XLIII POLISH YEARBOOK OF INTERNATIONAL LAW

2024 DOI 10.24425/PYIL.2025.156715

PL ISSN 0554-498X
e-ISSN 2957-1510

Milan Lipovský[*]

SUITABILITY OF THE PRINCIPLE OF NON-INTERVENTION TO REGULATE CYBER INFORMATION OPERATIONS TARGETING ELECTIONS

Abstract: *The principle of non-intervention belongs amongst the most often discussed rules of international law with the potential to regulate cyber information (dis- and misinformation) operations carried out by one state and dedicated to influence another state's elections results (through the electorate). Contributions to those discussions differ significantly however as to the suitability of the rule for this purpose. This article tackles the issue in a step-by-step analysis, first dealing with the elements of the principle of non-intervention and its position in the systematics of the law of international peace and security, secondly analysing the applicability of the rule in cyberspace, in order to thirdly determine and evaluate what are the critical issues in the application of the rule to cyber information operations targeting the electorate of another state. Because the principle belongs to the most approximate rules of international peace and security regulation to tackle these operations, the last section is dedicated to recommendations that if applied, they might increase the likelihood of the applicability of the principle of non-intervention to the operations discussed.*

Keywords: principle of non-intervention, cyber information operations, elections

INTRODUCTION

States have often attempted to influence the public opinion in other states. While propaganda has generally not been considered as violating international law, the reason might be seen before the invention of mass communications tools in the fact that propaganda delivery was complicated without accessing the territory of

[*] Lecturer and researcher (Ph.D.); Department of International Law, Faculty of Law, Charles University (Prague, Czech Republic); email: lipovsky@prf.cuni.cz; ORCID: 0000-0002-2636-3737. This work was supported by the European Regional Development Fund project "Beyond Security: Role of Conflict in Resilience-Building" (reg. no.: CZ.02.01.01/00/22_008/0004595).

the target state; consequently, it was limited by the regulation to resort to force. Propaganda was thus not regarded with interest by states.

Inventing modern media, and especially utilization of the internet and social media, have however technologically allowed the spread of information across borders without the need to physically cross them. By this development, previously existing reasons for not regulating propaganda suddenly disappeared and states are now facing a new situation and the need to legally address it. This issue is an example of the famous question: is international law (as it is) applicable to cyberspace or does it need to be updated?

Naturally, influencing a target state's public opinion via cyber tools is only possible as long as the targeted population has access to the internet and wishes to consume the information. That explains the interest regarding this issue in states with high portions of their populations using the so-called social media. The issue is exacerbated by the utilization of bots[1] that may share and multiply information on a previously unforeseen scale.

While sharing information on the social media (and internet in general) may have positive consequences, it can also be used for nefarious purposes.[2] A seemingly straightforward way to fight against them is to properly verify received information, however making a qualified opinion when overflown with false or manipulating information may be extremely difficult.

Cyber influence campaigns (or operations) targeting populations of various states, particularly in the short period before elections, have been publicly reported already.[3] Considering the fact that sometimes, the elections results are very close, the potential of such operations to change them is not negligible.

As a consequence, states and doctrine began discussing suitability of international law rules to regulate the campaigns in question. These most often analysed

---

[1] "[B]its of code designed to interact with and mimic human users." B. Sander, *Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 Chinese Journal International Law 1 (2019), p. 12.

[2] For a human rights-based perspective, *see e.g.* M. Hanych, M. Pivoda, *Disinformation and Fake News in Current Jurisprudence of the Strasbourg Court: An Unsolved Problem*, in: G. Terzis, G. Terzis, D. Kloza, E. Kużelewska, D. Trottier (eds.), *Disinformation and Digital Media as a Challenge for Democracy*, Intersentia, Cambridge: 2020.

[3] *E.g.* R.S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, vol. 1 of 2, US Department of Justice, Washington: 2019, available at: https://www.justice.gov/archives/sco/file/1373816/dl?inline= (accessed 30 June 2025) (Mueller Report). Several cyber operations targeting elections (usually without dealing with attribution) were also described on pp. 36–37 of M.N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19(1) Chicago Journal of International Law 30 (2018). In Romania, the Constitutional Court even annulled 1st round of presidential elections in 2024 on the basis of foreign interference. S. Rainsford, *Romanian court annuls result of presidential election first round*, BBC.com, 6 December 2024, available at: https://www.bbc.com/news/articles/cn4x2epppego (accessed 30 June 2025).

rules include the international law-based principles of non-intervention and/or sovereignty,[4] due diligence,[5] or self-determination.[6]

This article is focuses on the principle of non-intervention[7] and its goal is to assess its suitability in its current state in international law to regulate cyber disinformation and misinformation campaigns that target another state's electorate's voting. And if it is found unsuitable, to make recommendations as how to reinterpret it in order to satisfy the suitability. At the same time, the article leaves aside information operations conducted by non-state actors, except those whose activity is attributable to a state. The reason is that the principle of non-intervention applies on the interstate level.[8] It also leaves aside the issue of the regulation of foreign media residing in the target state and their regulation.[9]

To reach its goal, the article first needs to confirm a hypothesis (that even though the principle of non-intervention crystallized long before invention of cyberspace, it *is* generally applicable in this domain; at the same time however, its elements as they are understood now may not be applied in a way that would fit easily with the dis- and misinformation operations attempting to influence the target state's electorate in its voting). Subsequently, should the hypothesis be found incorrect, the principle would be suitable to regulate the campaigns in question. Since however research confirmed it to be correct, upon reaching its confirmation, the article addresses the research question: how do the elements of the principle of non-intervention need to be changed or reinterpreted in order for the principle to be suitable to regulate these operations?

