**Sheffield Centre for International and European Law**

School of Law

**Working Paper Series**

**Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace**

**Professor Nicholas Tsagourias**

 **2019/1**

**Forthcoming in:**

**Dennis Broeders and Bibi van den Berg, *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield, 2020)**

SCIEL builds on a long and distinguished tradition of international and European legal scholarship at the University of Sheffield School of Law. Research in the Centre focuses on the international and European aspects of legal issues, and more broadly draws on the School’s strengths in many forms of International, European and Comparative Law to consider the wider implications of current problems and the function of law in a globalised world. As part of this mission, the Centre publishes the present Working Paper Series.

General Editor, Professor Nicholas Tsagourias

Editor in Chief, Daniel Franchini

Managing Editor, Fiona Davies

Please visit [www.sheffield.ac.uk/law/sciel](http://www.sheffield.ac.uk/law/sciel) for more information about the Centre or follow us on Twitter @lawsheffield

The full Working Paper Series is available at

https://www.sheffield.ac.uk/law/research/centres-and-institutes/sciel/research

 © The Authors, 2019. This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Cite as: N. Tsagourias, ‘Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace’ (Forthcoming 2020); SCIEL Working Paper Series No 2019/1

**Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace**

**Nicholas Tsagourias\***

**Abstract**

*This chapter examines the application of the principle of non-intervention to electoral cyber interference. In the first place it discusses how the traditional definition of intervention can apply to such interference and identifies the normative and regulatory gaps that arise. For this reason, it proceeds to contextualise and reconceptualise the meaning of intervention in cyberspace and then applies this new definition to electoral cyber interference such as the interference into the 2016 US elections. Its main argument is that the baseline of intervention is control over choices whereas the function of the principle of non-intervention is to protect the principle of self-determination interpreted as the free construction of a state’s authority and will. Thus, external cyber interference amounting to control over the cognitive environment within which such authority and will are formed violates the principle of non-intervention.*

1. **Introduction**

It is by now accepted that International law applies to cyberspace. The 2013 Report of the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (GGE) affirmed that international law, especially the UN Charter, applies to cyberspace and that State sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to jurisdiction over ICT infrastructure within a state’s territory.[[1]](#footnote-1) The 2015 GGE Report went a step further by spelling out specific international norms and principles that apply or should apply to cyberspace. Among the international law principles that apply to cyberspace are the principle of state sovereignty and the principle of non-intervention in the internal affairs of other states. [[2]](#footnote-2) In the same vein, states have affirmed the application of international law and of the principle of non-intervention to cyberspace. According to China, ‘[c]ountries

shouldn’t use ICTs to interfere in other countries’ internal affairs and undermine other countries’ political, economic, and social stability as well as cultural environment’.[[3]](#footnote-3)

Notwithstanding such strong assertions, how international law or, more specifically, how the principle of non-intervention applies to cyberspace and to cyber operations is beset by uncertainty. According to the former Legal Advisor to the State Department, Brian Egan, ‘States need to do more work to clarify how the international law on non-intervention applies to States’ activities in cyberspace’.[[4]](#footnote-4) This state of affairs came to a head with regard to the Russian cyber interference in the 2016 US presidential election. Russia’s toolkit of electoral interference consisted of disinformation and ‘hack and leak’ operations.[[5]](#footnote-5) Views concerning the legal characterisation of Russia’s actions vary; from assertions that they violated the principle of non-intervention to assertions that they did not violate at all this principle.[[6]](#footnote-6) The US incident is not the only example of electoral cyber interference; other incidents involve elections in the Netherlands, the UK, France or Germany to name just a few.[[7]](#footnote-7) Although electoral interference is not a new phenomenon, cyberspace increases the scalability, reach, and effects of such interference and poses a serious threat to a state’s sovereign authority.

Against this background, this chapter examines the question of how the principle of non-intervention can be contextualised and reconceptualised in cyberspace in order to provide a normative framework according to which operations of electoral cyber interference are to be assessed and in order for the principle of non-intervention to attain its purpose of protecting a state’s sovereign authority. I will do this by explaining the values the principle of non-intervention protects with self-determination being one such value and by identifying the baseline of intervention and the pathways intervention can take in cyberspace and explain how they can impinge on the right to self-determination and consequently on non-intervention. It is hoped that by reconceptualising the concept of intervention for cyber purposes, its regulatory scope and effectiveness will be enhanced since cyberspace is linked to the political, economic, military, diplomatic, social, cultural functions of a state and is a domain within which or through which states operate, interact and exert power.

The chapter proceeds in the following manner. In the next section I explain the content and meaning of the principle of non-intervention as traditionally formulated in international law and then in the third section apply this definition to Russia’s interference in the 2016 US election. Because of the identified normative and regulatory gaps, in the fourth section I contextualise and reconceptualise the principle of non-intervention by exposing its relationship with the principle of self-determination, define the baseline of intervention as control and then explain the different pathways it can take in cyberspace. In the fifth section I apply this concept to electoral cyber interference such as the interference into the 2016 US election. The conclusion sets out the chapter’s overall findings.

