UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

Sovereignty in Cyberspace

A Study on Customary International Law on the Principle of Sovereignty

Master's Thesis in Public International Law

Author: Sam Safi

Course: Master Thesis, 30 higher education credits

Semester: Autumn 2019

Programme: Master of Laws, LL.M.

Department: Department of Law

Supervisor: Moa de Lucia Dahlbeck

Examiner: Andreas Moberg

Abstract

The global expansion of the internet has enabled the emergence of a relatively new theatre of inter-state conflicts; the domain of cyberspace. The emergence of cyberspace poses great challenges to the territorial understanding of the world order and raises important questions about fundamental concepts of international law. Unlike operations in the more traditional domains, i.e. land, sea, and air, cyber operations are characterised by their ability to transcend and defy international borders with ease. Consequently, the emerging conduct within cyberspace is challenging the traditional understanding of the notion of territorial sovereignty.

On the one hand, it is undisputed that the prohibition on the use of force and the principle of non-intervention apply to conduct in cyberspace. If the hacking into and manipulation of an air traffic tower's control system results in a collision between two aircrafts and ensuing loss of life, the fact that the operation is carried out by cyber means – instead of a bombardment of the air traffic tower – does not prevent it from being categorised as an unlawful use of force. On the other hand, when it comes to cyber operations that fall foul of the use of force and non-intervention thresholds – so-called low-intensity cyber operations – there is disagreement as to whether these are prohibited as a matter of law.

Against this backdrop, this thesis analyses the existence of a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. In doing so, the thesis investigates whether the principle of sovereignty in itself functions as a prohibitive primary rule of customary international law or whether it simply functions as an underlying principle from which other binding norms derive.

The thesis concludes that there currently exists a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. It also identifies and analyses the practical benefits and risks of having this rule.

Keywords: customary international law, cyberspace, sovereignty.

Acknowledgements

I want to thank my supervisor, jur.dr Moa de Lucia Dahlbeck, for her constructive and insightful comments on the many drafts during the process of writing this thesis. Your guidance and expertise have been very helpful and valuable. I also want to thank my friend Jonathan Ketto for helping me with proofreading and giving me feedback on the final draft.

Sam Safi

Gothenburg, 12 December 2019.

List of Abbreviations

DoD	Department of Defense
DRC	Democratic Republic of the Congo
GoE	Group of Experts
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
PCIJ	Permanent Court of International Justice
UNGA	United Nations General Assembly
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security
UNSC	United Nations Security Council

Table of Contents

1 Cyberspace and International Law……6

1.1 Background……....6

1.1.1 The Emergence of Cyberspace……6

1.1.2 Low-Intensity Cyber Operations and the Principle of Sovereignty……7

1.2 Purpose and Research Question…….....9

1.3 Scope of the Thesis…….....10

1.4 Preliminary Notes on Customary International Law……...11

1.4.1 Introduction……11

1.4.2 Customary International Law……11

1.4.2.1 State Practice……13

1.4.2.2 Opinio Iuris……...14

1.5 Method……15

1.6 Material……17

1.7 Outline……..19

2 The Characteristics of Cyberspace……...20

3 Use of Force, Armed Attack, and Non-Intervention……...22

3.1 Introduction……..22

3.2 The Use of Force and Armed Attack……...22

3.2.1 Use of Force……22

3.2.2 Armed Attack……24

3.3 Non-Intervention……..25

4 Rule 4 – Violation of Sovereignty……..29

4.1 Introduction……..29

4.2 Identifying the Scope of Rule 4……...29

4.2.1 The Criteria of Rule 4……29

4.2.1.1 The First Criterion – Degree of Infringement upon the Target State's Territorial Integrity……30

4.2.1.2 The Second Criterion – Interference with or Usurpation of Inherently Governmental Functions……...31

4.2.2 Are the Criteria Alternative or Cumulative? ……32

5 The Arguments For the Existence of a Primary Rule on Violations of Sovereignty in Cyberspace……..35

5.1 Introduction……..35

5.2 Evidence in State Practice and Opinio Iuris…….35

5.2.1 State Practice……..36

5.2.2 Opinio Iuris…….38

5.3 Evidence in International Judicial Decisions……...41

5.4 Evidence in International Fora……44

6 The Arguments Against the Existence of a Primary Rule on Violations of Sovereignty in Cyberspace……46

6.1 Introduction……..46

6.2 The US' Position on Sovereignty in Cyberspace……46

6.3 The UK's Position on Sovereignty in Cyberspace……...48

6.4 Evidence in International Judicial Decisions……...49

6.5 Evidence in International Fora……51

7 Analysis of Sovereignty in Cyberspace – Underlying Principle or Primary Rule?.....52

7.1 Introduction……..52

7.2 Assessing the Arguments from Chapters 5 and 6 and Analysing the Status of Sovereignty in Cyberspace……...52

7.3 Practical Benefits and Risks of a Primary Rule on Violations of Sovereignty……57

8 Closing Remarks……59

List of References……60

1 Cyberspace and International Law

1.1 Background

1.1.1 The Emergence of Cyberspace

Ever since the Westphalian peace treaty, the dominant model of the political world order and the project of international law has to a large extent been built around the idea of the nation state and its borders. Throughout history these borders have been more or less determined, primarily, by the domains of land, sea and air. With the emergence of technology and computer science, we have witnessed the genesis of a new domain: cyberspace. It is carved out not in nature but by humans, and as such it poses great challenges to the territorial understanding of the world order and it raises important questions about fundamental concepts of international law. One such concept is that of territorial sovereignty, which grants states the exclusive competence to exercise the functions of a state within its territory.[1] The concept thus has an interdependent relationship to the nation state and its borders, which are blurred in the domain of cyberspace.

In 1998, a twelve-year-old boy unknowingly hacked into the control system running Arizona's Theodore Roosevelt Dam.[2] Reportedly, the boy gained control of approximately 1 850 trillion litres of water, an amount which in theory could cover the state capital Phoenix in 1,5 metres if unleashed.[3] Two years later, in Queensland, Australia, Vitek Boden was pulled over by the police. In his car they found a computer and a radio transmitter. For a period of two months, Boden had used the equipment to hack into the control system of the drinking water and sewerage facilities. Having complete command of the system, Boden dumped large amounts of raw sewage out into parks and rivers, causing the death of wildlife and plants.[4] In 2007, a group of researchers at the US Department of Energy conducted an experimental cyber operation, involving the "hacking into a replica of a power plant's control system".[5] The researchers "chang[ed] the operating cycle of a generator. The attack sent the

[1] Shaw, Malcolm N. – International Law (Cambridge University Press, 2017), p. 363, [Shaw].

[2] Note that the veracity of the facts of this incident is disputed. The example is nonetheless mentioned in order to illustrate what cyber operations can accomplish. Harrison Dinniss, Heather – Cyber Warfare and the Laws of War (Cambridge University Press, 2012), p. 282-283. [Harrison Dinniss].

[3] Gellman, Barton – Cyber-Attacks by Al Qaeda Feared (The Washington Post, 27 June 2002), available at https://www.washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/, last visited 4 December 2019.

[4] Harrison Dinniss, *supra* note 2, p. 6, 285.

[5] Ibid., p. 6, 289.

generator out of control and ultimately caused it to self-destruct, alarming the federal government (…) about what might happen if such an attack were carried out on a larger scale".[6]

These examples are just a few of what cyber operations can accomplish. They reveal the capabilities and power of cyber operations and expose the vulnerability of societies built around critical infrastructure that can be manipulated in cyberspace.

