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

Nicholas Tsagourias

Cite as: Tsagourias, Nicholas. 2020. "Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 45-63. London: Rowman & Littlefield International.

Chapter 3

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

Nicholas Tsagourias

It is by now accepted that international law applies to cyberspace. The 2013 Report of the United Nations Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security 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 Information and Communication Technology (ICT)-related activities, and to jurisdiction over ICT infrastructure within a state's territory (U.N. General Assembly 2013, paras 19–20). 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 (U.N. General Assembly 2015, para. 26). 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" (P. R. C. Permanent Mission to the U.N. 2013).

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 adviser 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" (Egan 2017, 175).[1] 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 (U.S. ODNI 2017, 1; EU vs Disinfo 2019). Views concerning the legal characterization of Russia's actions vary and although commentators invoked the principle of non-intervention, the majority concluded that Russia's actions did not fulfill its conditions in particular that of coercion (Hollis 2016; Ohlin 2016; Watts 2016). The US incident is not the only example of electoral cyber interference; other incidents involve elections in the Netherlands, the United Kingdom, France, and Germany to name just a few (Brattberg and Maurer 2018; Galante and Ee 2018; Bay and Šnore 2019).[2] 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 contextualized and reconceptualized in cyberspace in order to attain its purpose of protecting a state's sovereign authority in cases of electoral cyber interference. I will do this by aligning the principle of non-intervention with the principle of self-determination and by identifying the baseline of intervention and the pathways intervention can take in cyberspace. By reassessing the concept of intervention, its regulatory scope and effectiveness in cyberspace will be enhanced since cyberspace is linked to the political, economic, military, diplomatic, social, and 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 interpreted in international law and in the third section I will 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 expose the relationship between the principle of non-intervention and that of self-determination, define the baseline of intervention as control, and explain the different pathways intervention can take in cyberspace. In the fifth section, I apply this concept to electoral cyber interference such as the interference in the 2016 US election. The conclusion sets out the chapter's overall findings and explains the importance of reassessing the meaning of intervention in the cyber context and more generally.

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 (*Nicaragua Case* 1986, para 202; Jamnejad and Wood 2009, 347–367).[3] 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" (U.N. General Assembly Res. 1965, Annex, para. 1).[4] 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."[5]

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 (Jennings and Watts 1992, 428; Vincent 1974, 14; U.N. General Assembly 1964, para. 216). 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.[6] 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 its will freely and make free choices in view 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 molded 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" (Jennings and Watts 1992, 428).[7] 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."[8] 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 affairs and, second, it should be coercive.

The first condition 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 systems and the formulation of foreign policy.[9] It thus transpires that the protected domain is a state's political, economic, social, and cultural system whereas the object of intervention is the ability to make free choices in this domain. That said, the aforementioned list is not exhaustive and can change in light of related developments concerning the meaning and scope of state sovereignty (Jennings and Watts 1992, 428). 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."[10] 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" (U.N. General Assembly Friendly Relations Declaration 1970).[11]

Such a construction of intervention can very well apply to cyberspace. For instance, if a state's governmental services are targeted by a Distributed Denial of Service (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,[12] in my opinion, they would constitute prohibited intervention (Tsagourias 2012, 35; Buchan 2012). In contrast, the 2014 Sony attack (Zetter 2014) 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 United States nor was there any attempt to coerce the US government to take a particular course of action.

INTERFERENCE IN THE 2016 US ELECTION AND THE PRINCIPLE OF NON-INTERVENTION

How would the abovementioned construction of intervention apply to Russia's interference in the 2016 US presidential election? Russian operations

included hacking into the Democratic National Committee e-mails and the release of confidential information as well as disinformation operations (U.S. ODNI 2017, 2-5). The former is referred to as doxing (Kilovaty 2018, 152) 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" (EU vs Disinfo 2019) 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" (European Commission 2018, 10).[13] 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 the publication of the materials in an attempt to "interfere with the US election process" (U.S. DHS and ODNI 2016) 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" (U.S. ODNI 2017, ii). 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" (Mueller Indictments 2018).[14]

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"[15] and went on to say that holding elections is a domestic matter.[16] 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" (Egan 2017, 175). 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" (U.K. Attorney General's Office 2018). These statements refer to 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 thus cancelling an election. Since Russia's operations, according to the aforementioned reports (U.S.

ODNI 2017, 3), did not amount to such interference, they do not breach the non-intervention norm.