1. **The principle of non-intervention**

Non-intervention is a fundamental principle of international law that has acquired customary law status even if it is not mentioned in the UN Charter.[[8]](#footnote-8) According to the 1965 General Assembly Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty which was repeated almost verbatim in the 1970 General Assembly Declaration on Friendly Relations: ‘No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.’[[9]](#footnote-9) In the *Nicaragua* case, the ICJ defined

non-intervention as ‘the right of every sovereign State to conduct its [external or internal] affairs without outside interference’.[[10]](#footnote-10)

The importance of the principle of non-intervention derives from the fact that it emanates from and protects essential aspects of the principle of state sovereignty.[[11]](#footnote-11) Sovereignty as the foundational principle of the modern international system is an all-embracing principle and can be dissected into more specific principles or rules that protect specific aspects of state sovereignty. The principle of non-intervention protects the integrity and autonomy of a state’s authority and will in the sense of its capacity to internal and external self-governance.[[12]](#footnote-12) Understood in this way, the principle of non-intervention creates a juridical space where the government as the holder of authority and will can exercise freely its will and make free choices in view also of the fact that in international law the state is represented by the government. Because it protects an essential aspect of state sovereignty, the principle of non-intervention acquired independent legal status and it is critical in an international system defined by sovereignty and by interactions between sovereign states. Its alignment however with the principle of sovereignty has important normative and operational implications in that the scope and content of the principle of non-intervention is moulded by the meaning and content of the principle of sovereignty as developed in international law and relations.

In order to define the content and meaning of the principle of non-intervention in international law, we need to explain the meaning of its opposite that is, intervention. According to Oppenheim’s definition, intervention is interference ‘forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question’.[[13]](#footnote-13) The ICJ in the *Nicaragua* case defined prohibited intervention as ‘one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely … and uses methods of coercion in regard to such choices, which must remain free ones’.[[14]](#footnote-14) From the above definitions, it transpires that in order for interference to constitute intervention it should satisfy two conditions: first, it should impinge on matters that fall within a state’s sovereign prerogative and, secondly, it should be coercive.

The first describes the domain within which interference should take place as well as the object of such interference. In this respect the ICJ mentioned the choice of political, economic, social and cultural system and the formulation of foreign policy.[[15]](#footnote-15) In other words the domain is the political, economic, social and cultural system and the object is the ability to make free choices in these domains. This list is not exhaustive and can change in light of related developments concerning the meaning and scope of state sovereignty.[[16]](#footnote-16) As a result, the domain protected from intervention may expand or decrease, something that will affect the scope of the non-intervention principle.

The second condition – coercion – refers to the nature of the interference and is what differentiates intervention from pure interference or influence. As the ICJ said, ‘the element of coercion … defines, and indeed forms the very essence of, [a] prohibited intervention’.[[17]](#footnote-17) Traditionally, coercion in international law has been taken to imply compulsion whereby one state compels or attempts to compel another state to take a particular course of action against its will thus obtaining in the words of the 1970 Friendly Relations Declaration ‘the subordination of the exercise of its sovereign rights’.[[18]](#footnote-18)

Such a construction of intervention can very well apply to cyberspace. For instance, if a state’s governmental services are targeted by a DDoS attack in order to compel its government to change its policies or decisions, this would amount to prohibited intervention. The 2007 DDoS attacks against Estonia come immediately to mind. They were launched after the Estonian government decided to relocate a Soviet era statue, a decision that was resisted by the country’s Russian speaking minority and was frowned upon by Moscow. To the extent that they were intended to put such pressure on Estonia to change its decision and provided that they were attributed to Russia[[19]](#footnote-19), in my opinion, they would constitute prohibited intervention.[[20]](#footnote-20) In contrast, the 2014 Sony attack – where a hacker group believed to be linked to North Korea hacked Sony Pictures Entertainment and leaked personal data of its employees as well information about unreleased films[[21]](#footnote-21) – does not amount to intervention because the target of the attack was a private company not connected to the US government and it did not involve a matter that falls within the sovereign prerogatives of the US neither was any attempt to coerce the US government to take a particular course of action.

1. **Interference into the 2016 US election and the principle of non-intervention**

How would the above-mentioned construction of intervention apply to Russia’s interference in the 2016 US presidential election? Russian operations included hacking into the Democratic National Committee emails and the release of confidential information as well as disinformation operations.[[22]](#footnote-22) The former is referred to as doxing[[23]](#footnote-23) whose objective is to ‘expose, disgrace, or otherwise undermine a particular individual, campaign, or organisation in order to influence public opinion during an election cycle’[[24]](#footnote-24) whereas disinformation is the dissemination of ‘false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit’ and can threaten the ‘democratic political processes and value’.[[25]](#footnote-25) The Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint statement claiming that the Russian government was responsible for the hack and publication of the materials in its attempt to ‘interfere with the US election process’[[26]](#footnote-26) and according to ODNI*,* the intention of the leaks was to ‘undermine public faith in the US democratic process, denigrate Secretary Clinton and harm her electability and

potential presidency’.[[27]](#footnote-27) Following investigations a number of Russian operatives were indicted. According to the Mueller indictment ‘[t]he conspiracy had as its object impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable the Defendants to interfere with U.S. political and electoral processes, including the 2016 U.S. presidential election.’[[28]](#footnote-28)