1.1.2 Low-Intensity Cyber Operations and the Principle of Sovereignty

In order to avoid that cyberspace becomes an anarchic domain, there is a palpable need to regulate the behaviour of states within this sphere. As already mentioned, the emerging conduct within cyberspace is challenging the traditional frameworks of international law and the understanding of the notion of territorial sovereignty. Nonetheless, cyber phenomena have somehow managed to fit into existing regulation. For example, there is a consensus that the prohibition against the threat or use of force in Article 2(4) of the Charter of the United Nations is applicable to cyber operations provided that such operations cross the threshold of threat or use of force.[7] Further, it is widely accepted that cyber operations may constitute an armed attack, triggering the right to self-defence in Article 51 of the UN Charter. While not all uses of force necessarily qualify as an armed attack, cyber operations are not precluded per se.[8] Widespread agreement also exists as to the applicability of the principle of non-intervention to cyber operations.[9]

However, like any operation, a cyber operation must be of a certain intensity to qualify as either a threat or use of force, armed attack, or unlawful intervention. Far from all cyber operations reach this level of high-intensity qualification and are thus not captured by the international regulation on the use of force or unlawful intervention. In fact, the vast majority of cyber activities classify as low-intensity cyber operations. The legality of these operations is widely discussed and disputed. In other words, these low-intensity cyber operations are conducted in a sphere of legal uncertainty; a grey zone of international law.[10]

---

[6] Ibid.

[7] Schmitt, Michael N.; Vihul, Liis (eds.) – Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p. 328, [Tallinn Manual 2.0].

[8] Henriksen, Anders – International Law (Oxford University Press, 2017), p. 273.

[9] Tallinn Manual 2.0, *supra* note 7, p. 312.

[10] Ibid., p. 1, 20.

Although high-intensity cyber operations appear to be a cause for greater concern because of their potential magnitude and devastating effects, they are exceptions rather than the rule in state practice. Most cyber activities fall short of the high-intensity threshold; i.e., they do not amount to an unlawful use of force or intervention. However, their occurrence is such that states face them on almost a daily basis.[11] In spite of their frequency, the discussion of the legal status of these low-intensity cyber operations has not gained as much attention as the discussion about high-intensity operations. This apparent lack of interest has given rise to the adoption of 'Rule 4 – Violation of sovereignty' in the 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', a publication created by a group of 19 distinguished experts in international law.

The Group of Experts (GoE) sought to examine whether the well-recognised principle of sovereignty may act as a rule of customary international law prohibiting the use of low-intensity cyber operations provided that such operations reach certain qualifications. The experts unanimously concluded that customary international law indeed prohibits such operations as violations of sovereignty. They codified this prohibition in Rule 4 of the Tallinn Manual 2.0. The rule reads: "[a] State must not conduct cyber operations that violate the sovereignty of another State".[12]

Essentially, Rule 4 of the Tallinn Manual 2.0 holds that even though a cyber operation is of a low-intensity character, i.e. not falling within the ambit of either use of force or unlawful intervention, it might still be prohibited by customary international law as a violation of sovereignty.[13] Thus, Rule 4 finds a threshold below the thresholds for unlawful interventions and prohibited uses of force. According to the GoE, Rule 4 is a primary rule[14] of international law, the breach of which triggers the apparatus of the law of state responsibility (i.e., it is deemed an internationally wrongful act). As such, violations of the rule may invoke state responsibility and thus allow the targeted state to employ countermeasures in order to bring the wrongful act to an end.[15] However, countermeasures must respect certain conditions. For example, the targeted state is not allowed to resort to a measure that would constitute a use of

[11] Ibid., p. 1.
[12] Ibid., p. 17.
[13] Ibid.
[14] A primary rule is a rule defining the content of an international obligation, the breach of which gives rise to responsibility, as defined in the General Commentary para. 1 to the Draft Articles on Responsibility of States for Internationally Wrongful Acts (International Law Commission, 2001).
[15] Article 49.1 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (International Law Commission, 2001).

force.[16] Resorting to use of force by way of self-defence is strictly limited to situations of armed attacks.[17] For this reason, it is crucial to differentiate a violation of sovereignty from a use of force and armed attack.

Rule 4 of the Tallinn Manual 2.0 has not been spared from criticism. Among those who oppose the Tallinn Manual 2.0 suggestion, we find the 'sovereignty-as-principle-only' approach. According to this doctrine, the principle of sovereignty does not function as a prohibitive primary rule in cyberspace, the breach of which can give rise to state responsibility. Rather, it is an underlying principle from which other binding rules derive, such as the prohibition against the use of force and the non-intervention principle. Essentially, the sovereignty-as-principle-only doctrine denies that the principle of sovereignty is an absolute rule that prohibits certain conduct in cyberspace.[18]

As evident from this brief review of the background debate, it is safe to say that at the time of writing this thesis, low-intensity cyber operations are being conducted in an obscure field of international law. However, as a consequence of the fact that international politics and international relations progress by other means than merely those connected to law, cyber operations are likely to become even more common in the future without waiting for legal answers or guidance. For this reason, it is important to shed some light on the debate about whether certain low-intensity cyber operations are prohibited as violations of sovereignty or not. That is the object of concern of this thesis.

1.2 Purpose and Research Question

The purpose of this thesis is to examine the existence of a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. In doing so, the thesis will investigate whether the principle of sovereignty in

[16] Ibid., Article 50.1(a).

[17] Article 51 of the UN Charter.

[18] See Corn, Gary P.; Taylor, Robert – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber (The American Journal of International Law Unbound, Vol. 111, 2017) p. 207-212, [Corn and Taylor]; United Kingdom, Wright, Jeremy – Cyber and International Law in the 21st Century (Speech at Chatham Royal Institute of International Affairs, 23 May 2018), available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, last visited 4 December 2019, [Wright].

itself functions as a prohibitive primary rule of customary international law or whether it simply functions as an underlying principle from which other binding norms derive. Accordingly, the research question of this thesis is whether it currently is possible to deduce a primary rule from customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. Additionally, this thesis aims to identify and analyse some practical benefits and risks of the existence of such a rule.

1.3 Scope of the Thesis

The scope of this thesis is limited to cyber operations that fall short of the prohibition on the use of force, armed attack, and non-intervention thresholds, but that do reach certain other qualifications which will be presented below. These operations do neither fall within the ambit of the *ius ad bellum*[19] regime nor the *ius in bello*[20] regime. This is so because they are not aimed at waging war. However, although the operations do not qualify as prohibited uses of force, armed attacks, or unlawful interventions, these concepts will nonetheless be dealt with. This is motivated by the conviction that an explanation of these concepts will facilitate the understanding of the cyber operations understood in accordance with the description in the first sentence of this paragraph.

Furthermore, the scope of this thesis is limited to such cyber operations that are carried out by, or on behalf of, a state vis-à-vis another state. In the same vein, the thesis looks only at such cyber operations that are being administered from outside of the targeted state's territory, thus omitting those cyber operations controlled by a state agent physically present in the targeted state's territory. The reason for this limitation is to emphasise a unique characteristic of cyberspace, which is that remote cyber activities do not require the aggressor's physical presence in the targeted state for a violation of sovereignty to occur.

Moreover, since the purpose of this thesis is to examine the existence of a primary rule in customary international law prohibiting certain low-intensity cyber operations, I will not delve into questions on state responsibility for internationally wrongful acts that could arise

[19] The legal regime governing the conditions of when states may resort to engaging in war.