Since problematic elements are identified, the last section builds upon them and identifies recommendations that, if applied, would increase the likelihood of applicability of the principle of non-intervention to the campaigns in question.

Thus, following necessary terminology and opening the topic, the text addresses the principle of non-intervention, its elements, and applicability in cyberspace (section 2). In section 3, it evaluates the principle's applicability to the dis- and

[4] *See e.g.* the references to it by states' representatives in the 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, 13 July 2021, A/76/136, available at: https://docs.un.org/en/A/76/136 (accessed 30 June 2025) (2021 Compendium).

[5] *E.g.* Sander, *supra* note 1, pp. 24–26.

[6] *E.g.* J.D. Ohlin, *Election Interference*, Cambridge University Press, Cambridge: 2020, pp. 90–117.

[7] The term interference is understood here as any activity within another state's sovereign sphere regardless of its legality, while intervention is a narrower concept limited to illegal/prohibited form that the principle of non-intervention covers.

[8] Schmitt, *supra* note 3, p. 48.

[9] For this topic, *see e.g.* M. Říha, *Freedom of Speech, Propaganda and EU at War: Case of Russia Today France*, 14(1) The Lawyer Quarterly 111 (2024).

misinformation operations targeting another state's electorate and the last chapter addresses the recommendations.

1. TERMINOLOGY AND SETTING THE SCENE

Campaigns targeting another state's electorate fit within so-called influence operations. And two types of influence operations[10] need to be distinguished: so-called doxing operations that utilize hacking electronic systems and leaking of non-public information found there,[11] and information operations.[12] Distinguishing the types of information operations turns out to be terminologically problematic, however. They are sometimes divided into malinformation and disinformation,[13] sometimes misinformation and disinformation,[14] and occasionally misinformation, malinformation, and disinformation are being distinguished.[15] This article adopts the differentiation used for example by the Australian authorities:

> Misinformation is false information that is spread due to ignorance, or by error or mistake, without the intent to deceive. Disinformation is knowingly false information designed to deliberately mislead and influence public opinion or obscure the truth for malicious or deceptive purposes.[16]

Consequently, the difference between disinformation and misinformation is in the intent. Both consists of false information, but a disinformation is spread

---

[10] M. Roscini, *International Law and the Principle of Non-Intervention*, Oxford University Press, Oxford: 2024, p. 396.

[11] Sander, *supra* note 1, p. 8. An example of hack and release operation was claimed to have happened by the Mueller, *Report...*, *supra* note 3, p. 1: "a Russian intelligence service conducted computer-intrusion operations against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents."

[12] Mueller, *Report...*, *supra* note 3, p. 1: "a Russian entity carried out a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton." Instead of using term information operation, the Mueller Report claimed (p. 4) existence of "a social media campaign designed to provoke and amplify political and social discord in the United States." Thus, whether/how to identify it as a particular information operation depends on further aspects.

[13] Roscini, *supra* note 10, pp. 396–397.

[14] *See e.g. Disinformation and Misinformation*, Australian Electoral Commission, available at: https://www.aec.gov.au/About_AEC/files/eiat/eiat-disinformation-factsheet.pdf (accessed 30 June 2025).

[15] *See e.g. Misinformation, Disinformation & Malinformation: A Guide*, rinceton, available at: https://princetonlibrary.org/guides/misinformation-disinformation-malinformation-a-guide/ (accessed 30 June 2025).

[16] *Disinformation...*, *supra* note 14. There are other similar definitions. Disinformation may be defined as epistemically wrong massively spread information intentionally manipulating the addressees in order to cause harm. T. Koblížek, M. Hanych, J. Kalenský, *Dezinformace a hate speech z hlediska filozofie, práva a bezpečnosti* [Disinformation and Hate Speech from the Perspective of Philosophy, Law, and Security], Academia, Praha: (to be published in 2025), ch. 1.

deliberately, while misinformation is spread without the intent to deceive by the last sharer (though the original source may have different motives). And it is exactly the possibly of malicious intent by the original source that last "sharer" of the information may be unaware of why this article includes misinformation into the research question.

The focus of this article is upon cyber information operations carried out by one state and targeting the electorate of another state to compel it to vote in a certain way or to refrain from voting. For simplicity, this article will call them *cyber electorate targeting information campaigns* (CETICs).[17] They will often be compared to doxing operations and so-called cyber tampering operations[18] however.

Though not explicitly addressing the dis-/misinformative topic (that this article considers an element of a CETIC) and also taking into account that this article works on the assumption of attribution of a CETIC to a state (while the relationship between the Internet Research Agency and Russian government remains unclear[19]), an otherwise fitting example of a CETIC that this article focuses upon is the Mueller Report's claimed Internet Research Agency's (IRA)[20] activity:

> The IRA conducted social media operations targeted at large U.S. audiences with the goal of sowing discord in the U.S. political system. [footnote omitted ...] Using fictitious U.S. personas, IRA employees operated social media accounts and group pages designed to attract U.S. audiences. These groups and accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists. Over time, these social media accounts became a means to reach large U.S. audiences.
>
> IRA employees posted derogatory information about a number of candidates in the 2016 U.S. presidential election. By early to mid-2016, IRA operations included supporting the Trump Campaign and disparaging candidate Hillary Clinton.[21]

Thus, "the objective was not only to convince individuals how to vote, but also to keep certain voters from the polls."[22] This exact kind of operation is considered to be within the grey zone of normative uncertainty of influence operations targeting elections. They are neither widely recognized as constituting violation of the

[17] Terms used by other authors such as elections meddling, disenfranchisement, etc. are avoided here because they are not specific enough to exclude for example doxing operations and tampering operations (*see* below). At the same time, the word "cyber" is used to point out that focus is on social media and other internet campaigns.