That said, many states since then have designated their electoral infrastructure (registration, casting and counting votes, submitting and tallying results) as critical national infrastructure (U.S. DHS "Election Security").[17] In the same vein, the Global Commission on the Stability of Cyberspace (GCSC) proposed a norm prohibiting the disruption of elections through cyberattacks on the technical infrastructure that supports elections (GCSC 2018).[18] 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, outcomes can be affected not only by interfering with the electoral infrastructure but also by interfering with the process of will formation. This is an issue that will be discussed in the next section.

CONTEXTUALIZING AND RECONCEPTUALIZING INTERVENTION IN CYBERSPACE

In this section, I revisit the phenomenon of intervention in order to contextualize and reconceptualize the principle of non-intervention for cyber purposes. This is necessary for many reasons. In the first place and 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 the scalability, reach, and effects of intervention enhanced.[19] Third, the very nature of the concept of intervention invites such reassessment. Intervention is not a static concept but a concept that is constantly contextualized in time or domain and whose meaning, scope, and practice changes accordingly. What intervention signified in the nineteenth century is not the same today, neither is the meaning of military, diplomatic, political, or legal intervention. It is for these reasons that the concept of intervention needs to be contextualized and reconceptualized 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.

Non-intervention and Self-Determination

With regard to the first issue, it was said in the first section 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 manifestation of such authority and will by the government. To explain, a government's authority and will remain free only when its sourcing is also free. This immediately brings to light the relationship between non-intervention and self-determination (Ohlin 2016; U.N. General Assembly 1964, para. 216), 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 (U.N. General Assembly ICCPR 1966, article 1(1); U.N. General Assembly 1970).

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" (Cassese 1995, 137).[20] 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.[21] External interference through disinformation combined with identity falsification, for example, distorts, undermines, or inverses this process and nullifies the genuine expression of authority and will by the people (Ohlin 2018). It also taints the internal or external manifestation or expression of authority and will by the government that emerges. 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" (Crawford 2007, 127).

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 government to the actual power holder, the people, and to the process of forming authority and will through which the goal of free choice is also attained. Whereas the government as the depository of such authority and will is protected by the principle of non-intervention, it is not the primary object of protection as the traditional reading holds, but a derivative one; the primary object of protection are the people and the process of authority and will formation.

Control as the Baseline of Coercion and the Pathways of Coercion

Having identified the domain and object of protection by the principle of non-intervention, I will now consider its second element, that of coercion. In international law, 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. 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 making 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 as 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.[22]

Regarding the pathways to coercion, or the means and methods through which coercion can be actualized, the ICJ spoke of "methods" of coercion in the plural and also spoke of direct and indirect methods. This means that there is a spectrum of coercion 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.[23] 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) and manipulates their operation, this would amount to coercion to the extent that the systems operate counterintuitively to how they were programed to operate by the victim state and produce actions and effects desired by 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.[24]

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. To explain, when a state interferes with the structures and 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,[25] 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 as self-governance which is protected by the non-intervention principle is essentially curtailed. Take, for example, the case of deep fakes when, during an electoral campaign, imageries, voices, or videos of politicians are simulated in order to

discredit them. To the extent that such operations are designed and executed in such a way as to manipulate the cognitive process where authority and will are formed and to take control over peoples' choices of government, they would constitute intervention.

As the aforementioned example shows, cyberspace provides a facilitative ecosystem where electoral interference can take place and as was said, it can also enhance its scalability, reach, and effects of coercion. To explain, cyberspace has made it easier to produce, disseminate, and share disinformation, enhances its accessibility by amplifying the circle of targeted audiences or by micro-targeting, increases the immediacy and speed of such operations, complicates attribution, and allows for remotely conducted operations.

The interference in 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 cognitive environment which enables the making of choices that are subsequently reflected in the type of government that emerges from the process (Hollis 2018, 36; Lin and Kerr 2017). As James Comey, the former FBI director, 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" (New York Times 2017). In a 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" (U.S. White House 2017, p. 14).

From the preceding discussion, it can be said that Russia's interference met the two conditions of unlawful intervention. Although one could have stopped here, it is important to consider a number of other issues which should be present although their status has not been firmly settled in legal doctrine.

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 (Schmitt 2017, Rule 66, para. 27), but there are also dissenting voices who treat intervention as an objective state of affairs (Watts 2015, 249, 268–269). If, as was said previously, intervention is relational and contextual, it can never be an objective state of affairs. 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."[26] 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.

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, intent distinguishes influence operations or in general propaganda from operations that are purposively designed to exert control over a sovereign matter (self-determination) through false, fabricated, misleading, or generally through disinformation.

