popularity of the insurgents among population. Alternatively, it could engage in indirect manner by providing the insurgents with tools enabling conducting more effective disinformation campaigns such as programmes to create deep fakes or training them in spreading disinformation more effectively. Such activities could be perceived as providing support to the insurgents and as such be treated as prohibited intervention.[156] They could potentially deprive the target State of control in several areas of *domaine réservé* such as freedom to choose its own political, economic, and social system. Such an involvement could also undermine the target State territorial integrity.

At the end of this section, I will make several remarks regarding all of the scenarios discussed above.

Firstly, the control model is more suitable to assess whether a disinformation campaign is coercive. The analysis of states' views would also indicate their preference, even if implicit, to apply this model. None of the states that referred to disinformation in their national positions even mentioned a demand or threat that forms an indispensable part of coercion under the extortion model. Instead, they spoke about disrupting or subverting the internal order (Costa Rica),[157] impeding the orderly conduct of an election and the casting of ballots (Germany)[158], undermining a state's public health efforts (New Zealand)[159], resulting in civil unrest (Poland)[160],

155 Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations (GA Res. 2625(XXV)), 1970.

156 *Military and Paramilitary Activities in and Against Nicaragua*, Merits, ICJ judgment of 1986, I.C.J. Rep 14, paras. 192, 205, and 242.

157 Position of Costa Rica.

158 Position of Germany.

159 Position of New Zealand.

160 Position of Poland.

engineering the public opinion (Iran)[161]. While Austria refers to activities that are undertaken to compel another state to involuntarily change its behaviour, which could indicate a preference for the extortion model, the example it provides in its position paper (disinformation campaign leading to a governmental crisis) seems to be closer to the control model.[162]

Secondly, as we observed in section 3.1.1. above, a foreign State's activities must reach a certain threshold of intensity to be treated as coercion. This requirement is critically important in the context of disinformation, otherwise the principle of non-intervention could become over inclusive and cover an enormous amount of influence in the operations conducted by states. Thus, in each case disinformation campaign, to be qualified as coercion, it must be broad and effective enough to reach a significant part of population and be able to influence the way its recipients think and/or act in a meaningful way. The positions of Poland, Germany, and New Zealand veer in this direction. Poland believes that a disinformation campaign to violate the non-intervention principle must be wide-scale and targeted and its results must require specific responses from the target State.[163] Germany refers to the scale and effects criteria.[164] While according to New Zealand, the threshold may be reached when the disinformation operation is prolonged and coordinated and when its impact is significant.[165]

Yet, how to precisely assess when a threshold of intensity is reached is far from certain and must be analysed on case-by-case basis. After all, a disinformation campaign will never leave the targeted population without a choice. The audience can always switch to another website or stop following the sites spreading fake news. At the same time, the psychological mechanism of reinforcing biases and echo-chambers leaves the targeted population vulnerable and unaware that it is being subjected to manipulation which, as we have noted, can be treated as coercion.

The manipulation used in disinformation campaigns is typically twofold: a) news that is spread is false or misleading; b) the foreign authors

161 Position of Iran. The Iranian position poses challenges from the Freedom of Expression and Opinion perspective. Yet, the deeper analysis of human rights implications of disinformation or responses thereto goes beyond the scope of this article.

162 Position of Austria.

163 Position of Poland.

164 Position of Germany.

165 Position of New Zealand.

of disinformation are unknown to the target audience.[166] This doubled-pronged manipulation technique allows one to control the victim[167] whose perception of reality has been mischievously transformed and who is deprived of his/her freedom to think and act independently. The presence or lack thereof of these two elements of manipulation should weigh on the assessment of the effectiveness of disinformation campaigns.