[20] The legal regime governing the conduct of war, without prejudice to what initiated the war, commonly known as international humanitarian law.

from such operations. Investigating state responsibility for low-intensity cyber operations does not contribute to reaching the purpose of the thesis as it is an investigation that would have had to be made subsequent to the one concerning the existence of a primary rule in the first place. These rules and principles of state responsibility are only actualised once an established rule of international law has been breached, which is the main problem for this thesis. Accordingly, issues such as state responsibility and attribution of cyber operations will be omitted from the discussion.

Lastly, it merits elucidating that the principal question of this thesis revolves around the principle of sovereignty as it functions in cyberspace, and not in the other more traditional domains of land, sea, air, and outer space.

1.4 Preliminary Notes on Customary International Law

1.4.1 Introduction

One of the more persistent issues discussed when it comes to customary international law is whether a certain rule indeed forms part of the law or not. This issue is also the main focus of this thesis. Before describing the method that will be used in order to examine the existence of the rule in question, it is necessary to have a preliminary understanding of the concept of customary international law. This is so because the method that will be used presumes a given understanding of customary international law. In what follows of this section I will therefore explain what I take to be the nature of customary international law, how it emerges, and how it is usually identified. The subsequent section will present the method applied on the investigation of the research question.

1.4.2 Customary International Law

In most domestic legal orders laws are adopted by parliaments and then applied, and hence further developed, by courts. The question of whether a legal rule exists or not is usually not too difficult to answer within the realm of domestic legal systems. Instead, the main problem in this context is often to ascertain the meaning of a given rule and how it applies to different circumstances. However, international law is essentially very different

from domestic legal systems. First, there is no central legislative body within international law. Second, in addition to different positions with respect to the meaning of a given rule of law and how this should apply to specific circumstances, there is – within the context of international law – often disagreement on the existence of the rules. This makes the discovery of the law a central issue to international law whereas it is virtually a non-issue for domestic law.[21]

The most authoritative and widely recognised starting point for discussions about the sources of international law is Article 38(1) of the Statute of the International Court of Justice.[22] It posits that the valid sources of international law are (a) international conventions, (b) international customary law, (c) general legal principles, and (d) judicial decisions and the teachings of the most highly qualified publicists.

For a rule of customary international law to exist, the existence of two elements are necessary: (1) state practice (*usus*), i.e. an actual behaviour of states consistent with a rule stipulating this behaviour, and (2) a subjective belief on the part of the acting state that such behaviour is being conducted as a matter of law (*opinio iuris sive necessitatis*) and not for any other reason. Depending on the nature of the rule, the state practice necessary for confirming the existence of a rule of customary international law can be required, prohibited, or allowed.[23] The second element is psychological in the sense that it focuses on the belief that a state behaves in a certain way because it is under a legal obligation to do so. Its function is to distinguish legal custom from principles of morality, conduct of courtesy, or mere social usage.[24] Therefore, a central challenge inherent to the confirmation of the existence of a customary international rule is to identify the point at which state behaviour ceases to be optional and becomes legally required, prohibited, or allowed.

When a state behaves in a certain way with the conviction that such behaviour is required by existing or emerging law, the reaction of other states is crucial as to whether such a norm actually exists or not. The following example articulated by Professor Malcolm Shaw may illustrate how customary international law can emerge this way.[25] Suppose that a state proclaims a twelve-mile limit to its territorial sea despite the existing legal regulation

[21] Shaw, *supra* note 1, p. 51-52.
[22] Ibid., p. 52.
[23] Doswald-Beck, Louise; Henckaerts, Jean-Marie; International Committee of the Red Cross – Customary International Humanitarian Law: Volume I: Rules (Cambridge University Press, 2005), p. xxxviii, [ICRC].
[24] Shaw, *supra* note 1, p. 55.
[25] Ibid., p. 65.

stipulating a maximum three-mile limit. The state does so in the belief that "the circumstances are so altering that a twelve-mile limit might now be treated as becoming law".[26] Should other states accept this limit and follow suit, a new customary law may be emerging. However, in the case that the behaviour is not accepted, "the projected rule withers away and the original rule stands, reinforced by state practice and common acceptance".[27]

As will be demonstrated below, it is generally accepted that when determining the existence of a rule of customary international law, an inductive method is to be employed first. The International Committee of the Red Cross has provided a comprehensive model of the inductive method, i.e. to look for customary international law in state practice first and to then establish *opinio iuris*.[28]

1.4.2.1 State Practice

The assessment of state practice can be divided into two separate methodological procedures: (1) "selecti[ng] (…) [state] practice that contributes to the creation of customary international law", and (2) "assess[ing] (…) whether this practice establishes a rule of customary international law".[29]

In the first process, both physical and verbal acts constitute state practice. Physical acts include, e.g., the use of certain weapons and the way states conduct themselves in their use of those weapons. Verbal acts include, e.g., instructions to military personnel, statements in international organisations, etc.[30] An additional and related element to establish with respect to state practice supposed to prove customary international law is that the act must be disclosed. The act is not disclosed should other states not know of the act. Thus, in order to be valid as state practice, the act must give other states an opportunity to react.[31] Moreover, although decisions of international courts are not state practice, they can influence and reinforce customary international law. Should a court find a certain rule valid as part of customary international law, then there is "persuasive evidence to that effect".[32] Additionally, court decisions can influence the subsequent practice of states because of their value as

[26] Ibid.
[27] Ibid.
[28] ICRC, *supra* note 23, p. xxxvii-xlviii.
[29] Ibid., p. xxxviii.
[30] Ibid.
[31] Ibid., p. xl.
[32] Ibid.

precedents.[33] Furthermore, although international organisations are not states, they sometimes have legal personality and can accordingly contribute to the creation of customary international law.[34]

With respect to the second process, the selected state practice must be "sufficiently "dense"" in order to establish a rule of customary international law.[35] This assessment focuses on whether the practice has been "virtually uniform, extensive and representative".[36] Virtually uniform implies that different states must not act substantially different regarding a certain question, save for "a few uncertainties or contradictions".[37] The extensive and representative criterion does not require a specific number or percentage of states participating in the practice. "[I]t is not simply a question of how many States (…), but also *which* States".[38] Finally, some time must normally pass before these criteria are fulfilled and the practice is considered sufficiently dense. However, no specific amount of time is required.[39] "It is all a question of accumulating a practice of sufficient density, in terms of uniformity, extent and representativeness".[40]

1.4.2.2 Opinio Iuris

The second element for the creation of customary international law, *opinio iuris*, relates to the belief that a state is acting in accordance with the law and not, e.g., out of courtesy or morality. Depending on whether the involved rule contains a requirement, prohibition, or allowance, the way in which the legal conviction needs to be manifested differs. When it comes to rules that prohibit certain conduct, such as the one discussed in this thesis, *opinio iuris* can be expressed in at least three different ways: (1) by statements that the conduct is forbidden, (2) by condemning cases where the forbidden conduct took place, and (3) by abstaining from the prohibited conduct. In this last case, if the abstention is coupled with

[33] Ibid.
[34] Ibid., p. xli.
[35] Ibid., p. xlii.
[36] Ibid.
[37] Ibid., p. xliii.
[38] Ibid., p. xliv.
[39] Ibid., p. xlii, xlv.
[40] Ibid., p. xlv.

silence, the state must indicate that the international community legitimately expects abstention.[41]

Separating state practice from *opinio iuris* is not always necessary because one and the same act can reflect both state practice and *opinio iuris*. In fact, in some cases it might be impossible to separate the two elements, particularly because verbal acts can count as practice and manifest *opinio iuris* at the same time. In short, if the state practice is sufficiently dense, *opinio iuris* is most likely contained within the practice.[42]

1.5 Method

In order to achieve the purpose of this thesis, which is to examine the existence of a primary rule in customary international law that prohibits certain low-intensity cyber operations, I will employ the same method that can be derived from the practice of the International Court of Justice (ICJ).