One can plausibly say that Russia’s actions satisfied the first condition of unlawful intervention by targeting the conduct of elections. As the ICJ opined in the *Nicaragua* case the ‘choice of political system’ is a matter falling within a state’s sovereign prerogatives which should remain ‘free from external intervention’[[29]](#footnote-29) and went on to say that holding elections is a domestic matter.[[30]](#footnote-30) There are problems however with the second condition namely, that of coercion. According to Brian Egan, ‘a cyber operation by a State that interferes with another State’s ability to hold an election or that manipulates a State’s election results would be a clear violation of the rule of non-intervention’.[[31]](#footnote-31) Likewise, according to the former UK Attorney General, ‘the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state … must surely be a breach of the prohibition on intervention in the domestic affairs of states.’[[32]](#footnote-32) These statements concentrate on interference with the electoral administration, for example, interference with electoral registers to delete voters’ names as well as on interference with the electoral infrastructure, for example, interference with the recording or counting of votes or the blocking of voting machines cancelling thus an election. Since Russia’s operations, according to the aforementioned reports[[33]](#footnote-33), did not amount to such interference, they do not breach the non- intervention norm.

That said, since then many states designated the electoral infrastructure (registration, casting and counting votes, submitting and tallying results) as critical national infrastructure.[[34]](#footnote-34) In the same vein, the Global Commission on the Stability of Cyberspace (GCSC) proposed a norm prohibiting the disruption of

elections through cyber attacks on the technical infrastructure that supports elections.[[35]](#footnote-35) Although these are important developments, they only address one aspect of the phenomenon of electoral cyber interference that is, meddling with the electoral infrastructure but do not extend to the process according to which the will of the people is formed and how intervention can impact on them. Yet infrastructure is integral to the whole process and outcomes can be affected not only by interfering with the electoral infrastructure but also by interfering with the process. This is an issue that will be discussed in the next section.

**IV. Contextualising and reconceptualising intervention in cyberspace**

In this section I revisit the phenomenon of intervention in order to contextualise and reconceptualise the principle of non-intervention as applied in cyberspace. This is necessary for many reasons. In the first place, as was said earlier, cyberspace is a new domain but one that is embedded in the political and legal environment where states operate. States thus use cyberspace as a conduit of power and indeed as a conduit of intervention by employing not only the traditional diplomatic, political, military, or economic tools of coercion but also new tools suitable to cyberspace. Second, because of the particular features of cyberspace such as its interconnectedness and anonymity, the pathways of coercion can diversify whereas its scalability, reach and effects enhanced.[[36]](#footnote-36) Third, it is the very nature of the concept of intervention that invites reassessment. Intervention is not a static concept but a concept that is constantly contextualised in time or domain and whose meaning, scope and practice changes accordingly. What intervention signified in the 19th century is not the same today, neither is the meaning of military, diplomatic, political or legal intervention the same. It is for these reasons that the concept of intervention needs to be contextualised and reconceptualised for cyber purposes and in what follows I will do this by first explaining the intimate relationship between non-intervention and self-

determination hence repositioning the domain and object of intervention and, secondly, by reassessing the baseline of coercion and by explaining the pathways coercion can take in cyberspace and how they impact on self-determination and consequently on the principle of non-intervention.

With regard to the first issue, it was said in section I that intervention acquires meaning within a configuration of sovereign relations by protecting the integrity and autonomy of a state’s authority and will against external interference. As was also explained, the domain protected from intervention consists of the state’s sovereign prerogatives whereas the object of intervention is the ability to make free choices on these matters. This traditional reading of intervention focuses on the internal and/or external manifestation of authority and will by the state represented by the government; it vests in other words all sovereign authority and will in the government which is then protected from intervention but does not take into account how this authority and will are formed and how intervention can impact on the process of their formation. Instead, it treats the state and its government as if they were cut off from the prior process of authority and will formation. However, that process of authority and will formation is connected with the internal and external manifestations of such authority and will by the government. To explain, a government’s authority and will remains free only when its sourcing is also free. This immediately brings to light the relationship between non-intervention and self-determination[[37]](#footnote-37), another principle that derives from and protects the principle of state sovereignty. Self-determination refers to the right of peoples to determine freely and without external interference their political status and to pursue freely their economic, social and cultural development.[[38]](#footnote-38)

From this definition it transpires that the scope of the right to self-determination is broader and is not exclusively linked to the right of peoples to form their own state. Moreover it does not cease once a state has been created but thereafter self-determination refers to the ‘right to authentic self-government, that is, the right of a people really and freely to choose its own political and economic regime’.[[39]](#footnote-39) It follows from this that the principle of non-intervention protects against external interference the expression of authority and will by the people and also protects the conditions that

enable the people to form authority and will freely and make free choices.[[40]](#footnote-40) External interference for example through disinformation combined with identity falsification[[41]](#footnote-41) distorts, undermines or inverses this process and nullifies the genuine expression of authority and will by the people. It also taints the internal or external manifestations or expressions of authority and will of the government that emerge. For this reason, in the words of Crawford ‘the principle of self-determination is represented by the rule against intervention in the internal affairs of that state.’[[42]](#footnote-42)

By aligning the principles of non-intervention and self-determination, the normative and operational scope of the principle of non-intervention shifts. More specifically, the domain and object of intervention shifts from the power holder, the government, to the people and to the process of forming authority and will, for example, the electoral process, through which the goal of free choice is attained. The government as the depository of such authority and will and its carrier is protected by the principle of non-intervention but it is not the primary object of protection as the traditional reading hold but a derivative one; the primary is the people and the process.