This explains why the open involvement of an intervening State into the electoral process by, for example, spreading propaganda about candidates[168] or stating publicly that election of State A would have a negative impact on bilateral relations and would not reach the level of coercion. Arguably, the public dissemination of false information about electoral candidates by a foreign state would not be coercive either. The target audience would know about the involvement of a foreign power and it could assume that this power has its own interests in influencing the results of the elections. Sharing with the target audience information extracted through cyber operations (so called doxfare), would not be coercive either[169] unless the intervening State would threaten to publish compromising material in case its demands are not met.[170]

Depriving the target State of its freedom of choice does not need to be complete to treat it as coercion as the African Union rightly pointed out in its statement on the application of international law to cyberspace.[171] In some cases, like in the spread of the pandemic, it is enough that a disinformation campaign manipulates only a limited portion of the population to achieve far-reaching consequences that eventually may result in the death or serious disease of thousands or millions. Similarly, a foreign state may undermine

166 To Schmitt a covert nature of influence operations would be an additional argument to treat them as coercive. Because the target audience (the voters) does not know about being manipulated by another state pursuing its own interests its decision making is undermined. It is precisely the deception that separates a coercive operation from mere interference even in cases where the impact on elections outcome is indirect Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", 52. Similarly, Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 42.

167 Strauss, "Persuasion, Autonomy, and Freedom of Expression", 334, 354.

168 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 42.

169 Wheatley, "Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion"", 24.

170 Milanović, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", 634.

171 Common African Position.

the public order of another state by radicalising a relatively small group of people if a disinformation campaign incites them to resort to violence. In the case of electoral manipulation, the threshold will depend on the political situation of the target State, in some situations impacting on a thousand voters may lead to a distorted voting result, in others changing the views of hundreds of thousands will not have broader political implications. Overall, the loss of control will mean different things in different contexts.

Thirdly, because disinformation, unlike misinformation, is by definition intentional in all the aforementioned cases there must be an intent of the creator or the peddler of disinformation to mislead the target audience.

Fourthly, coercive behaviour does not need to be successful to be classified as coercion. Thus, to be treated as coercion a disinformation campaign does not need to, for example, change the voting outcome, destabilise the political system, or lead to a civil unrest.[172] It is enough that it could potentially achieve these goals if either the campaign was better planned or executed or if the target State were less resilient. Moreover, disinformation does not need to have a direct impact on the target State behaviour. Hence, it is sufficient, for example, to try to manipulate voters without directly targeting the voting tally. We do not need to prove direct causation of harm or potential harm; it is enough to establish a reasonably high probability of it.[173] Nonetheless, in the case of disinformation, it may be difficult to prove that an unsuccessful attempt to change the views of the target audience would result in negative effects serious enough to treat the foiled campaign as an intervention.

Finally, an additional argument for recognising the aforementioned cases as prohibited intervention is that disinformation campaigns described in these scenarios would arguably violate other norms of international law, i.e. international human rights law. Spread of disinformation regardless of its goal could violate the right to freedom of expression and opinion, which 'includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media'.[174] When a disinformation campaign is based on micro-targeting, it could also violate the right to privacy. In case of influencing an electoral campaign,

172 Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", 42.

173 Dias, *Study on International Norms for Foreign Information Manipulation and Interference*, 5.

174 Article 19 of ICCPR.

the right to free and fair elections, the right to participate in public affairs, and the right to self-determination could also be breached. Undermining a state's effort to find the pandemic could be analysed from the perspectives of the right to health or the right to life. Destabilising the internal order and supporting insurgents could violate the prohibition of propaganda for war and of advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, and violence.[175] Notably, under international human rights law, the target State is obliged to protect the human rights of individuals and groups under its jurisdiction.

6. Conclusions

My goal in this article was to demonstrate that disinformation campaigns in certain circumstances may violate the principle of non-intervention. By applying mainly the control model, I analysed how these kinds of operations may coerce the target State by depriving it of control in areas where it should be allowed to decide freely. While assessing which kind of disinformation campaigns can violate the principle of non-intervention, I tried to avoid interpreting the principle in too broad a manner while also avoiding a too limiting understanding of the term coercion which to my mind would favour the interfering states *vis-à-vis* the potential victims.