When the ICJ is examining the existence of a rule in customary international law, three different methods can be discerned in its case law, namely induction, deduction, and assertion.[43] Induction may be defined as "inference of a general rule from a pattern of empirically observable individual instances of State practice and *opinio juris*".[44] Deduction may be defined as "inference, by way of legal reasoning, of a specific rule from an existing and generally accepted (but not necessarily hierarchically superior) rule or principle".[45] Put differently, the inductive method is a technique of moving from the specific to the general whereas the deductive method is a technique of moving from the general to the specific. Induction and deduction are by no means competing methods. Rather, deduction is complementary to induction. It is generally accepted that when ascertaining the existence of a rule in customary international law, induction is to be employed first. However, there are

[41] Ibid., p. xlv-xlvi.
[42] Ibid., p. xlvi.
[43] Talmon, Stefan – Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion (European Journal of International Law, Vol. 26, Issue 2, 2015) p. 417.
[44] Ibid., p. 420.
[45] Ibid.

situations when it is practically impossible to apply the inductive method, as will be demonstrated below. In such cases, one may resort to deduction.[46]

The third method employed by the Court to determine the rules of customary international law, assertion, can be described as a methodological shortcut. Simply put, assertion is to conclude that a certain rule reflects customary international law without engaging in an examination of state practice and *opinio iuris* or employing a deductive process. Often, although not exclusively, the Court uses assertion for what may be regarded as notorious custom.[47]

According to Professor Stefan Talmon, "[c]ustomary international law rules prohibiting certain actions [– such as the one discussed in this thesis –] are (…) mo[st] likely to be arrived at by deduction".[48] Therefore, out of the three aforementioned methods used by the ICJ, deduction is the most appropriate to use in this thesis. The reason for this is twofold. First, state practice in cyberspace is still rather sparse, making it impossible to use induction. Second, there are three different methods of deduction: normative, functional, and analogical deduction.[49] Due to the sparse state practice that explicitly concerns the cyber domain, I will resort to analogical deduction. This method allows for analogising the rationale of an existing rule in domains with sufficient state practice to the domain of cyberspace. In order to draw conclusions about the *lex lata* in the domain of cyberspace, numerous scholars have sought recourse to the same method.[50]

Analogical deduction is, however, not without controversy. The notions of territorial borders and territorial sovereignty have historically been considered of fundamental value in international law. Hence there is a tendency to turn to these notions also when trying to configure existing and/or new international regulation of cyberspace.[51] Accordingly, when attempting to regulate cyberspace, many scholars have suggested that it is possible to make analogical deductions drawing from the traditional domains with territorial and geographical focus, when thinking about the cyber domain where borders are blurred at best or non-existent

[46] Ibid., p. 420-423.
[47] Ibid., p. 434.
[48] Ibid., p. 422.
[49] Ibid., p. 423.
[50] See e.g. Schmitt, Michael N.; Vihul, Liis – Respect for Sovereignty in Cyberspace (Texas Law Review, Vol. 95, Issue 7, 2017), p. 1639-1676, [Schmitt and Vihul].
[51] Finkelstein, Claire; Govern, Kevin; Ohlin, Jens David (eds.) – Cyber War: Law and Ethics for Virtual Conflicts (Oxford University Press, 2015) p. 129. [Finkelstein et al.].

at worst.[52] However, the fact that territorial borders have been demarcated in different times and contexts, and without cyberspace in mind, might make it somewhat problematic to apply these notions on a situation completely unrelated to geographic and territorial issues. The great difference in character between cyber operations and ordinary physical operations has therefore led to suspicions being raised in so far as the appropriateness to rely on analogies is concerned.

One scholar claims that the analogical method must be adjusted in favour of other non-analogous methods because "[c]yberspace requires new thinking (…) on how information technology relates to legal regimes, governance, and law".[53] Another one holds that analogies are misleading, constraining and setting up limitations to innovative solutions for new technology. It is claimed that analogical reasoning should be rejected in favour of adopting new regulation for the specific context of cyberspace.[54]

The misgivings raised are not completely unfounded and deserve to be recognised. However, considering the fact that state practice is still not sufficiently dense in the cyber domain and that the international community, as to date, has not adopted a new supplemental law specifically regulating the cyber domain, analogical deduction remains an important, useful, and widely accepted method, not least considering its strong foothold in the jurisprudence of the ICJ.

1.6 Material

The material used in this study principally consists of literature on public international law, articles in various journals, international case law, and documents of various states' cyber security strategies.

One source, in particular, is of fundamental importance in this thesis; the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. This is so because the problem around which this thesis largely revolves is collected from the Tallinn Manual 2.0 and from

[52] See e.g. Schmitt and Vihul, *supra* note 50.
[53] Finkelstein et al., *supra* note 51, p. 174.
[54] Crootoft, Rebecca – Autonomous Weapon Systems and the Limits of Analogy (Harvard National Security Journal, Vol. 9, Issue 2, 2018) p. 52, 79-82.

other sources referring to the Manual. Therefore, a few words about the Tallinn Manual 2.0 are necessary.

The Tallinn Manual 2.0 is authored by a group of 19 renowned experts in international law at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. The Manual attempts to regulate the cyber domain by identifying 154 rules accompanied by comments. It is important to note that the rules represent the personal views of the experts and not the official positions of states, although some states have provided their unofficial input to the publication. Therefore, the Tallinn Manual 2.0 is not *per se* a legally binding document.[55]

The aim of the Tallinn Manual 2.0 is primarily to serve as a roadmap for national legal advisers and governments, but also to be important for the realisation of academic endeavours.[56] The GoE holds that the Manual is an "objective restatement of the *lex lata*" of customary international law in the cyber domain.[57] Thus, rather than purporting to make new law, it only codifies extant law.

Each rule of the Tallinn Manual 2.0 was adopted according to the principle of consensus within the GoE. The commentary attached to each rule aims to "identify the rule's legal basis, explain its normative content, address practical implications in the cyber context, and set forth differing positions as to scope or interpretation".[58] The method used by the GoE in interpreting extant law to the cyber domain was the use of analogies between "kinetic (physical) and cybernetic domains".[59]

The Tallinn Manual 2.0 has sparked significant reaction among states and scholars, ranging from approval and support to heavy critique of the Manual's rules. Some states have approved certain rules in the Manual as customary international law, while rejecting others. Many states' reactions have been silent and ambiguous, making it difficult to ascertain whether states wish the rules to become authoritative reflections of international law regulating cyberspace. However, as cyber operations are picking up pace and become more common, recent development indicate that states are more inclined to enforce accountability in the cyber domain. This may lead to a more approving attitude towards the Tallinn Manual

[55] Tallinn Manual 2.0, *supra* note 7, p. 1-2.
[56] Ibid., p. 2.
[57] Ibid., p. 3.
[58] Ibid., p. 4.
[59] Efrony, Dan; Shany, Yuval – A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice (The American Journal of International Law, Vol. 112, Issue 4, 2018), p. 584.