[18] Operations that hack the elections counting systems and change the results therein or the casted ballots. *Similarly see* Sander, *supra* note 1, p. 4.

[19] Schmitt, *supra* note 3, p. 35.

[20] A Russian entity once funded by Y.V. Prigozihin (Mueller, *Report...*, *supra* note 3, p. 14).

[21] *Ibidem*, p. 14.

[22] Schmitt, *supra* note 3, p. 35.

principle of non-intervention (like cyber tampering operations), nor are they clearly considered legal (like for example, media newsfeed with a clear source).[23]

2. PRINCIPLE OF NON-INTERVENTION, ITS ELEMENTS, AND APPLICABILITY IN CYBERSPACE

In order to assess suitability of a certain rule to a certain situation, it is necessary first to establish its elements. For that reason, this section explains the principle and finds out whether it is applicable in cyberspace because should the answer be negative, the entire debate would be pointless. In explaining the elements, the article also points out critical issues that will play a significant role in the subsequent section.

Although the principle of non-intervention belongs to the core of international peace and security regulation, it was omitted by the authors of the UN Charter[24] in its explicit textual regulation. The closest reference to it can be found in Art. 2(7) UN Charter,[25] however that provision applies to the relationship between the UN and its member states, not to the interstate level.

The principle can be however deduced implicitly from rules contained in Art. 2 UN Charter.[26] Non-intervention is closely related to the principle of equal sovereignty of states contained in Art. 2(1) of the UN Charter,[27] in fact it is considered as its corollary.[28] A state independent of any other power than its own (sovereign) is logically entitled to demand no intervention in its internal and/or external affairs (that in fact being the key point of the principle of non-intervention), otherwise it would not be independent.[29]

[23] *See e.g. ibidem*, p. 50.

[24] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 892 UNTS 119 (UN Charter).

[25] "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state 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."

[26] F. Delerue, *Cyber Operations and International Law*, Cambridge University Press, Cambridge: 2020, p. 235.

[27] Ohlin, *supra* note 6, chapter 3. On p. 71, the author highlights the reference to non-intervention in the Montevideo Convention (Convention on the Rights and Duties of States (adopted 26 December 1933, entered into force 26 December 1936) 165 LNTS 19) and its connection to sovereignty as its basis. The principle is similarly closely connected to the use of force prohibition as the ICJ noted in ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, 27 June 1986, ICJ Rep 1986, p. 14, para. 212 (*Nicaragua* judgment).

[28] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para. 202. *See also* M.N. Schmitt, L. Vihul (eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press, Cambridge: 2017, p. 312 (rule 66) (Tallinn Manual 2.0); or Delerue, *supra* note 26, pp. 233–234.

[29] Even the very first sentence (para. 202) of the *Nicaragua* judgment dealing with the principle states: "The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside *interference*."

The principle of non-intervention has been elaborated upon by the International Court of Justice (ICJ) in its *Nicaragua* judgment.[30] Based upon it, the obvious case of a violation of the principle of non-intervention is a forcible intervention that deprives the target state of its free will to govern its territory. The ICJ divided forcible intervention into two subcategories - direct intervention where one state uses force against another, and indirect one involving "support for subversive or terrorist armed activities within another State."[31] By this notion, the ICJ also confirmed that supporting armed groups in another state may constitute a use of force.[32] Confirmation of the possibility of indirectness of non-forcible intervention is however a controversial topic . In order to be applicable to CETICs, the principle must however also cover non-forcible and indirect forms of intervention. For that reason, this article addressed this topic in section 3.

In the same judgment, the ICJ confirmed two elements of the principle: a) internal or external affairs of a state (*domaine réservé*[33] or sovereign discretion[34]),[35] and b) coercion.[36]

These two elements (*domaine réservé* and coercion) complement each other, and the principle of non-intervention is thus based on the prohibited nature of deprivation of the free will of target state in the sphere that it is entitled to decide on its own.

By virtue of general international law, *domaine réservé* denotes spheres in which every state is entitled to make free decisions without outside intervention. It includes "political, economic, social and cultural system, and the formulation of foreign policy."[37] As such it covers both internal as well as external affairs.[38] It should be

[30] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para 205.

[31] *Ibidem*.

[32] *E.g. ibidem*, para. 241. For analysis of supporting a state, not an armed group, by providing weapons, *see e.g.* M. Lipovský, *Assessing the Legal Boundaries of Military Support to Ukraine from the Perspective of Use of Force*, 50(1–2) Review of Central and East European Law 87 (2025).

[33] "[T]hose matters on which international law does not speak or that international law leaves solely to the prerogative of States [...] and are therefore to be regarded as protected from intervention by other States." Schmitt, Vihul, *supra* note 28, p. 314 (rule 66). Note that *domaine réservé* is sometimes understood as synonymous only to internal affairs. External affairs left to state's free will are however also part of this element and they include "choice of extending diplomatic and consular relations, recognition of States or governments, membership in international organisations, and the formation or abrogation of treaties." *ibidem*, p. 317. To simplify the references in this article however, the first element is called *domaine réservé* and understood as including both the internal and external affairs.