Regarding coercion, there has been little consideration of the threshold or the baseline of coercion above which intervention takes place. Oppenheim’s definition is however quite instructive. According to him, the essence of coercion is the fact that a state intervened against is in effect deprived of control over a matter. The baseline of coercion then is control. Control means one state’s intentional direction *over* another state’s authority and will which prevents the latter from discharging its authority and will freely and make free choices. When a state assumes control over a matter at the expense of the state which has a legitimate claim of authority and will over that matter because it falls within its sovereign prerogatives, it effectively curtails the latter’s capacity to self-determination and self-governance which as was said are protected by the principle of non-intervention. It inverses these values by forcing the state to act counterintuitively to what its free authority and will would advocate.[[43]](#footnote-43)

Regarding the pathways to coercion or the means and methods through which coercion can be actualised, the ICJ spoke of ‘methods’ of coercion in plural and also spoke of direct and indirect methods. This means that there is a spectrum of coercion as control which can manifest itself through various

means and methods. In the first place, coercion, as Oppenheim noted, can be forcible. In the *Nicaragua case* the ICJ said that one of the most obvious forms of coercion is the one that 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.[[44]](#footnote-44) In this case, the intervened against state loses control over a matter, for example over parts of its territory, through the use of armed force. Forcible coercion is direct and perhaps the most dramatic and serious form of coercion and for this reason it acquired its own legal meaning and status in the rule prohibiting the use of force contained in Article 2(4) of the UN Charter and in customary law.

Another pathway to coercion mentioned by Oppenheim is that of dictatorial interference. Dictatorial interference is when a state prescribes a course of action in imperative terms and usually by threatening negative consequences, forcing thus the will of the recipient state. This is again a direct form of coercion and describes a situation where two sovereign ‘wills’ clash over a matter and one state loses control over a matter by subordinating its will.

In addition to these direct pathways, there are also other more subtle or indirect pathways to coercion where one state extends its will over another and thus assumes control even if the latter state appears to behave freely. This can happen when the intervening state arranges the targeted state’s choices in such a way that it has no effective choice. Another instance is when the intervenor, through manipulation, arranges the other state’s preferences in such a way that the state acts in accordance with the intervenor’s preferred choices. In these cases coercion as control does not appear to be conflictual since the victim state apparently acts voluntarily but the intervenor exerts control over the other and extends its will by rearranging the available choices or by rearranging preferences to align them with its own. For example, if a state assumes control over another state’s governmental systems (or systems supporting critical national infrastructure) such as its national defence command and control system and manipulates their logistics operations, this would amount to coercion if the systems operate counterintuitively to how they were programmed to operate by the victim state and produce actions and effects tailored to meet the interests of the intervener. Also, when a state, through cyber espionage, acquires information on another state’s policies

which is then used to direct the choices of the victim state, it controls the latter’s choices against its wishes.[[45]](#footnote-45)

**Electoral cyber interference and intervention**

Where coercion as control can manifest itself more acutely is when a state’s authority and will are manipulated at its source; in the process of their formation. When a state interferes with the structures but also with the environment that condition and facilitate the formation of authority and will by the people and substitutes the legitimate process of self-determination with an artificially constructed process in order to generate particular attitudes, and results to serve its particular interests,[[46]](#footnote-46) the intervening state controls not only the attitudes, will and choices of the people but also the will of the government that emerges. Consequently, the right to self-determination and self-governance which is protected by the non-intervention principle is essentially curtailed.

Cyberspace provides a facilitative ecosystem where this can take place but, as was said, it can also enhance the scalability, reach and effects of coercion. The interference into the 2016 US elections is a case in point. As was said, Russian operations included the hacking and release of confidential information and social-media enabled disinformation. The primary target of such operations was the process of authority and will formation by the people and more specifically the cognitive environment which enables the making of choices which are subsequently reflected in the type of government that emerges from the process.[[47]](#footnote-47) As the former F.B.I. director James Comey said before the Senate Intelligence Committee:‘[t]his is such a big deal, … we have this big, messy, wonderful country where … nobody tells us what to think, what to fight about, what to vote for, except other Americans .… But we’re

talking about a foreign government that, using technical intrusion, lots of other methods, tried to shape the way we think, we vote, we act.’[[48]](#footnote-48) In similar vein, the 2017 US National Security Strategy opined that ‘[a] democracy is only as resilient as its people. An informed and engaged citizenry is the fundamental requirement for a free and resilient nation. … Today, actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies. Adversaries target media, political processes, financial networks, and personal data.’ [[49]](#footnote-49)