2.0 as a comprehensive and specific framework of international law governing the domain of cyberspace.[60]

1.7 Outline

The structure of the thesis is as follows. Chapter 2 offers a brief insight into the characteristics of cyberspace. Chapter 3 explains the notions of use of force, armed attack, and non-intervention. Chapter 4 delves into Rule 4 of the Tallinn Manual 2.0 and explains its normative content. Chapter 5 explores the various evidence and arguments for the existence of a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. Chapter 6 then explores the arguments against the existence of such a rule. Chapter 7 analyses the evidence and arguments from Chapters 5 and 6 and concludes on whether there currently exists a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. Finally, Chapter 8 offers some closing remarks.

[60] Ibid., p. 584-586.

2 The Characteristics of Cyberspace

The global expansion of the internet is one the most remarkable features of our age. It is the main reason for the interconnectivity and interdependency of business, government and civil society today. A major transformation is the increased reliance of states and their military on computer systems, which has largely contributed to the emergence of cyberspace.[61] Cyberspace can be defined as "[t]he environment formed by physical and non-physical components to store, modify, and exchange data using computer networks"[62] or as "a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein".[63]

Cyberspace has both differences and similarities to the more traditional domains of international law, which concern land, sea, air, and outer space. The principal characteristic of cyberspace that makes it differ from other domains is that it is an electronic space rather than a physical one. As such, it is completely man-made and not restrained by physical boundaries like territorial borders. Essentially, this means that the effects of a cyber operation can spread far beyond the site of its source.[64]

Although the cyber domain is not a physical domain, its means of infrastructure – such as computers, cables and machines – exists within one. Hence, activities in cyberspace can have kinetic effects in the physical world, similar to the effects usually caused in the more traditional theatres of conflict. For example, cyber activities can cause direct physical harm such as death or injury to persons or damage or destruction to objects.[65] The difference is that the activity itself is intangible. Cyber activities can of course also cause effects of a lesser degree of severity, such as disrupting or destroying information, collecting intelligence, or blocking communications. A striking difference from operations conducted in the traditional domains is the difficulty of attribution. In cyberspace, an aggressor can "make it appear that some other organisation or individual has initiated or undertaken certain cyber activity", so

[61] Melzer, Nils – Cyberwarfare and International Law (UNIDIR Resources, 2011), p. 3, [Melzer].
[62] Tallinn Manual 2.0, *supra* note 7, p. 564.
[63] Melzer, *supra* note 61, p. 4.
[64] Ibid., p. 5.
[65] Ibid., p. 4-5.

called ‘spoofing’.[66] Of course, this is possible in the physical domains as well. However, in the physical domains, there is often forensic evidence to prove attribution.

[66] Tallinn Manual 2.0, *supra* note 7, p. 567.

3 Use of Force, Armed Attack, and Non-Intervention

3.1 Introduction

From the fundamental concept of sovereignty derives a number of important notions for international law, such as the prohibition against the use of force and the principle of non-intervention. As mentioned above, Rule 4 of the Tallinn Manual 2.0 identifies a threshold for violations of sovereignty below the thresholds for non-intervention, use of force, and armed attack. In order to understand the scope and nature of a violation of sovereignty, it is helpful to first understand the scopes of use of force, armed attack, and unlawful intervention. This chapter will therefore provide a brief explanation of these notions and illustrate their relationships to one another.

3.2 The Use of Force and Armed Attack

Although the UN Charter predates the emergence of cyberspace, it is widely accepted that it does apply to cyber conduct.[67] Article 2(4) and Article 51 of the UN Charter enshrine the prohibition on the threat or use of force and the right to self-defence against an armed attack respectively. These rules are of fundamental importance in international law. However, the scopes of the articles are widely contested, and states are divided as to how they should be interpreted.[68]

3.2.1 Use of Force

Article 2(4) holds that states shall refrain from the threat or use of force against other states but does not specify what kind of force is intended. The article is filled with normative content but offers little by way of guidance. Historically, developing states have claimed that economic or political force is part of the prohibition, while developed states have maintained

[67] Dev, Priyanka R. – "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response (Texas International Law Journal, Vol. 50, Issue 2/3, 2015), p. 387.

[68] See e.g. Ruys, Tom – 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice (Cambridge University Press, 2010), p. 143-149. [Ruys].

that the article only prohibits armed force.[69] In this regard, the *travaux préparatoires* (preparatory works) to the UN Charter reveal that the proposition of including economic or political force within the scope of Article 2(4) was expressly rejected.[70] Thus, the prevailing understanding among scholars and states is that Article 2(4) solely covers armed force and does not extend to economic or political force.[71]

Article 2(4) is applicable without prejudice to the choice of means of attack. As the ICJ stated in the advisory opinion on the *Legality of Nuclear Weapons*, Article 2(4) "appl[ies] to any use of force, regardless of the weapons employed".[72] Accordingly, just because a computer, rather than a conventional weapon, is used during an operation does not mean that the application of Article 2(4) is excluded.[73] What is determinative of whether a cyber operation amounts to a use of force is if "its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[74] For example, a cyber operation aimed at manipulating the control system of the London DLR (a driverless and automatic passenger railway system) in order to cause the trains to travel out of control and collide, could potentially result in death or injury to persons and damage or destruction to objects. Such an operation would thus constitute a prohibited use of force.[75]

It is more difficult, however, to establish a use of force regarding cyber operations that do not directly cause death, injury, damage or destruction.[76] Suppose, for example, a cyber operation intended to disable the electric power grid of an entire city. While its direct intention might be to cause economic loss, it could also indirectly cause death, injury, damage, or destruction, e.g. by shutting down life support devices or electricity-dependent facilities. Regarding this category of cyber operations, the Tallinn Manual 2.0 refers to eight factors as determinative of whether such operations qualifiy as uses of force.[77]

---

[69] Evans, Malcolm D. (ed.) – International Law (Oxford University Press, 2019), p. 604.

[70] Buchan, Russell – Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? (Journal of Conflict and Security Law, Vol. 17, Issue 2, 2012), p. 216, [Buchan].

[71] Abass, Ademola – Complete International Law: Text, Cases, and Materials (Oxford University Press, 2012), p. 351.

[72] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, p. 226, para. 39.

[73] Tallinn Manual 2.0, *supra* note 7, p. 328.

[74] Ibid., p. 330.

[75] Melzer, *supra* note 61, p. 7.

[76] Ibid.

[77] See Tallinn Manual 2.0, *supra* note 7, p. 333-337 for the factors. Note that the factors are neither exhaustive nor formal legal criteria.

On the other hand, there is a consensus that some cyber operations do not amount to uses of force at all. It has been suggested that because Article 41 of the UN Charter mentions interruption of communication as a measure falling short of use of force, a denial of service attack[78] would not qualify as a use of force.[79] Neither would a "non-destructive cyber psychological operation" aimed at weakening the support for a government.[80]

3.2.2 Armed Attack

One of the exceptions to the prohibition on the use of force is the right to self-defence articulated in Article 51 of the UN Charter. It provides that self-defence is permissible in response to armed attack but does not offer any guidance for determining when an act constitutes an armed attack. It is therefore necessary to consider what, if anything at all, differentiates a use of force from an armed attack.