That having been said, it should be acknowledged that it is difficult to establish intent. There may exist some factual and demonstrable evidence to prove intent in the form of statements or the involvement of state operatives (U.S. ODNI 2017; Mueller Indictments 2018), otherwise intent can be constructed from circumstantial evidence and from surrounding circumstances. For example, the target of the operation[27] and the means used (disinformation) are important indicators (U.S. ODNI 2017, 3; Mueller Indictments, para. 2). With regard to the latter, one can look into whether the confidentiality, integrity, or availability of information has been breached (Herpig, Schuetze and Jones 2018, 14ff). For example, in the case of deep fakes or leaked e-mails, it is the authenticity, integrity, and confidentiality of the disseminated information that is breached but even in the case of true information, it is its integrity and authenticity that is encroached if it is mixed with false information or is presented in a false or fabricated context or if it relates to partial truths. Other factors to take into account to establish intent are 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. With regard to the latter, the Mueller indictment demonstrated the widespread and systematic nature of Russia's interference. [28]

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 (Schmitt 2017, Rule 66, para. 25). In international relations theory, which views coercion as an instrument of power and usually identifies it with threats, 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 (Lindsay and Gartzke [2014] 2018, 179).

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 behavior 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 United States from claiming that it was victim of unlawful intervention although whether it will do so is a matter of politics.

Finally, such interference needs to reach a certain level of severity to amount to intervention. Severity can be assessed against the importance of the values affected which in this case is the value of self-determination; the consequences of intervention which in this case is the control of a state's authority and will and, according to McDougal and Feliciano, the extent to which values are affected and the number of participants whose values are so affected.[29] Although no analytical tool exists to measure the real impact of electoral interference on people or how their voting preferences were affected, however, analysis of social networks can reveal the number of viewers or artificial movements and to some extent measure the number of affected individuals (Howard et al. 2018).[30]

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 are a difficult exercise that can impact 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 contextualized and reassessed 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 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 that 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 intervention but extend to the concept of intervention in general which, as was said, is a dynamic concept that requires constant reevaluation. 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 in democracies unlawful whereas 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.

NOTES

1. In the same vein, the UK attorney general said: "The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space" (U.K. Attorney General's Office 2018).

2. For similar activities during the 2018 elections in Cambodia, see Henderson et al. (2018).

3. 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" *Leiden Journal of International Law* 22 (2009): 345, 347–367.

4. See also: U.N. General Assembly Res., *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the United Nations*, October 24, 1970, U. N. Doc. A/RES/2625 (XXV), Annex: "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."

5. *Nicaragua Case*, para 202.

6. Ibid., para 202.

7. See also: Philip Kunig, "Prohibition of Intervention" *Max Planck Encyclopedia of Public International Law* (2012) para 1.

8. *Nicaragua Case*, para 205.

9. Ibid.

10. Ibid.

11. See also: Christopher C. Joyner, "Coercion" *Max Planck Encyclopedia of Public International Law* (2006): "Coercion in inter-State relations involves the government of one State compelling the government of another State to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force."

12. For attribution see: Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict Security Law* 17, no. 2 (2012): 229.

13. According to *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 its 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": *EU vs Disinfo*, "Methods of Foreign Electoral Interference," April 2, 2019, 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: Jean-Baptise Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina 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.

14. U.S. District Court, District of Columbia, United States v. Internet Research Agency LLC et al. (Indictment, 16 February 2018), Criminal Action No. 100032 (DLF), para 25 and United States v. Victor Borisovich Netyksho et al. (Indictment, 13 July 2018), Criminal Action No. 00215 (ABJ), para. 28 (The Mueller Indictments), https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf.

15. *Nicaragua Case*, para 205.

16. Ibid., paras 257–259.

17. U.S. Department of Homeland Security, "*Election Security*," https://www.dhs.gov/topic/election-security.

18. See also: U.K. Cabinet Office, National Security Capability Review, March 28, 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: Government Offices of Sweden, Ministry of Justice, "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, Global Commission on the Stability of Cyberspace, "Protecting the Electoral Process and its Institutions," January 2018, https://cyberstability.org/research/.

19. For example, the U.S. ODNI Report 2017, says that Russia's actions "represented a significant escalation in directness, level of activity and scope of effort."

20. See also: Patrick Thornberry, "The Democratic or Internal Aspect of Self-Determination with Some Remarks on Federalism" in *Modern Law of Self-Determination*, edited by Christian Tomuschat (Dordrecht, Boston and London: Martinus Nijhoff, 1992), 101.

21. According to Universal Declaration of Human Rights, Article 21(3): "[t]he will of the people shall be the basis of the authority of government." See: U.N. General Assembly Res., *Universal Declaration of Human Rights*, December 10, 1948, 183rd Plenary Meeting, U.N. Doc. 217A (III).