[34] Term used by Ohlin, *supra* note 6, p. 72.

[35] Although the Court did not use the term *domaine réservé*, it basically described it in para. 205 of the ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*: "A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely."

[36] "Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones" (*ibidem*, para. 205).

[37] *Ibidem*.

[38] Also confirmed by Schmitt, Vihul, *supra* note 28: "Rule 66 – Intervention by States: A State may not intervene, including by cyber means, in the internal or external affairs of another State."

noted that this statement depends on general international law. States are obviously allowed to voluntarily limit their *domaine réservé* in mutual relations and even allow for other states to exercise their powers within those areas.[39] It will turn out that this element is not problematic from the perspective of applying non-intervention to CETICs (see next section).

The same may not be stated about coercion though. This second element is based on removal of free will of the coerced actor.[40] In written sources of international law, the term is used for example in Art. 52[41] of the Vienna Convention on the Law of Treaties (VCLT).[42] This provision confirms the absolute invalidity of a (would be) treaty in case of coercion of a state by the threat or use of force contrary to the principles of the UN Charter in relation to its conclusion. Thus, the provision confirms coercion to be based upon removal of free will.

When explaining coercion, other sources refer to subordination[43] or subjugation,[44] or dictatorial character of interference.[45] By doing so, they also point out a common basis in the removal of free will of the coerced actor. In the Tallinn Manual 2.0, the element is claimed not to be defined by international law and understood as "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 [footnote omitted]."[46]

As is visible from the various descriptions of the second element, coercion rests in removal of free will but it may not relate to *anyone*'s free will, it must focus on the will of the targeted state. Even the other article of the VCLT that refers to coercion[47] speaks of bending the will of the targeted state ("expression of a state's consent") through

[39] *See ibidem*, comment on p. 316.

[40] Its precise content is somewhat foggy and disputed (Sander, *supra* note 1, p. 21) and must thus be deduced from sources working with it on a case-by-case basis.

[41] "Article 52 Coercion of a State by the threat or use of force: 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." For a contribution focusing on Art. 52 VCLT and its effects upon peace treaties, *see e.g.* K. Urbanová, *Potential Peace Treaty Solution for the Ukraine Conflict and its Validity under International Law*, 44 Polish Yearbook of International Law 49 (2024).

[42] Vienna Convention on the Law of Treaties (adopted 22 May 1969, entered into force 27 January 1980), 1155 UNTS 331.

[43] Annex to the UNGA Resolution of 24 October 1970, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, Doc. A/RES/2625(XXV), p. 123.

[44] Ohlin, *supra* note 6, p. 73.

[45] Para. 98 of the Dissenting opinion of Judge Schwebel to ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Rep 1986.

[46] Schmitt, Vihul, *supra* note 28, p. 317.

[47] "Article 51 Coercion of a representative of a State: The expression of a State's consent to be bound by a treaty which has been procured by the coercion of its representative through acts or threats directed against him shall be without any legal effect."

subjugation of free will of its representative when performing governmental functions. While it is obviously possible to imagine that a state coerces another state's private individual inhabitant and such action may even violate international law norms, such as human rights, the element of coercion in such a situation will not be necessarily related to the will of the state of nationality of the coerced individual. That turns out to be one of the crucial points as will be seen in the next section.

And this point hits the crucial issue of applicability of non-intervention to CETICs. As the next section highlights, during these operations, the direct target is not the state itself, but its electorate (in order to compel it – deprive of free will – to vote differently than they otherwise would and hence deprive the state of its free will regarding populating its organs). For that reason, the next section includes an analysis upon this issue.

Another matter that might be problematic for the next section is whether, in order to fulfil the element of coercion, its consequences must materialize or not? Should they be required to materialize, a failed CETIC would be outside of the regulation in any case. However, requiring materialization of coercion to allow for the applicability of the principle of non-intervention would be too radical. It would paradoxically exclude the principle's protection from those that would manage to resist the coercion, even at high stakes. Thus, all that is necessary is to coerce, not to be successful in it.[48] For that reason, the next section does not discuss this issue extensively.

Before delving specifically into interpreting the elements of non-intervention in relation to CETICs, it is also necessary to confirm the applicability of the principle to cyberspace and activities conducted therein. Without such confirmation, combined with the fact the CETICs by definition take place in cyberspace, any subsequent discussion would be without merit.

The applicability of rules of international law in cyberspace is debated for several decades already. For example, the famous Tallinn Manual series[49] represent a large doctrinal work focusing among others on the international peace and security rules, including the principle of non-intervention. Neither states nor intergovernmental organizations stayed away and convened six Groups of Governmental Experts (GGEs)[50] and two Open-ended Working Groups (OEWGs).[51] Both GGEs and

[48] Schmitt, Vihul, *supra* note 28, p. 322.

[49] There are currently 2 Tallinn Manuals completed with third being worked upon. *See Webpage*, NATO Cooperative Cyber Defence Centre of Excellence, available at: https://ccdcoe.org/research/tallinn-manual/ (accessed 30 June 2025).

[50] *See Webpage*, United Nations, available at: https://disarmament.unoda.org/group-of-governmental-experts/ (accessed 30 June 2025). The sixth GGE (2019-2021) submitted the UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 14 July 2021, A/76/135, available at: https://docs.un.org/en/A/76/135 (accessed 30 June 2025). The report is accompanied by the 2021 Compendium.