What stems from the analysis is that it is by no means easy to assess the effects of disinformation on states' freedom of action which is necessary to establish whether a prohibited intervention took place. This type of operation aims at affecting the cognitive sphere of individuals. It is not clear to what extent it is effective in changing their beliefs. Even if members of the target audience change their views it may not always be clear what part disinformation may have in a change and if it resulted in altered behaviour. The impact of disinformation may be long-term and achieve the goals of the intervening State after a considerable amount of time. The difficulty also lies in assessing how large a part of the population must be manipulated by disinformation to convincingly claim that the tipping point was reached and the target State lost control over an area belonging to its *domaine réservé*.

175 Countering disinformation for the promotion and protection of human rights and fundamental freedoms, Report of the Secretary General, 2022, A/77/287; Rikhter, International law and policy on disinformation in the context of freedom of the media, Brief Paper for the Expert Meeting organised by the Office of the OSCE Representative on Freedom of the Media.

These obstacles may explain the relative scarcity of State practice regarding the assessment of specific cases of disinformation as violations of international law, including violations of the non-intervention principle. The covert nature of disinformation no doubt poses a challenge in evaluating the state practice too.

Yet, the landscape has been changing quickly in recent years. A number of States have referred in their national statements to disinformation in the context of the principle of non-intervention. The African Union consisting of fifty-five states referred to instruments of information. In 2024, the Constitutional Court of Romania decided to annul the first round of presidential elections stating that the foreign disinformation campaign 'distorted the free and fair nature of the vote expressed by citizens and the equality of opportunity of electoral competitors, affected the transparency and fairness of the electoral campaign and disregarded the legal regulations regarding its financing'.[176] Also, in 2024 the Council of the European Union adopted sanctions against individuals involved in disinformation activities under the sanctions regime regarding Russia's destabilising activities which was established by Council Decision (CFSP) 2024/2643 and Council Regulation (EU) 2024/2642. Under the sanction regime, disinformation is perceived as one type of destabilising activities.[177] In the Decision the Council provides that the activities covered by the sanction regime, including coordinated information manipulation and interference can undermine or threaten independence and sovereignty of member states or third countries.[178]

This increase in activities regarding disinformation undoubtedly derives from the growing awareness of the fact that this phenomenon serves as a highly effective tool capable of disrupting and debilitating adversarial states. The difficulties in assessing its impact and causal links between such campaigns and harm caused should not leave disinformation in the legal grey zone. The democratic states with their open society and robust protections of freedom of speech stand to lose the most from such legal uncertainty. Luckily, the principle of non-intervention provides us with a proper legal framework to address this challenge.

176 Kleczkowska, "The Russian Disinformation Campaign During the Romanian Presidential Elections: The Perfect Example of a Violation of International Law?".

177 Preambular paragraph 3. Council Decision (CFSP) 2024/2643.

178 Article 2(1)(a)(iv) Council Decision (CFSP) 2024/2643.

Bibliography

1. *Armed activities on the territory of the Congo* (Democratic Republic of the Congo v. Ruanda), Judgment, I.C.J. Rep 2006, p. 168.
2. *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, I.C.J. Rep 2010, p. 403.
3. Baade, Björnstjern. "Fake News and International Law." *The European Journal of International Law* 29 no. 4 (2018): 1357-1376.
4. Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 (2012): 212–227.
5. Buchan, Russell, and Nicholas Tsagourias. "The Crisis in Crimea and the Principle of Non-Intervention." *International Community Law Review*, 19 2-3 (2017): 165-193.
6. Charter of United Nations. United Nations, Treaty Series vol. 1, p. 16.
7. Charter of the Organization of American States. United Nations, Treaty Series vol. 119, p. 3.
8. Charter of Organization of African Unity. United Nations Treaty Series, vol. 39, p. 479.
9. Charter of ASEAN, United Nations Treaty Series, vol. 2642, p. 223.
10. *Corfu Channel Case*, Judgment, I.C.J. Rep 1949, p. 4.
11. Covenant of the League of Nations. League of Nations Treaty Series vol. 188, p. 108.
12. Countering disinformation for the promotion and protection of human rights and fundamental freedoms, Report of the Secretary General, 2022, A/77/287.
13. Dias, Talita. *Study on International Norms for Foreign Information Manipulation and Interference*. November 2023. https://www.eeas.europa.eu/sites/default/files/documents/2024/Study%20international%20norms%20on%20FIMI.pdf.
14. Disinformation and freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, 2021, A/HRC/47/25.
15. Efrony, Dan, and Yuval Shany. "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *American Journal of International Law* 112 issue 4 (2018): 583 - 657.
16. Ferreira Caceres, Maria Mercedes, Juan Pablo Sosa, Jannel A. Lawrence, Cristina Sestacovschi, Atiyah Tidd-Johnson, Muhammad Haseeb Ul Rasool, et. al. "The impact of misinformation on the COVID-19 pandemic." *AIMS Public Health* 9(2) (2022): 262-277.
17. Final Act of the Conference on Security and Co-operation in Europe. International Legal Materials, vol.14, p.1292.
18. Floridi, Luciano. *The fourth revolution: how the infosphere is reshaping human reality*. Oxford: Oxford University Press UK, 2014.
19. Gill, Terry. "Non-Intervention in the Cyber Context." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski. Estonia: NATO CCD COE Publication, 2013.
20. Guess, A., and Benjamin A. Lyons. „Misinformation, Disinformation and Online Propaganda." In *Social Media and Democracy The State of the Field, Prospects*