From the preceding discussion it can be said that Russia’s interference met the two conditions of unlawful intervention; it impinged on sovereign prerogatives in a coercive manner. Although one could have stopped here, it is important to consider two other issues which are discussed in the literature but whose status has not been firmly settled. The first is intention and more specifically whether coercion should be intentional. The Tallinn Manual treats intent as a constitutive element of the principle of non-intervention[[50]](#footnote-50) but there are also dissenting voices who treat intervention as an objective state of affairs.[[51]](#footnote-51) That said, if as was said previously intervention is relational and contextual, it can never be an objective state of affairs. It is for this reason that in the opinion of the present writer intent is critical, particularly in cyberspace, where operations are often factually indistinguishable and their effects permeate borders unintentionally. Moreover, without intent the release of non-public information of public interest will be treated as unlawful intervention because it may lead to changes in governmental policy.

It seems that the ICJ in the *Nicaragua case* required intent when it said that ‘in international law, if one State, *with a view to* the coercion of another State, supports and assists armed bands in that State whose purpose is to overthrow the government of that State, that amounts to an intervention by the one State in the internal affairs of the other, whether or not the political objective of the State giving such support and assistance is equally far-reaching.’[[52]](#footnote-52) What the Court meant is that a state should have the intention to coerce another state by using proxies although it may not share the particular objective of the proxies it is supporting.

That having been said, it should be conceded that it is difficult to establish intent. There may exist some factual and demonstrable evidence to prove intent for example in the form of statements or the involvement of state operatives,[[53]](#footnote-53) otherwise intent can be constructed from circumstantial evidence and from surrounding circumstances. For example, the means used, the target of the operation,[[54]](#footnote-54) the level of disinformation, the covert nature of the operation, the political and ideological competition that exists between states, the strategic or other interests served by the operation, the timing of the operation, the intensity and widespread nature of the operation[[55]](#footnote-55) can all be taken into account to prove intent. With regard to the latter, no analytical tool exists to measure the real impact of electoral interference on people or how their voting preferences were affected but analysis of social networks can reveal the number of viewers or artificial movements and to some extent measure the number of affected individuals.[[56]](#footnote-56) In any case, it should be recalled that coercion does not need to materialise in order to be caught by the non-intervention principle. If such evidence is taken into account when assessing intent, it can support a claim that Russia’s operations were intentional.

The second condition is that of knowledge in the sense of whether the victim state should be aware of the coercion. Certain commentators contend that knowledge is not required whereas others claim that it is required because a state cannot be coerced when it is unaware of the act of coercion.[[57]](#footnote-57) In international relations theory (which views coercion as an instrument of power and usually identifies it with threats[[58]](#footnote-58)), knowledge of the threat and of its author is important because it relates to the persuasiveness and credibility of the threat. For this reason, some international relations commentators view cyber coercion as inconsequential because of the covert nature of cyber operations.[[59]](#footnote-59)

The difference however between international law and international relations is that the latter takes a functional approach to intervention whereas international law takes a normative approach. It is thus submitted that knowledge is not a constitutive element of intervention but knowledge is required in order to trigger a claim that intervention has taken place. This also means that the fact that intervention

may be covert or that it was attempted without actually succeeding will not affect the qualification of the impugned behaviour as intervention for international law purposes when the intervened against state becomes aware of the situation, provided of course that the criteria of intervention have been satisfied. To put it differently, the intervening state cannot claim that there was no intervention or that there is no breach of the non-intervention rule because at the time intervention happened the victim state was not aware of the intervention. This also means that the victim state is not prevented from taking countermeasures after acquiring knowledge of the intervention even if the act of intervention occurred much earlier because there will be temporal proximity between the countermeasures and the claim of wrongfulness. In the US case, the fact that subsequent reports established the facts will not prevent the US form claiming that it was victim of unlawful intervention although whether it will do so is a matter of politics.

**Conclusion**

This chapter has shown that cyberspace is a new domain where the principle of non-intervention can apply. However, deciphering its content and understanding how it applies to cyberspace is a difficult exercise that can impact on its effectiveness to regulate cyber activities. Consequently, reassessing the meaning of intervention in the cyber domain is critical because cyberspace is a domain where states compete and exert power and it is an environment which increases the scalability, reach and effects of intervention.

For this reason, in this chapter I contextualised and reconceptualised the principle of non-intervention for cyber purposes. More specifically I aligned the principle of non-intervention with that of self-determination and argued that non-intervention protects not just the integrity and autonomy of a state’s authority and will as it manifests itself internally and externally through the government but primarily it protects its source, the people, and the process of according to which authority and will are formed. I then identified the baseline of coercion as control over a matter that falls within a state’s sovereign prerogatives and applied this definition to cyberspace by looking into the different ways control – and, therefore, coercion – manifests itself. In relation to electoral interference, it manifests itself as control over the conditions that enable the exercise of self-determination by the people in the sense of freely forming authority and will which subsequently extends to control over the manifestation and expression of such authority and will by the government.