[51] The first OEWG (Open-ended working group on developments in the field of information and telecommunications in the context of international security – *Open-ended Working Group*, United Nations,

OEWGs operated under the auspices of the United Nations and either focused or touched upon the issue of application of international law to cyberspace.

Crucially for applicability of the principle of non-intervention to CETICs, it may be summarized that both states and a majority of authors of the doctrine do not see it questionable whether international law applies to cyberspace or not, it simply does.[52] And that obviously including the principle of non-intervention.[53]

There remains however hesitation as to whether the principle as it currently is needs any update or is applicable in cyberspace without changes. The nature of cyberspace[54] complicates the matter because activities within cyberspace have a naturally foggy transboundary character while the principle of territoriality is strongly embedded in many rules of international law, particularly the rules of international peace and security like the principle of non-intervention.[55] The focus of this article is however on CETICs that are an activity of one state that attempts to[56] succeed in coercion of another state. In such situation, the extraterritorial aspect is clearly fulfilled and thus the unclear borders of jurisdictions of states in cyberspace do not present a problem. It must be admitted though that it is an interesting topic worth addressing in further research.

Based on this section, three particular issues may be identified as problematic for the research question, all of them related to coercion. Firstly, in order to be applicable to CETICs (inherently nonforcible action), the principle of non-intervention must also cover both forcible and non-forcible coercion. Secondly, the possibility of indirectness (e.g. through an electorate instead of the state directly) of non-forcible coercion remains to be confirmed. And thirdly, it might also be claimed that online campaigns may be "only" participation in discussions rather

available at: https://disarmament.unoda.org/open-ended-working-group/ (accessed 30 June 2025) already submitted final report. The work of the second OEWG (*Open-ended Working Group on security of and in the use of information and communications technologies*, United Nations, available at: https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021 (accessed 30 June 2025) is currently in progress.

[52] *See e.g.* statements in the 2021 Compendium of representatives of Australia (p. 3), Brazil (p. 17), Estonia (p. 23), Germany (p. 31), Japan (p. 46), the Netherlands (p. 55), Norway (pp. 65 and 66), Romania (p. 75), Singapore (p. 82), or Switzerland (p. 86).

[53] Explicitly stated e.g. by representatives of Estonia (p. 25), the Netherlands (p. 55), Singapore (p. 83), and Switzerland (p. 88) in the 2021 Compendium. Also see rule 66 of the Schmitt, Vihul, *supra* note 28.

[54] For example, defined on p. 12 of the Schmitt, Vihul, *supra* note 28 by three components – physical, logical and social.

[55] For example, the ICJ claimed that "[t]he effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of non-intervention." ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Rep 1986, para. 251.

[56] Attempt is considered in this article to be an operation that was conducted but did not succeed in its goals (changing the elections results). As coercion does not need to be successful for the principle of non-intervention to be violated, this difference is legally insignificant.

than coercion – claiming it does not have the capacity to remove the free will of the individual voters.

Consequently, the following section, after dealing with *domaine réservé*, addresses these three issues identified above specifically.

3. SUITABILITY OF THE PRINCIPLE OF NON-INTERVENTION TO REGULATE CETICS

This section is divided according to the elements of the principle of non-intervention and elaborates upon them in connection with the CETICs, focusing particularly on the above-noted problematic issues.

3.1. Domaine réservé

Holding elections and announcing their results are without a doubt matters that fit within the core of *domaine réservé* of each state.[57] As a fundamental mechanism of populating democratic state's organs, elections are considered an essential aspect of political system, and it should be stressed that "[e]very State possesses a fundamental right to choose and implement its own political [... system]."[58]

Thus, this element is fulfilled in the case of CETICs. Nonetheless, a point highlighted in connection with coercion – the matter of its indirectness – needs to be addressed here as well due to their interplay. An argument against the conclusion that CETICs affect the *domaine réservé* might be that the target is not the state itself but rather its population. To answer such hypothetical argument from the perspective of *domaine réservé*, it should be stressed that

> [i]ntervention into the *domaine réservé* of a State need not be directed at State infrastructure or involve State activities. Rather, the key to satisfaction of this first element of intervention is that the act in question must be designed to undermine the State's authority over the *domaine reserve*.[59]

Because there is no doubt that holding and properly administering elections are matters of sovereign authority of each state, interference within them undermining such authority must be considered as negatively affecting the *domaine réservé*. From the perspective of the CETICs, the element of *domaine réservé* is fulfilled.[60]

---

[57] As confirmed e.g. in the statement of representative of Brazil on p. 19 to the 2021 Compendium.

[58] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para. 258.

[59] Schmitt, Vihul, *supra* note 28, p. 315 (rule 66).

[60] Obviously, there are other aspects that need to be taken into account in a comprehensive assessment of any cyber campaign. Particularly the matter of the attributability of such campaign. For debates on

3.2. Coercion

In the previous sections, the element of coercion has been identified as problematic to the suitability of the principle of non-intervention to CETICs with regard to particularly three topics. They are thus dealt with individually in the following text and recommendations contained in the sub-sections are reflected in section 4.

3.2.1. Coercion only via threat or use of force (forcible) or also by other means (non-forcible)?

An issue that may present a problem is understating of the material contents of coercion. In general, coercion might be understood as limited to a physical act of violence or threat of it that leads to a change in the target's behaviour. On the interstate level, that analogy would be fulfilled by a use of force or threat of use of force (as confirmed by the ICJ). Such limited understanding might be seemingly supported by Art. 52 VCLT. And should the understanding of coercion be limited to forcible traits, non-intervention would have no potential to regulate CETICs. The reason would rest in the fact that there is no physical compulsion, or its threat imposed upon that electorate or the targeted state itself. CETICs are conducted cybernetically and nonforcibly.