The ICJ pronounced its view on the relationship between use of force and armed attack in the *Nicaragua* case.[81] It separated "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms".[82] Essentially, the Court asserted that there is a wide gap between Article 2(4) and Article 51. Thus, it placed the threshold of the latter article above the former's. Further, the Court explained that what distinguishes an armed attack from other less grave forms of use of force is its scale and effects.[83] According to this view, the scale and effects of an armed attack exceed those of a use of force.

The pronouncements in the *Nicaragua* case have spawned criticism from scholars and states alike. According to a view contrary to the one upheld by the ICJ in its decision, the gap between a use of force and armed attack is construed so narrow as to render even small-scale uses of force as armed attacks. Some have taken this reasoning even further, claiming that there exists no gap at all between uses of force and armed attacks, effectively arguing that any unlawful use of force triggers the right to self-defence.[84]

[78] Defined as "[t]he non-availability of computer system resources to their users" in Ibid., p. 564.
[79] Melzer, *supra* note 61, p. 7.
[80] Tallinn Manual 2.0, *supra* note 7, p. 331.
[81] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, ICJ Reports 1986, p. 14, [Nicaragua].
[82] Ibid., para. 191.
[83] Ibid., para. 195.
[84] Ruys, *supra* note 68.

On the one hand, the United States appears to have adopted a position along the lines of this contrary view. The US Department of Defense (DoD) has pronounced that the right to self-defence "applies against any illegal use of force".[85] The US thus adopts the view that there is no gravity threshold distinguishing an unlawful use of force from an armed attack, or at least, that the gap is very narrow. On the other hand, several statements made during the adoption of the UN General Assembly (UNGA) Resolution 3314 (XXIX) supports the view that the threshold of armed attack is placed above that of use of force.[86] It can be concluded therefore that there is a wide gap between the two interpretations of the relevant thresholds.

As evident from this brief review of Articles 2(4) and 51 of the UN Charter, there is a gravity threshold built in the concept of use of force in which operations falling foul of the threshold do not qualify as uses of force. Further, it is safe to conclude that there is no consensus as to the scopes of uses of force and armed attacks. While there is widespread agreement that every armed attack constitutes a use of force, the question of whether all uses of force constitute armed attacks is disputed. A cyber operation can qualify as a use of force provided that it passes the scale and effects test. But whether such an operation will also be deemed as an armed attack, triggering the right to resort to force in self-defence, is a matter of contention.

3.3 Non-Intervention

The emergence of cyberspace undeniably extends the possibilities of states to intervene in the internal and external affairs of other states. A well-known incident is the cyber attack in Estonia in 2007, which crashed important government websites and crippled banks and media

[85] United States, Department of Defense: Law of War Manual (Office of the General Counsel of the Department of Defense, June 2015, updated December 2016), p. 47, 1017, available at https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190, last visited 4 December 2019.

[86] Ruys, Tom – The Meaning of "Force" and the Boundaries of the *Jus ad Bellum*: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)? (The American Journal of International Law, Vol 108, Issue 2, 2014), p. 162-164.

stations.[87] It has been argued that the cyber attack against Estonia violated the prohibition against intervention.[88]

Like the prohibition against the use of force, the non-intervention principle is an outgrowth of the concept of state sovereignty. The fact that the principle has been violated numerous times has led some to question its position as customary international law. However, the ICJ stated in *Nicaragua* that even though the principle is violated frequently, "it is part and parcel of customary international law".[89] An ample amount of state practice and *opinio iuris* has contributed to the hardening of the principle into customary international law.[90]

Although the international community has agreed on the existence of the principle of non-intervention for quite some time now, its precise scope and application is not entirely clear due to "ever-evolving and increasingly inter-tangled international relations".[91] Nevertheless, there appears to be broad consensus that an unlawful intervention consists of two components: (1) the act must have bearing on a matter falling under the target state's internal or external affairs and (2) the act must be coercive in nature.[92]

The reference to a matter falling under the target state's internal or external affairs aims at specifying the objects protected against intervention. The concept of internal affairs originates from the notion of *domaine resérvé*, first addressed by the predecessor of the ICJ, the Permanent Court of International Justice (PCIJ) in the *Nationality Decrees* advisory opinion.[93] The Court noted that the *domaine resérvé* covers such matters that "are not, in principle, regulated by international law".[94] Thus the *domaine resérvé* consists of such matters that international law leaves to the domestic affairs of each state. In *Nicaragua*, the ICJ elaborated on the concept of *domaine resérvé* by stating that "[a] prohibited intervention must (…) be one bearing on matters in which each state is permitted (…) to decide freely".[95] It then put forth the following examples of such matters: "the choice of a political, economic, social

[87] See Buchan, *supra* note 70, p. 218, 225-226 for a more detailed account of the incident.
[88] Ibid., p. 225-226.
[89] Nicaragua, *supra* note 81, para. 202.
[90] Ibid.
[91] Watts, Sean – Low-Intensity Cyber Operations and the Principle of Non-Intervention (Baltic Yearbook of International Law, Vol. 14, Issue 1, 2015), p. 145, [Watts].
[92] Tallinn Manual 2.0, *supra* note 7, p. 314; Buchan, *supra* note 70, p. 223-225; Ibid., p. 146, 153.
[93] Nationality Decrees Issued in Tunis and Morocco (France v. United Kingdom), Advisory Opinion No. 4, 1923, PCIJ, Series B. – No. 4.
[94] Ibid., p. 24.
[95] Nicaragua, *supra* note 81, para. 205.

and cultural system, and the formulation of foreign policy".[96] The other objects protected against intervention are matters falling under a state's external affairs and which are covered by that state's prerogatives, such as engaging in diplomatic relations or recognising other states and governments.[97]

The second element of an unlawful intervention is the coercive nature of the act. The ICJ pronounced in *Nicaragua* that "[i]ntervention is wrongful when it uses methods of coercion" and that "[t]he element of coercion (…) defines, and indeed forms the very essence of, prohibited intervention".[98] While there is no unanimously established definition of coercion, it is agreed that the coercive act need not be physical.[99] What is of central importance when assessing coercion is whether the act in question is designed to force a state to involuntarily act in a particular way or to involuntarily refrain to do so.[100] For instance, in the *Nicaragua* case, the Court found it to be a breach of the principle of non-intervention when the government of the US gave support to the *contras* (those engaged in fighting against the government of Nicaragua) for their military and paramilitary activities.[101]

Extending to the cyber domain, the following example taken from the Tallinn Manual 2.0 may serve as an illustration.[102] Suppose that state A blocks the access of its citizens to media platforms in state B. In order to compel state A to reopen access, state B carries out cyber operations that disturb state A's government media outlets. State B has in this case violated the principle of non-intervention because (1) the choice of state A to block access to certain media platforms is a matter falling under its internal affairs and (2) state B has conducted cyber operations designed to compel state A to act in a particular way, i.e. to reopen access to the media platforms. By way of contrast, it would not amount to a breach of the non-intervention principle if state B instead had decided to publish content on social media criticising state A as a censoring and undemocratic state. Such an act is not coercive in nature. Thus, it is important to distinguish coercive acts from mere critical, disruptive or persuasive ones.[103] The criterion of coercion makes sure that only those acts that subjugate the sovereign will of other states violate the non-intervention principle.