By reassessing what the principle of non-intervention entails in the cyber era, international law will be able to fill many normative and operational gaps that currently exist when it is called upon to apply to cyber operations. The implications of such reconceptualization are not limited to cyber but extend to the concept of intervention in general which, as was said, is a dynamic concept that requires constant re-evaluation. However, it should be admitted that this is not the end of the road because it is for states to take up the mantle and provide normative and operational clarity as to the meaning of intervention in cyberspace and, more broadly, in the physical world. Yet, even if agreement on the meaning of cyber intervention is attained, intervention will still be a controversial concept because there is disagreement as to which interventions are lawful or unlawful but justified. For example, is electoral cyber interference to prevent a racist group from taking power or a cyber campaign to overthrow a dictatorial regime lawful or at least justified? To the extent that these issues have not been settled in international law, intervention and non-intervention will remain a Jekyll and Hyde concept even in the cyber context. That having been said, this is a second order enquiry because the first order enquiry is ontological; it is about the meaning of intervention to which this chapter attempted to provide an answer.

1. \*Professor of International Law, University of Sheffield (nicholas.tsagourias@sheffield.ac.uk).

 UNGA, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, 24 June 2013, UN Doc A/68/98, paras. 19-20. [↑](#footnote-ref-1)
2. UNGA, “Group of Governmental Experts on Developments in the Field of Information and
Telecommunications in the Context of International Security”, 22 July 2015, UN Doc A/70/174, para 26. [↑](#footnote-ref-2)
3. PRC Permanent Mission to the UN, ‘Statement by Ms. Liu Ying of the Chinese Delegation at the Thematic Debate on Information and Cyber Security at the First Committee of the 68th Session of the UNGA’ (30.10.2013) [www.china-un.org/eng/hyyfy/t1094491.htm](http://www.china-un.org/eng/hyyfy/t1094491.htm) [↑](#footnote-ref-3)
4. BJ Egan, ‘International Law and Stability in Cyberspace’, 35 *Berkeley JIL* (2017), 169, 175. In the same vein, the UK A-G said ‘The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space’ UK AG Cyber and International Law in the 21st Century <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [↑](#footnote-ref-4)
5. #  Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution’ in ICA, “Assessing Russian Activities and Intentions in Recent US Elections”, ICA 2017-01 (6 January 2017) p. 1, available at: <https://www.dni.gov/files/documents/ICA_2017_01.pdf> Methods of Foreign Electoral Interference, 2 April 2019 https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/

 [↑](#footnote-ref-5)
6. Sean Watts, *International Law and Proposed U.S. Responses to the DNC Hack,* JUST SEC. (Oct.
14, 2016); Duncan Hollis, *Russia and the DNC Hack: What Future for a Duty of NonIntervention?* OPINIO JURIS (July 25, 2016); Jens David Ohlin, ‘Did Russian Cyberinterference in the 2016 Election Violate International Law?’ 95 *Texas Law Review* (2017), 1579 [↑](#footnote-ref-6)
7. Erik Brattberg and Tim Maurer, Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, May 23, 2018 <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435> Laura Galante and Shaun Ee, Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents Atlantic Council, September, 2018 <https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf> ]

### Sebastian Bay, Guna Šnore , Protecting elections: a strategic communications approach NATO STRATCOM COE Riga, June 2019 [https://www.stratcomcoe.org/download/file/fid/80396](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwix_bOPw8DjAhWVSxUIHRLrDicQFjAFegQIAhAC&url=https%3A%2F%2Fwww.stratcomcoe.org%2Fdownload%2Ffile%2Ffid%2F80396&usg=AOvVaw13s14p-TaWOWVUUeQhpfTX)