Coercion is however not limited to the means of imposing physical (military) force or its threats.[61] Even Art. 51 VCLT itself accepts a possibility of coercion through others acts, although not enumerated. While not every nonforcible measure will be coercive, it does not automatically mean that every coercion has to be physical, violent, or military in the interstate context.[62] Coercion may in fact take various forms, the use of force and its threats including, but also encompassing economic or diplomatic coercion.[63] Also, the conclusion that cyber tampering operations constitute a violation of non-intervention confirms that coercion does not necessarily need to be forcible. Cyber tampering operations are also nonforcible.

From the perspective of this point, there would be no problem in the application of the non-intervention principle to CETICs, yet it needed to be made taking into account the fact that the ICJ was not clear upon the issue yet as discussed above.

3.2.2. Indirectness of coercion

Similar to the perspective of *domaine réservé*, the indirect nature of nonforcible coercion poses a problem. Cyber tampering operations (consisting of hacking another state's counting systems and changing the casted ballots or already counted

attributability of activities within cyberspace, *see e.g.* N. Tsagourias, M. Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31(3) European Journal of International Law 941 (2020).

[61] Explicitly stated in 2021 Compendium by the representative of Germany (p. 34).

[62] *See e.g.* Ohlin, *supra* note 6, p. 78.

[63] Delerue, *supra* note 26, pp. 237.

results in the system) must be assessed differently from CETICs. Since in the former, coercion would surely be established[64] due to its direct nature,[65] such action would constitute a violation of the principle of non-intervention.[66] The targeted state is directly coerced into establishing another result of its elections.

In case of CETICs, the targeted state is not coerced *directly*, however. The campaign is focused at its population with the intent of changing its political views / opinions in order to make them decide differently when casting the ballots. The desired result might be the same – the outcome of the elections being different. Nonetheless, the indirectness of nonforcible coercion presents a challenge to the applicability of the principle of non-intervention.

In order to find out to what extent can nonforcible coercion be indirect, it is possible to get inspired by the previous case law of the ICJ. In context of indirect nonforcible intervention, the ICJ has excluded economic pressure, such as imposition of embargoes and withdrawal of economic aid, from the notion of intervention.[67] By doing so, it may seem that it excluded indirect nonforcible coercion from the elements of the principle of non-intervention as such.[68] Such a conclusion would similarly exclude CETICs targeting the population of another state with the intention of changing elections results due to the indirectness of such nonforcible action. However, the ICJ's conclusion should not be overstated.

Firstly, the Court was extremely brief in the statement and did not elaborate upon it in more than one sentence.[69] Secondly, it can hardly be stated that there is

[64] Since coercion is fulfilled when the targeted state is deprived of free will to establish election results and thus of populating its representative political bodies according to its own will.

[65] Because in such operations, the acting state itself directly acts and changes the results.

[66] Schmitt, Vihul, *supra* note 28, p. 313. See also expressions of state representatives in the 2021 Compendium (e.g. Australia, p. 5); on p. 69, the Norwegian representative went as far as to claim that violation of non-intervention could be even committed by "cyber operations with the intent of altering election results in another State, for example by [...] unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak')". The text does not however relate such violation to indirect coercion. It may be (though not stated so explicitly either) that it rather relates to exercising governmental powers within another state's jurisdiction without its consent. It is similarly not clear how to interpret the US position on p. 140: "a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."

[67] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para. 245. While the Court did not elaborate on it in detail, the reason may rest in the indirectness of the activity as well as refusal of states to accept economic pressure as intervention.

[68] Especially considering that unlike in case of economic pressure, the Court found indirect forcible coercion via providing "support for subversive or terrorist armed activities within another State" as both violation of the prohibition of use of force and the principle of non-intervention (*ibidem*, para. 205).

[69] As opposed to the ICJ, the authors of the Tallinn Manual 2.0 on one hand agreed that economic measures do not generally amount to intervention, but they also acknowledged view distinguishing two situations. First one involves free choice of trading partners (no intervention generally established by it); the second different scenario however "involve[s] active technical measures, rather than simply desisting from trade" (Schmitt, Vihul, *supra* note 28, p. 324).

a consensus upon the exclusion of every possible economic measure to be outside of the scope of coercion.[70] Afterall, even the Friendly Relations Declaration counts with economic measures when referring to coercion by stating that "[n]o 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 rights and to secure from it advantages of any kind [highlighting added]."[71] And last but not least, when it comes to intervention, rather than indirectness or directness of coercion, it may be that "[t]he key is that the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take)."[72] Thus, it is not that easy to exclude indirect nonforcible coercion consisting of economic (or any other) pressure from the principle of non-intervention. In fact, there is a lot to conclude positively. And the conclusion similarly applies to indirect coercion via CETICs.

Furthermore, even if the controversial nature of the economical character of coercion is taken into account, such measures should be distinguished from pressure upon the fundamental processes of the constitutional order of a target state. Those are not matters related to free economic choices, i.e., an issue that arguably is behind the opposition to economic pressure being qualified as coercion.