for Reform, edited by Nathaniel Persily, and Joshua A. Trucker: 10-33. Cambridge University Press, 2020.
21. Hamm, Lauren. "The Few Faces of Disinformation." *EU Disnfo Lab*. May 11 2020. https://www.disinfo.eu/publications/the-few-faces-of-disinformation/#:~:text=With%20the%20use%20of%20fake%20identities%2C%20online%20profiles%20and%20websites,of%20undermining%20climate%20protection%20measures.
22. Helal, Mohamed. "On Coercion in International Law." 52 *New York Uniersity Journal of International Law and Policy* 1 (2019): 49-54.
23. Human Rights Council. A/HRC/RES/49/21 (2022).
24. Human Rights Council. A/HRC/RES/55/10 (2024).
25. International Covenant on Civil and Political Rights. United Nations, Treaty Series, vol. 999, p.171.
26. International Law Commission, Draft Declaration on Rights and Duties of States, 1949. Yearbook of the International Law Commission 1949, Vol. I, pp 286-290.
27. International Law Commission, Responsibility of States for Internationally Wrongful Acts. Supplement No.10 (A/56/10), chp.IV.E.1, November 2001.
28. Jamnejad, Maziar, and Michael Wood. *The Principle of Non-intervention*, Cambridge University Press, 2009.
29. Jennings, Robert, and Arthur Watts. *Oppenheim's International Law – Vol. 1: Peace*, 9th ed. Oxford University Press, 2008.
30. Kahler, Miles. "Foreign Influence and Democratic Governance." *Council on Foreign Relations*. October 7 2024. https://www.cfr.org/report/foreign-influence-and-democratic-governance.
31. Keller, Helen. "Friendly Relations Declaration (1970)." *Max Planck Encyclopedia of Public International Law*. 2021.
32. Kilovaty, Ido. "The Elephant in the Room: Coercion." *AJIL Unbound*, 113 (2019): 87-91.
33. Kleczkowska, Agata. "The Russian Disinformation Campaign During the Romanian Presidential Elections: The Perfect Example of a Violation of International Law?" *Opinio Iuris*. January 27 2025. https://opiniojuris.org/2025/01/27/the-russian-disinformation-campaign-during-the-romanian-presidential-elections-the-perfect-example-of-a-violation-of-international-law/.
34. Kułaga, Łukasz. „Działania w cyberprzestrzeni wpływające na wybory w innym państwie a zasada nieinterwencji". In *Przestrzeń cyfrowa. Nowe wyzwania dla prawa międzynarodowego i prawa Unii Europejskiej*, edited by Cezary Mik and Łukasz Kułaga. Warsaw: Wyd. UKSW, 2021.
35. Kunig, Philip. "Prohibition of Intervention." *Max Planck Encyclopedia of Public International Law*. 2008.
36. Kranz, Jerzy. *Pojęcie suwerenności we współczesnym prawie międzynarodowym*, Warszawa 2015.
37. Lauterpacht, Hersch. *The International Protection of Human Rights*. Librairie du Recueil Sirey 1947.
38. Lowe, Alan Vaughan. *International Law*. Oxford University Press, 2007.
39. Marshall, Hannah, and Alena Drieschova. "Post-Truth Politics in the UK's Brexit Referendum". *New Perspectives* 26, no. 3 (2018): 89-106.