 [↑](#footnote-ref-7)
8. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 para 202 [hereinafter referred to as *Nicaragua Case*]. See Maziar Jamnejad and Michael Wood, *The Principle of Non-Intervention in International Law*, 22 Leiden J. Int’l L. 345, 347–67 (2009) [↑](#footnote-ref-8)
9. G.A. Res. 2131 (XX), annex, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (*Dec.21, 1965), para 1; G.A. Res. 2625 (XXV), annex, *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the United Nations* (Oct. 24, 1970): ‘No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.’ [↑](#footnote-ref-9)
10. *Nicaragua Case,* para 202. [↑](#footnote-ref-10)
11. R. Y. Jennings and A. D. Watts, *Oppenheim’s International Law*, 9th edn, (Oxford: Oxford University Press, 1992), 428; A/5746 para 216; John Vincent, Non-intervention and International Order (New Jersey: Princeton University Press, 1974), 14 [↑](#footnote-ref-11)
12. *Nicaragua Case*, para 202 [↑](#footnote-ref-12)
13. *Oppenheim’s International Law*, supra, 428; Philip Kunig, “Prohibition of Intervention,” *Max Planck Encyclopedia of Public International Law,* para 1 [↑](#footnote-ref-13)
14. *Nicaragua* *Case,* para 205 [↑](#footnote-ref-14)
15. *Nicaragua* *Case,* para 205. [↑](#footnote-ref-15)
16. *Oppenheim’s International Law*, supra, 428. [↑](#footnote-ref-16)
17. *Nicaragua* *Case,* para 205. [↑](#footnote-ref-17)
18. G.A. Res. 2625 (XXV), supra. See also Christopher C Joyner, ‘Coercion’ in Max Planck Encyclopedia of Public International Law [MPEPIL]: ‘Coercion in inter-State relations involves the government of one [State](https://opil-ouplaw-com.sheffield.idm.oclc.org/view/10.1093/law%3Aepil/9780199231690/law-9780199231690-e1749?rskey=rbspGr&result=1&prd=EPIL) compelling the government of another State to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force’. [↑](#footnote-ref-18)
19. For attribution see Nicholas Tsagourias, ‘Cyber Attacks, Self-defence and the Problem of Attribution’, 2012 17 Journal of Conflict Security Law 229, [↑](#footnote-ref-19)
20. Nicholas Tsagourias, ‘The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II – The Use of Force’ 15 *Yearbook of International Humanitarian Law*, 2012 19–43, 35; Russell Buchan, ‘Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?’(2012)17 Journal of
Conflict & Security Law 211. [↑](#footnote-ref-20)
21. Sony Got Hacked Hard: What We Know and Don't Know So Far 12.03.14 <https://www.wired.com/2014/12/sony-hack-what-we-know/> [↑](#footnote-ref-21)
22. Ibid, 2-5 [↑](#footnote-ref-22)
23. #  See Ido Kilovaty, ‘Doxfare: Politically Motivated Leaks and the Future of the Norm on NonIntervention in the Era of Weaponized Information’, 9 Harvard National SecurityJournal (2018), 152. For similar activities during the 2018 elections in Cambodia see [Scott Henderson](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/scott-henderson), [Steve Miller](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/cap-steve-miller), [Dan Perez](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/dan-perez), [Marcin Siedlarz](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/marcin-siedlarz), [Ben Wilson](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/ben-wilson), [Ben Read](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/ben-read) ‘Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally’ July 10, 2018 <https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html>

 [↑](#footnote-ref-23)
24. #  EU vs Disinfo Methods of Foreign Electoral Interference <https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/>

 [↑](#footnote-ref-24)
25. European Commission, *A Multi-Dimensional Approach to Disinformation, Report of the
Independent High Level Group on Fake News and Online Disinformation*, March 2018, p. 10. According to the EU vs Disinfo disinformation is ‘The fabrication or deliberate distortion of news content aimed at deceiving an audience, polluting the information space to obscure fact-based reality, and manufacturing misleading narratives about key events or issues to manipulate public opinion. Disinformation is the most persistent and widespread form of the Kremlin’s interference efforts. Importantly, it is not limited only to election cycles, but has now become a viral feature of our information ecosystem’ and is objective is ‘To paralyse the democratic process by fuelling social fragmentation and polarisation, sowing confusion and uncertainty about fact-based reality, and undermining trust in the integrity of democratic politics and institutions’. <https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/> Others speak of “information manipulation” encompassing three criteria: a coordinated campaign ,the diffusion of false information or information that is consciously distorted, and the political intention to cause harm’ See B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, 21 [↑](#footnote-ref-25)
26. Director of National Intelligence, “Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security” (7 October 2016), available at: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> [↑](#footnote-ref-26)
27. ‘Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution’ in ICA, “Assessing Russian Activities and Intentions in Recent US Elections”, ICA 2017-01 (6 January 2017) p. 1, available at: <https://www.dni.gov/files/documents/ICA_2017_01.pdf> [↑](#footnote-ref-27)
28. Indictment, United States v. Internet Research Agency LLC et al., No. 1:18-cr-00032, 2018 WL 914777,
(D.D.C. Feb. 16, 2018), para 25 and Indictment, United States v. Victor Borisovich Netyksho et al., Case 1:18-cr-00215-ABJ (July 13, 2018); para 28 <https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf> [↑](#footnote-ref-28)
29. *Nicaragua Case* para 205 [↑](#footnote-ref-29)
30. *Nicaragua Case* paras 257-9 [↑](#footnote-ref-30)
31. BJ Egan, International Law and Stability in Cyberspace, supra, 175 [↑](#footnote-ref-31)
32. UK A-G, supra, [↑](#footnote-ref-32)
33. ODNI, 3 [↑](#footnote-ref-33)
34. <https://www.dhs.gov/topic/election-security> [↑](#footnote-ref-34)
35. ####  <https://cyberstability.org/research/global-commission-urges-protecting-electoral-infrastructure/> See also UK, National Security Capability Review (March 2018) 34:

#### <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf>. For Sweden see National Strategy for Society Information and Cyber Security (June 2018), 6-7: <https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213>. Sean Kanuck, [Protecting the Electoral Process and its Institutions](https://cyberstability.org/research/gcsc-thought-piece-protecting-the-electoral-process-and-its-institutions/) (January 2018), <https://cyberstability.org/research/>