Consequently, based on the requirements of international law, a CETIC designed to produce a different outcome in a process of filling political positions (such as elections) may not be automatically excluded from the notion of coercion; despite it being imposed indirectly and nonforcibly. As long as there is a sufficiently close casual nexus[73] between the campaign and the possibly different outcome of

[70] "Although there might not be customary law norms against economic coercion generally, some argue that specific forms of economic coercion might be illegal. Unless the countries involved have specific treaty commitments between them, the arguments for illegality would be based upon interpretations of the principles of the prohibition of intervention, and the prohibition of the use of force, as noted above and as found in the UN Charter" (B.E. Carter, *Economic Coercion*, in: *Max Planck Encyclopedia of Public International Law*, available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1518 (accessed 30 June 2025)).

[71] UNGA Resolution of 24 October 1970, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, Doc. A/RES/2625(XXV), p. 123.

[72] Schmitt, Vihul, *supra* note 28, p. 319.

[73] The requirement of causality and whether the causal nexus between effect and coercion must be direct or not was addressed by majority of the Tallinn Manual experts positively when they agreed that even an indirect causal nexus suffices (*ibidem,* p. 320). Such conclusion makes sense, especially considering the fact that the effect does not even need to materialize (intervention be successful) in order for the violation of non-intervention to occur. Thus, demanding strict application of direct causal nexus would run against the logic of the principle.

an election, the element as it is defined in international law now, may be in fact considered fulfilled.

However, it must be accepted that such conclusions are rather theoretical, and practice and opinions of states do not actively confirm it yet. The conclusion is rather that the law as it exists, does not contravene the conclusion. It remains necessary for states to explicitly support this understanding of coercion in order to guarantee the applicability of the rule to CETICs. Thus, the need to confirm the possibility of indirectness of nonforcible coercion is reflected in the first recommendation contained in the next section.

Additionally, while effectivity of CETICs in changing opinions is notoriously hard to prove, fulfilling the element of coercion does not require its success. Consequently, the ambiguity regarding success of the campaigns is not an obstacle in fulfilling the element of coercion.[74]

3.2.3. Coercion or deception?

The last identified problematic cluster of aspects of the suitability of the principle of non-intervention to CETICs relates to the difference between discussion and deception and whether the latter may qualify as coercion while the former may not. The issue was brought up by Jens D. Ohlin who stated when commenting upon the Russian campaign preceding the 2016 US elections as follows: "True, the Russians sought to influence the outcome of the election and moreover they did so with deception. But deception is not the same thing as coercion."[75]

In other words, even if coercion can be indirect and nonforcible, the question remains whether influencing public opinion (and then elections results) is anything more than just a debate or propaganda (i.e., not coercive because debate does not remove free will of the target) as opposed to coercing a certain result. The outcome of accepting that deception is noncoercive would be that CETICs would not fulfil the criterion of coercion. Ohlin further points out, that "legal requirement of coercion [...] tracks the methods used"[76] rather than the result it brings or may bring. Together with the distinction from deception, that is another key in this argument. Because this article submits that deceptive actions may indeed be coercive, it needs to tackle the counterarguments raised and the following text first addresses the latter one.

Regarding the issue of coercion being defined by methods used, the question is whether fulfilling the element of coercion rest in the methods (as Ohlin put it)

[74] In any way, measuring the possible effects of CETICs will heavily depend on technical capabilities and availability of data from for example social media (through so-called data mining) where the operations took place.

[75] Ohlin, *supra* note 6, p. 82.

[76] *Ibidem*, p. 83.

or whether the key is rather that it simply "must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take)"[77] regardless of the method that was applied – in fact the argument raised above and accepted by the author of this article. Ohlin tends to the methods, the result being that he disqualifies CETICs from coerciveness.

While the argument has certain merits, it does not corelate with the opinions of some states. For example, the German representative contributed to the 2021 Compendium by stating that "cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts [highlighting removed]."[78] Thus, instead methods used, the focus is on the results and their scale and effects. Similarly, Steven J. Barela suggests that scale and reach of an operation should be the defining concepts when considering whether an operation is coercive or not.[79] Thus, it is suggested here (and in the second recommendation stated in the next section), that instead of methods, it should be the scale and effects[80] of operation that define it as coercive. Once again, the conclusion however needs stronger confirmation by state practice and opinions and that is why it is included in the second recommendation in next section.

The other key to Ohlin's argument is the distinction between coercion and deception. And it must be admitted again that the argument is persuasive, nonetheless not completely bulletproof. It is suggested here that the deceptive nature of CETICs is actually an element that helps to understand them as coercive as opposed to campaigns with a clear source.

Elections are a tool for democratic states to populate their political and some other constitutional organs. Thus, democratic states decide who will be their representatives by elections. By intervening into the electorate's decision-making process, the interfering state attempts to compel the target state to respect someone else as its representative than it otherwise would. And what makes this operation different from "mere" propaganda is exactly its covert nature. If the source was clear, the electorate would understand that the reason behind the information might be an attempt to manipulate. But when the operation is of a covert nature (for example through the use of social media profiles pretending to be local citizens

[77] Schmitt, Vihul, *supra* note 28, p. 319.

[78] 2021 Compendium, p. 34.

[79] S.J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, Just Security, 29 March 2018, available at: https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law/ (accessed 30 June 2025).

[80] With respect to effects, it must be noted that it should rather be defined as 'expected effects' or the operation's *reach* because coercion does not need to materialize, as it was stated above, and yet prohibited intervention may occur.

and/or organizations), the information coming from the operation only seems to stem from those who have the right to decide/elect rather than from a foreign state. The targeted electorate may consequently consider such information as legitimate contributions to public debate rather than an attempt to manipulate them and change whom they will vote.