[96] Ibid.
[97] Tallinn Manual 2.0, *supra* note 7, p. 317.
[98] Nicaragua, *supra* note 81, para. 205.
[99] Tallinn Manual 2.0, *supra* note 7, p. 318; Watts, *supra* note 91, p. 148.
[100] Tallinn Manual 2.0, *supra* note 7, p. 317.
[101] Nicaragua, *supra* note 81, para. 228.
[102] Tallinn Manual 2.0, *supra* note 7, p. 318.
[103] Ibid., p. 318-319.

On the spectrum of international wrongs, Professor Sean Watts describes that coercive intervention is placed below use of force because an unlawful intervention is a less grave violation than an unlawful use of force.[104] In other words, the threshold of non-intervention is placed lower than the threshold of use of force, making them two distinct concepts.[105] Despite this state of affairs, the relationship between the two notions is sometimes overlapping. For example, in the *Nicaragua* case, the ICJ held that violations of the principle of non-intervention "will also, if they (…) involve the use of force, constitute a breach of the principle of non-use of force in international relations".[106] Thus, if an act qualifies as a use of force, it will automatically qualify as an unlawful intervention as well.

In conclusion, an act constitutes an unlawful intervention when it is coercive in regard to a matter falling under the target state's internal or external affairs. The threshold of the principle of non-intervention is placed below that of the prohibition against the use of force. However, under certain circumstances, one and the same act can simultaneously violate both prohibitions.

Now that the notions of the prohibition on the use of force and the prohibition against intervention have been explained, it is useful to consider whether a cyber operation that neither qualifies as a use of force nor an unlawful intervention is prohibited under contemporary international law. We shall turn our attention to this issue in Chapter 7. First, however, I will look at the purported violation of sovereignty rule and the arguments for and against its existence.

[104] Watts, *supra* note 91, p. 138.

[105] Jennings, Robert; Watts, Arthur (eds.) – Oppenheim's International Law: Volume 1. Peace. Introduction and Part 1 (Longman, 1992), p. 429.

[106] Nicaragua, *supra* note 81, para. 209.

4 Rule 4 – Violation of Sovereignty

4.1 Introduction

As mentioned above, the majority of conducted cyber operations fall short of qualifying as prohibited uses of force or prohibited interventions. The occurrence of these low-intensity cyber operations is such that states are involved with them every day.[107] This state of affairs has elicited a debate about the lawfulness of such operations. The authors of the Tallinn Manual 2.0 claim through Rule 4 that the principle of sovereignty acts as a primary rule, the breach of which gives rise to state responsibility. Thus, it is claimed that even those cyber operations that do not qualify as uses of force or prohibited interventions are illegal, provided that they reach certain other qualifications which will be presented below. Before exploring the arguments for and against the legality of these cyber operations, it is necessary to explain the scope of violations of sovereignty in cyberspace by dissecting Rule 4 of the Tallinn Manual 2.0.

4.2 Identifying the Scope of Rule 4

4.2.1 The Criteria of Rule 4

Rule 4 of the Tallinn Manual 2.0 stipulates that "[a] State must not conduct cyber operations that violate the sovereignty of another State".[108] The commentary to the rule elaborates that "[c]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of (…) sovereignty and are prohibited by international law".[109] Rule 4 thus finds a threshold below the thresholds of use of force and non-intervention. It seeks to capture cyber operations that neither amounts to prohibited uses of force nor prohibited interventions. However, as has already been implied, it does not seek to capture all conceivable cyber operations falling foul of these thresholds. In order for Rule 4 to be applicable, the cyber operation must cross the violation of sovereignty threshold.

[107] Tallinn Manual 2.0, *supra* note 7, p. 1.
[108] Ibid., p. 17.
[109] Ibid.

According to the Tallinn GoE, whether a cyber operation amounts to a violation of sovereignty depends on (1) the degree of infringement upon the target state's territorial integrity, and (2) whether there has been an interference with or usurpation of inherently governmental functions.[110]

4.2.1.1 The First Criterion – Degree of Infringement upon the Target State's Territorial Integrity

The first criterion was analysed by the GoE on three different grounds: (1) physical damage, (2) loss of functionality, and (3) infringement upon territorial integrity falling below the threshold of loss of functionality. As to the first ground, physical damage, the GoE concurred that a cyber operation that causes physical damage or injury will amount to a violation of the victim state's sovereignty. As an example, the GoE mentioned the case of a cyber operation that causes the overheating of certain equipment which results in components melting down.[111] As to the second ground, loss of functionality, although the GoE agreed that a cyber operation that causes loss of functionality of cyber infrastructure could violate the target state's sovereignty, it could not find common ground on when exactly this occurs due to the absence of sufficient *opinio iuris* on the matter. Even so, the GoE did agree that in case restoration of functionality following a cyber operation requires repair or replacement of physical components, such an operation would reach the violation of sovereignty threshold. The motivation behind this conclusion is that "such consequences are akin to physical damage or injury".[112] As to the third ground, infringement upon territorial integrity falling below the threshold of loss of functionality, the GoE could not agree whether such cyber operations cross the violation of sovereignty threshold.[113]

What stands out from the first criterion is the dubious relationship between Rule 4 of the Tallinn Manual 2.0 and Article 2(4) of the UN Charter when a cyber operation results in physical damage or injury. As has been demonstrated, physical damage or injury is a requirement found in both rules. Thus, when a cyber operation results in physical damage or injury, it is difficult to tell the scopes of Rule 4 and Article 2(4) apart. As the ICJ noted in

[110] Ibid., p. 20.
[111] Ibid.
[112] Ibid., p. 21.
[113] Ibid.

Nicaragua, the scopes of violation of sovereignty and use of force can overlap.[114] This parallel nature of the rules might *prima facie* appear as problematic because depending on whether the cyber operation merely constitutes a violation of sovereignty or the more severe wrongful act, use of force, the victim state is permitted to resort to different means of response. However, considering that the use of force threshold is placed above that of violation of sovereignty, a cyber operation resulting in physical damage or injury and which therefore constitutes a use of force will also always constitute a violation of sovereignty. One could say that an act amounting to an unlawful use of force constitutes a "particularly obvious" form of a sovereignty violation.[115] Hence, the appeared problem does not seem to be a real one.

4.2.1.2 The Second Criterion – Interference with or Usurpation of Inherently Governmental Functions

The second criterion of Rule 4 for establishing a violation of sovereignty consists in, as already revealed, the question of whether a cyber operation interferes with or usurps inherently governmental functions of the targeted state. The GoE could not agree on an exact definition of inherently governmental functions. It did, however, concur that the following examples are exclusively reserved to states and thus inherently governmental: "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities".[116] With regard to usurpation, suppose that state A conducts a law enforcement operation (an inherently governmental function) by cyber means in order to take down a botnet[117] on the territory of state B without the latter's consent or without an allocation of authority. State A will in this case violate state B's sovereignty by usurping an inherently governmental function of state B.[118] This raises the interesting question of whether Rule 4 precludes states from engaging in law enforcement cyber operations against the cyber infrastructure of terrorist organisations located on the territory of another state, more of which will be discussed in Chapter 7.

[114] Nicaragua, *supra* note 81, para. 251.
[115] Ibid., para. 205.
[116] Tallinn Manual 2.0, *supra* note 7, p. 22.
[117] Defined as "[a] network of compromised computers, so-called 'bots', (…) used to conduct coordinated cyber operations" in Ibid., p. 563.
[118] Ibid, p. 22.