 [↑](#footnote-ref-35)
36. For example the ODNI report says that Russia’s actions ‘represented a significant escalation in directness, level of activity and scope of effort’, supra, 5 [↑](#footnote-ref-36)
37. Jens David Ohlin, ‘Did Russian Cyber interference in the 2016 Election Violate International Law?’ 95 *Texas Law Review* (2017), 1579. A/5746 para 216 [↑](#footnote-ref-37)
38. Article 1(1), International Covenant on Civil and Political Rights 1966; 1970 Friendly Relations Declaration [↑](#footnote-ref-38)
39. Antonio Cassese, *Self-Determination of Peoples: A Legal Reappraisal* (Cambridge: Cambridge
University Press, 1995), 137; Patrick Thornberry, "The Democratic or Internal Aspect
of Self-Determination with Some Remarks on Federalism" in Christian Tomuschat (ed), *Modern Law of Self-Determination,* (Dordrecht, Boston and London: Martinus Nijhoff, 1992), 101 [↑](#footnote-ref-39)
40. According to art 21(3) UDHR ‘[t]he will of the people shall be the basis of the
authority of government.’ [↑](#footnote-ref-40)
41. Jens David Ohlin Election Interference: The Real Harm and The Only SolutionCornell Law School research paper No. 18-50 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3276940> [↑](#footnote-ref-41)
42. J. Crawford*, The Creation of States in International Law, (*Oxford, Oxford University Press, 2007), 127 [↑](#footnote-ref-42)
43. Rosenau for example speaks about a sharp break with conventional patterns of behaviour. J. Rosenau, ‘Intervention as a scientific concept’ (1969) 13 *Journal of Conflict Resolution* 149, 162-3 [↑](#footnote-ref-43)
44. Nicaragua Case, para 205 [↑](#footnote-ref-44)
45. ##  For cyber espionage see also Russell Buchan, [*Cyber Espionage and International Law*](https://www.bloomsburycollections.com/book/cyber-espionage-and-international-law)*,* (Hart, 2018), 48-69

 [↑](#footnote-ref-45)
46. According to Rosenau intervention is addressed to ‘the authority structure of the target society-that is, to the identity of those who make the decisions that are bind- ing for the entire society and/or to the processes through which such decisions are made. New foreign policy initiatives designed to modify the behavior of voters abroad are thus likely to be regarded as interventionary even though equally extensive efforts to modify the behavior of tourists in the same country are not’. J. Rosenau, ‘Intervention as a scientific concept’ (1969) 13 *Journal of Conflict Resolution* 149, 163; Myres S. McDougal & Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War* 67 *Yale LJ* (1958), 771, 793: ‘The use of the ideological instrument commonly involves the selective manipulation and circulation of symbols, verbal or nonverbal, calculated to alter the patterns of identifications, demands and expectations of mass audiences in the target-state and thereby to induce or stimulate politically significant attitudes and behavior favorable to the initiator-state’. Contra see Hollis, 41 [↑](#footnote-ref-46)
47. Duncan Hollis, The Influence of War; The War for Influence, 32 Temple Journal
of International & Comparative Law (2018), 31, at 36; Herbert Lin and Jaclyn
Kerr,On Cyber-Enabled Information/Influence Warfare and Manipulation,
(2017), <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cyber-enabled_influence_warfare-ssrn-v1.pdf> [↑](#footnote-ref-47)
48. *Full Transcript and Video: James Comey’s Testimony on Capitol Hill*, N.Y.Times (June 8, 2017), <https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html> [↑](#footnote-ref-48)
49. *National Security Strategy of the United States of America*, December 2017, p. 14 <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> [↑](#footnote-ref-49)
50. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS
(Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0], Rule 66, para 27 [↑](#footnote-ref-50)
51. *See* Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention, in* Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 268-9 (OUP, 2015) [↑](#footnote-ref-51)
52. *Nicaragua Case* para 241 [↑](#footnote-ref-52)
53. See for example the ODNI report and the Muller indictment mentioned above [↑](#footnote-ref-53)
54. According to the ODNI report, the target was the Democratic candidate. Also ‘Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign’, supra, 3; Mueller Indictment, supra, para 2 [↑](#footnote-ref-54)
55. Mueller’s indictment for example reveals the systematic and widespread nature of Russian activities. [↑](#footnote-ref-55)
56. Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly & Camille François, “The IRA, Social Media and Political Polarization in the United States, 2012-2018.” Working Paper 2018.2. Oxford, UK which provides data about the activities of the Russia’s Internet Research Agency [↑](#footnote-ref-56)
57. Tallinn Manual 2.0 Rule 66, para 25 [↑](#footnote-ref-57)
58. Greenhil, Kelly M. and Peter Krause, eds.,Coercion The Power to Hurt in International Politics. New York, N.Y.: Oxford University Press, 2018 [↑](#footnote-ref-58)
59. Lindsay, Jon R., and Erik Gartzke. 2014. “Coercion Through Cyberspace: The Stability-Instability Paradox Revisited.” In Kelly M. Greenhill and Peter J. Krause (eds), *Coercion: The Power to Hurt in International Politics* (Oxford 2018), 179 [↑](#footnote-ref-59)