22. Rosenau, for example, speaks about a sharp break with conventional patterns of behavior. See: James N. Rosenau, "Intervention as a Scientific Concept," *Journal of Conflict Resolution* 13, no. 2 (1969): 149–171, 162–163.

23. Nicaragua Case, para 205.

24. For cyber espionage, see also: Russell Buchan, *Cyber Espionage and International Law* (Hart, 2018), 48–69.

25. 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 binding 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": Rosenau, "Intervention as a Scientific Concept," 149–171, 163; Myres S. McDougal and Florentino P. Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War," *The Yale Law Journal* 67 (1957): 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: Duncan Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32 (2018): 31, 41.

26. *Nicaragua Case*, para 241.

27. According to the ODNI Report 2017, the target was the Democratic candidate. Also, "Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign"; Mueller Indictments.

28. Mueller's indictments, for example, reveal the systematic and widespread nature of Russian activities.

29. McDougal and Feliciano, supra note 25, 782–783.

30. Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012–2018." Working Paper 2018 (University of Oxford), which provides data about the activities of the Russia's Internet Research Agency.

BIBLIOGRAPHY

Bay, Sebastian, and Guna Šnore. 2019. "Protecting Elections: A Strategic Communications Approach." *NATO Strategic Communications Centre of Excellence*, June 2019. https://www.stratcomcoe.org/download/file/fid/80396.

Brattberg, Erik, and Tim Maurer. 2018. "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.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law*, 17(2): 212–227.

Buchan, Russell. 2018. *Cyber Espionage and International Law*. Bloomsbury: Hart Publishing.

Cassese, Antonio. 1995. *Self-Determination of Peoples: A Legal Reappraisal.* Cambridge: Cambridge University Press.

Crawford, James. 2007. *The Creation of States in International Law*. Oxford: Oxford University Press.

Egan, Brian J. 2017. "International Law and Stability in Cyberspace." *Berkeley Journal of International Law*, 35(1): 169.

EU vs Disinfo. 2019. "Methods of Foreign Electoral Interference." April 2, 2019. https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/.

European Commission. 2018. "A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation." Publications Office of the European Union.

Galante, Laura, and Shaun Ee. 2018. "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." *Atlantic Council,*

Scowcroft Center for Strategy and Security, September 2018. https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf.

Global Commission on the Stability of Cyberspace. 2018. "Global Commission Urges Protecting Electoral Infrastructure." May 24, 2018. https://cyberstability.org/research/global-commission-urges-protecting-electoral-infrastructure/.

Henderson, Scott, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, Ben Read. 2018. "Chinese Espionage Group TEMP. Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally". *FireEye*, July 10, 2018. https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html.

Herpig, Sven, Julia Schuetze and Jonathan Jones. 2018. "Securing Democracy in Cyberspace, an Approach to Protecting Data-Driven Elections." October 2018. https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf.

Hollis, Duncan B. 2016. "Russia and the DNC Hack: What Future for a Duty of Non Intervention?" *Opinio Juris*, July 25, 2016. http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/.

Hollis, Duncan. 2018. "The Influence of War; The War for Influence." *Temple International and Comparative Law Journal*, 32(1): 31.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille François. 2018. "The IRA, Social Media and Political Polarization in the United States, 2012–2018." Working Paper 2018. University of Oxford.

I. C. J., Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14.

Jamnejad, Maziar, and Michael Wood. 2009. "The Principle of Non-Intervention." *Leiden Journal of International Law*, 22(2): 345–381.

Jennings, Robert Y., and Arthur D. Watts. 1992. *Oppenheim's International Law*, 9th edn. Oxford: Oxford University Press.

Joyner, Christopher C. 2006. "Coercion." *Max Planck Encyclopedia of Public International Law*. https://opil.ouplaw.com/home/mpil.

Kanuck, Sean, Global Commission on the Stability of Cyberspace. 2018. "Protecting the Electoral Process and Its Institutions." January 2018. https://cyberstability.org/research/.

Kilovaty, Ido. 2018. "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non Intervention in the Era of Weaponized Information." *Harvard National Security Journal*, 9:146.

Kunig, Philip. 2012. "Prohibition of Intervention." *Max Planck Encyclopedia of Public International Law*. https://opil.ouplaw.com/home/mpil.

Lin, Herbert., and Jaclyn Kerr. 2017. "On Cyber-Enabled Information/Influence Warfare and Manipulation." https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cyber-enabled_influence_warfare-ssrn-v1.pdf.