It might be legitimately stated that in operations like these that occurred, it was exactly

> the covert nature of the troll operation [that] deprive[d the] electorate of its freedom of choice by creating a situation in which it could not fairly evaluate the information it was being provided. As the voters were unaware that they were being manipulated by a foreign power, their decision making, and thus their ability to control their governance, was weakened and distorted. The deceptive nature of the trolling is what distinguishes it from a mere influence operation.[81]

In conclusion, the deceptive nature of the operation might be in fact understood as exactly the point that shifts CETICs towards coercion (regarding populating the target's organs). One might ask what else other than coercion is an operation that changes the target state's decision whom to choose as its representative?[82]

But again, it must be admitted that even this conclusion is theoretical, not yet confirmed by widespread practice and opinions, and it would be beneficial if the suggested interpretation of the element of coercion was confirmed by states. Hence, it is reflected in third recommendation in the next section.

One of the most approximate opinions that were publicly pronounced by representatives of states in this direction, is the one by the German representative in the 2021 Compendium:

> 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 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.[83]

---

[81] Schmitt, *supra* note 3, p. 51.

[82] In this regard, the understanding of coercive means expressed by Australia is particularly indicating: "Coercive means are those that effectively deprive or are intended to deprive the State of the ability to control, decide upon or govern matters of an inherently sovereign nature" (2021 Compendium, p. 5).

[83] *Ibidem*, p. 35.

Thereby, in the last part of the quoted paragraph above, the representative went as far as to accept that cyber operations leading to large portions of electorate not participating in the elections may be coercive, thus possibly fulfilling the elements of non-intervention. Whether the same would be accepted if the voters participated but voted differently, is however another matter and would also benefit from explanation by states.

4. LAW MAKING RECOMMENDATIONS

Taking into account three facts:

a. that even states discuss the principle of non-intervention as belonging among the most approximate rules of international law with the potential to regulate CETICs,
b. that interpretation of the elements of the principle contains significant shortcomings indicated above with regard its applicability to CETICs, and
c. that the number of CETICs keeps rising and states perceive them negatively and thus its international law-based regulation is desirable,

this section is dedicated to pointing out aspects of the principle of non-intervention that the interpretation and application of which would need to be updated to secure the suitability of the principle to CETICs. Thus, the following points may also be viewed as a sort of law-making recommendations that if followed would help to clarify the principle as a suitable option to regulate the CETICs. They are divided into five points, the first three being based upon the partial conclusions contained in previous section, and the last two serving as a confirmation of the interpretation of the principle specifically to CETICs.

As a preliminary matter, it should be stated that it would be beneficial if more states made their positions regarding their understanding of the principle public. The number of state representatives that expressed their views publicly remains limited.[84]

Thus, in those statements (as well as in practice), should states wish to reach a situation when the principle of non-intervention is applicable to CETICs, it would be beneficial if they (among others) in relation to the principle of non-intervention:

a. explicitly confirmed that the causal nexus between coercion and the desired effect may be indirect,
b. clarified that rather than methods used, the scale and reach of cyber operations are what defines them as coercive,
c. distinguished between overt state newsfeed and covert information operations that hide their source. The latter having the potential to be coercive due to its hidden nature,

[84] For example, only 15 states have publicly explained their positions in the 2021 Compendium.

d. explicitly confirmed that not only cyber tampering operations but also hack and release and information operations targeting electorate of another state in order to compel it to vote differently than they otherwise would, have the potential to coerce the target state and to violate the principle of non-intervention, and
e. invoked international responsibility of the intervening states in dispute settlement mechanisms for even CETICs.

To conclude the recommendations, it is clear that current international law has yet to keep up (at least from the perspective of the principle of non-intervention) with reality. While some may claim that adopting an international treaty that would encompass regulation of the CETICs via among others the principle of non-intervention would help to clarify the matter, it is submitted here that until customary international law is clarified satisfactorily in that regard, such a treaty would have small chances of success and might in fact prevent further development of customary law.

However, it should be kept in mind that this desired (at least by author of this article) applicability of the principle of non-intervention to CETICs is only one part of the large-scale discussions regarding the effects of dynamic changes upon the international community, caused by rapid technological development.

And so, it is commendable that states have commenced addressing the issue in the GGEs and OEWGs, as well as in other fora. One might only hope that this development will not be halted by the current state of international relations and the law will eventually catch with reality in this regard.

CONCLUSIONS

The article focuses on the issue of suitability of the principle of non-intervention to regulate cyber electorate targeting information operations, i.e., operations through which one state targets the electorate of another state before or during elections in the latter with the intent of changing the elections results.

Since the principle of non-intervention crystallized in pre-cyber age, the article identifies its "shortcomings" in this respect and suggests an "update" or clarification that states might consider in their practice and opinions, should they wish to secure the applicability of the principle to the operations in question.

The final conclusion may be summarized as follows: the principle's elements are not applied and interpreted in a way that would inherently prevent the applicability of the rule to CETICs. Nonetheless, in order to allow for it, it would still need to be clarified so that the law would positively reflect all elements needed for the applicability. These *clarifications* primarily concern the element of coercion that

is unsatisfactorily (or not in manner widespread and uniform enough) interpreted and applied in this regard in current international law. They include the need for an explicit confirmation that the causal nexus between nonforcible coercion and its desired effect may be indirect; that rather than methods used, the scale and reach of cyber operations are what defines them as coercive; and the confirmation of a distinction between overt state actions and covert information operations that hide their source.