40. Mik, Cezary. „Fenomenologia regionalnej integracji państw. Studium prawa międzynarodowego". In t. 2: *Regionalne organizacje integracyjne z perspektywy analitycznej prawa międzynarodowego*. C.H. Beck, 2019.
41. Milanović, Marco. "Revisiting Coercion as an Element of Prohibited Intervention in International Law". *American Journal of International Law*, 117, issue 4 (2023): 601 – 650.
42. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)*, Judgment, I.C.J. Rep 1986, p. 14.
43. Moynihan, Harriet. "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", *Chatham House Research Paper*, December 2019.
44. *Nationality Decrees Issued in Tunis and Morocco*, Advisory Opinion, 1923 P.C.I.J. Rep Ser. B No. 4, p. 22.
45. Nolte, George. „Article 2(7)". In *The Charter of the United Nations: A Commentary*, edited by Bruno Simma 3rd Edition. Oxford: Oxford University Press, 2012.
46. Office of the United Nations High Commissioner for Human Rights, Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, 2022.
47. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. A/76/136.
48. Ohlin, Jens David. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (2017): 1579–98.
49. Rikhter, Andrey, "International law and policy on disinformation in the context of freedom of the media." Brief Paper for the Expert Meeting organized by the Office of the OSCE Representative on Freedom of the Media, 14 May 2021.
50. Roberts, Dexter. "China's Disinformation Strategy, Its Dimensions and Future." *Atlantic Council*, 2020.
51. Schmitt, Michael (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edition. Cambridge: Cambridge University Press, 2017.
52. Schmitt, Michael. "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Chicago Journal of International Law* 19, no. 1, article 2 (2018): 30-67.
53. Schmitt, Michael, and Liis Vihul. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *American Journal of International Law Unbound* 111 (2017): 213 – 218.
54. Skafle, Ingjerd, Anders Nordahl-Hansen, Daniel S. Quintana, Rolf Wynn, Elia Gabarron. "Misinformation About COVID-19 Vaccines on Social Media: Rapid Review". *J Med Internet Res*. 4;24 (8) (2022).
55. Strauss, David. "Persuasion, Autonomy, and Freedom of Expression" *Columbia Law Review* 91 (1991): 333- 371.
56. Tsagourias, Nicholas. "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace." *EJIL: Talk!* 26 August 2019. https://www.ejiltalk.org/

electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.
57. UN General Assembly. "Countering disinformation for the promotion and protection of human rights and fundamental freedoms". A/RES/76/227 (2021).
58. UN General Assembly. "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States." A/RES/20/2131 (1965).
59. UN 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". 2625(XXV) (1970).
60. Vienna Convention on the Law of Treaties. United Nations Treaty Series, vol. 1155, p. 331.
61. Wanyana, Racheal. "Cognitive Warfare: Does it Constitute Prohibited Force?" *EJIL: Talk!* 30 January 2025. https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/.
62. Wardle, Claire, and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking." Council of Europe, 31 October 2017.
63. Watts, Arthur. "Low-Intensity Cyber Operations and the Principle of Non-Intervention". In *Cyber War: Law and Ethics for Virtual Conflict*, edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein. Oxford University Press, 2025.
64. Wheatley, Steven. "Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion."" *Duke Journal of Comparative & International Law*, 31 (2020): 161-197.
65. Yaffe, Gideon. "Indoctrination, Coercion, and Freedom of Will." *Philosophy and Phenomenological Research* LXVII (2) (2003): 335-356.
66. Ziegler, Katja. "Domaine Réservé", *Max Planck Encyclopedia of Public International Law*. 2008.