Lindsay, Jon R., and Erik Gartzke. 2014. "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited." In *Coercion: The Power to Hurt in International Politics.* 2018, edited by Kelly M. Greenhill and Peter J. Krause. Oxford: Oxford University Press.

McDougal, Myres S., and Florentino P. Feliciano. 1957. "International Coercion and World Public Order: The General Principles of the Law of War." *The Yale Law Journal*, 67(5): 771.

New York Times. 2017. *Full Transcript and Video: James Comey's Testimony on Capitol Hill*. *New York Times*, June 8, 2017. https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html.

Ohlin, Jens D. 2016. "Did Russian Cyber Interference in the 2016 Election Violate International Law." *Texas Law Review,* 95: 1579.

Ohlin, Jens D. 2018. "Election Interference: The Real Harm and the Only Solution." *Cornell Law School Research Paper,* No. 18–50: 1–26.

P. R. C., Permanent Mission to the U.N. 2013. *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*, October 30, 2013. www.china-un.org/eng/hyyfy/t1094491.htm.

Rosenau, James N. 1969. "Intervention as a Scientific Concept." *Journal of Conflict Resolution*, 13(2): 149–171.

Schmitt, Michael N. (ed). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edn. Cambridge: Cambridge University Press.

Sweden, Government Offices of Sweden, Ministry of Justice. 2018. "National Strategy for Society Information and Cyber Security." June 2018. https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

Thornberry, Patrick. 1992. "The Democratic or Internal Aspect of Self-Determination with Some Remarks on Federalism." In *Modern Law of Self-Determination*, edited by Christian Tomuschat. Dordrecht, Boston and London: Martinus Nijhoff.

Tsagourias, Nicholas. 2012. "Cyber attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law*, 17(2): 229–244.

Tsagourias, Nicholas. 2012. "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force." *Yearbook of International Humanitarian Law*, 15: 19–43.

U.K. Attorney General's Office. 2018. *Cyber and International Law in the 21st Century*, May 23, 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

U.K. Cabinet Office. 2018. National Security Capability Review. March 28, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

U.N. General Assembly Res. 1948. *Universal Declaration of Human Rights*, December 10, 1948, 183rd Plenary Meeting, U.N. Doc. 217A (III).

U.N. General Assembly Res. 1965. *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, December 21, 1965, U.N. Doc. A/RES/20/2131 (XX), Annex.

U.N. General Assembly Res. 1970. *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the United Nations*, October 24, 1970, U. N. Doc. A/RES/2625 (XXV), Annex.

U.N. General Assembly. 1964. *Consideration of Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations, Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States*, November 16, 1964, 19th sess., U.N. Doc. A/5746.

U.N. General Assembly. 1966. International Covenant on Civil and Political Rights "ICCPR" (Concluded December 16, 1966, entered into force March 23, 1976) 999 UNTS 171.

U.N. General Assembly. 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, June 24, 2013, 68th sess., U.N. Doc. A/68/98.

U.N. General Assembly. 2015. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 22, 2015, 17th sess., U.N. Doc. A/70/174.

U.S. Department of Homeland Security and Office of the Director of National Intelligence. 2016. "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security". DHS Press Office. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

U.S. Department of Homeland Security. "Election Security". https://www.dhs.gov/topic/election-security.

U.S. District Court, District of Columbia, United States v. Internet Research Agency LLC et al, (Indictment, February 16, 2018), Criminal Action No. 00032 (DLF) *and* United States v. Victor Borisovich Netyksho et al (Indictment, July 13, 2018), Criminal Action No 00215 (ABJ). https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf.

U.S. Office of the Director of National Intelligence. 2017. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" in *Assessing Russian Activities and Intentions in Recent US Elections*. ICA 2017–01, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

U.S., The White House. 2017. *National Security Strategy of the United States of America*. December 2017. Washington, DC. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Vilmer, J.B. Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera. 2018. "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." August 2018. Paris.

Vincent, John. 1974. *Non Intervention and International Order*. Princeton, NJ: Princeton University Press.

Watts, Sean. 2015. "Low-Intensity Cyber Operations and the Principle of Non-Intervention." In *Cyber War: Law and Ethics for Virtual Conflicts*, edited by Jens David Ohlin, Kevin Govern and Claire Finkelstein. Oxford: Oxford University Press.

Watts, Sean. 2016. "International Law and Proposed US Responses to the DNC Hack." *Just Security*, October 14, 2016. https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/.

Zetter, Kim. 2014. "Sony Got Hacked Hard: What We Know and Don't Know So Far." *Wired*, March 12, 2014. https://www.wired.com/2014/12/sony-hack-what-we-know/.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.