There is a parallel nature between Rule 4 and the principle of non-intervention because the concept of inherently governmental functions is reminiscent of the concept of *domaine resérvé*. What, if anything at all, distinguishes an inherently governmental function from a matter falling under a state's *domaine resérvé*? The GoE of the Tallinn Manual 2.0 recognises that the concepts overlap but insists that they are not identical.[119] However, the experts do not provide any explanation for this claim, which is unfortunate because it would have been a good opportunity to clarify what they claim distinguishes inherently governmental functions from matters falling under the *domaine resérvé*. Neither the ICJ nor the GoE have given much guidance on how to define the concepts at hand. However, in light of what hitherto has been said, it is safe to assume that inherently governmental functions such as conducting elections, delivering social services, etc., also are matters over which states are permitted to decide freely and thus fall under the *domaine resérvé*.

Although the scopes of Rule 4 and the principle of non-intervention overlap, a major difference between the two is that an act amounting to a violation of sovereignty need not be coercive, while coercion is essential for an act to violate the non-intervention principle. Consider, for example, the aforementioned case of state A conducting a law enforcement operation in order to take down a botnet in state B without the latter's consent. Although state A violates state B's sovereignty, it does not breach the principle of non-intervention because state A is not coercing state B to act in a particular way or refrain to do so.[120]

4.2.2 Are the Criteria Alternative or Cumulative?

The Tallinn Manual 2.0 is not entirely clear on whether the criteria set up in Rule 4 are alternative or cumulative, i.e. must a cyber operation satisfy just one or both criteria in order to amount to a violation of sovereignty? From a linguistic point of view, the usage of the word 'and' rather than 'or' between the criteria suggests that they are cumulative. However, this is contradicted later in the Manual when the GoE notes that if a cyber operation interfers with or usurps an inherently governmental function (the second criterion), it need not result in physical damage, injury, or loss of functionality (the first criterion) in order to amount to a violation of sovereignty.[121]

[119] Ibid., p. 24.
[120] Ibid.
[121] Ibid., p. 22.

The GoE is silent as to whether this reasoning also applies on the opposite case, i.e. if a cyber operation results in physical damage, injury, or loss of functionality, does it also have to interfere with or usurp an inherently governmental function in order to qualify as a violation of sovereignty? By combining the facts that the word 'and' is used between the two criteria and that the GoE has explicitly stated that if the second criteria is satisfied then the first need not be – while simultaneously failing to mention whether this reasoning also applies on the opposite case – there is textual support for the interpretation that this question must be answered in the affirmative. In other words, according to this interpretation, a cyber operation that results in physical damage, injury, or loss of functionality must also interfere with or usurp an inherently governmental function in order to qualify as a violation of sovereignty. This interpretation places a rather high violation of sovereignty threshold.

Whether the GoE intended Rule 4 to be interpreted this way is not possible to answer definitively. However, given that the object and purpose of the principle of sovereignty is, as the GoE itself says, to give states "control over (…) activities on their territory" and to protect their "territorial integrity", it seems unlikely that this was the GoE's intention.[122] Furthermore, as mentioned above, with respect to cyber operations that cause physical damage or injury without interfering with or usurping inherently governmental functions, these can qualify as uses of force and as such they will automatically also qualify as violations of sovereignty. Consequently, there can be no other conclusion than that the criteria in Rule 4 are alternative, and not cumulative. This ambiguity could have easily been eliminated by replacing the word 'and' with 'or' between the criteria.

In conclusion, Rule 4 finds a violation of sovereignty threshold below the thresholds of use of force and non-intervention. Whether a cyber operation qualifies as a violation of sovereignty according to Rule 4 will depend on (1) the degree of infringement upon the target state's territorial integrity, or (2) whether there has been an interference with or usurpation of inherently governmental functions. Both of these criteria show resemblances to those of use of force and unlawful intervention. Thus, the scope of Rule 4 overlaps to some extent with those of use of force and unlawful intervention.

As mentioned above, the Tallinn Manual 2.0 is claimed by the GoE to be a codification of extant customary international law in the cyber domain. Thus, the GoE claims that Rule 4 has operative effect under contemporary customary international law. This claim has been met

[122] Ibid., p. 20-21.

with considerable resistance and rejection by those who claim that low-intensity cyber operations do not give rise to responsibility because the principle of sovereignty is merely an underlying principle, and does therefore not in itself operate as a primary rule. The following chapters will explore the various arguments put forth by the two factions.

5 The Arguments For the Existence of a Primary Rule on Violations of Sovereignty in Cyberspace

5.1 Introduction

The question at hand is whether the principle of sovereignty operates as a binding rule of customary international law in cyberspace as Rule 4 claims, or whether it simply functions as an underpinning principle from which other binding norms emanate. The assertion that Rule 4 of the Tallinn Manual 2.0 is reflective of contemporary customary international law is elaborated by two of the Manual's authors, Michael Schmitt and Liis Vihul.[123] The authors, who argue for the 'sovereignty-as-rule' approach, support their assertion by pointing to a plethora of instances of state behaviour that have been categorised as violations of sovereignty by international courts, states, and international organisations. The following sections will present the evidence that speak in favour of the existence of a rule in customary international law that prohibits certain low-intensity cyber operations. Chapter 6 will in turn present the arguments that speak against the existence of such a rule. The arguments presented in Chapters 5 and 6 will be assessed and analysed in Chapter 7.

5.2 Evidence in State Practice and Opinio Iuris

The presentation of the evidence supporting the assertion that Rule 4 is part of customary international law will begin with delving into state practice and *opinio iuris*. This is motivated by the fact that state practice and *opinio iuris* constitute obligatory elements of customary international law, as was explained in Section 1.4.

Schmitt and Vihul initially cautions that some incidents that have violated states' sovereignties have also involved armed forces and therefore even crossed the use of force or prohibited intervention thresholds. In such cases, it occurs that states choose to discuss the violation of sovereignty separate from the unlawful use of force or prohibited intervention, which supposedly demonstrates that the violation of sovereignty principle is a distinct and

[123] Schmitt and Vihul, *supra* note 50.

independent primary rule.[124] They also warn that the term sovereignty is often used in a political context "without necessarily carrying legal weight".[125] Therefore, it is important to be highly aware of the obligatory components of customary international law when examining state practice and expressions of *opinio iuris*. The examples that Schmitt and Vihul present and that follow below are said to "have been carefully selected as illustrations of the way in which States treat the issue of sovereignty in international law".[126]

5.2.1 State Practice

In the domain of land, the Israeli abduction of Adolph Eichmann, a key actor and organiser of the Holocaust, is considered as a case supporting the sovereignty-as-rule doctrine. Following the Second World War, Eichmann fled to Argentina where he lived until 1960 when agents of the Israeli intelligence service, Mossad, captured him on Argentine territory and put him on trial in Israel. Argentina brought the matter before the UN Security Council (UNSC) accusing Israel of violating its sovereignty by exercising authority on Argentine territory. The UNSC in turn adopted Resolution 138[127] in which it noted the illegality of violating another state's sovereignty and requested the Israeli government to make reparation in accordance with international law.[128]

In 1978, the Soviet satellite Cosmos 954 carrying on board a nuclear reactor re-entered the earth's atmosphere above Canadian territory. The satellite disintegrated upon re-entry and its debris landed in Canada. Canada claimed that the trespass of the satellite violated its territorial sovereignty both over its airspace and on land. Canada then demanded compensation which was subsequently paid by the Soviet Union, suggesting that the Soviets admitted a violation of Canadian sovereignty.[129]

In the aerial domain, two incidents in 1960 provide strong support for the existence of the violation of sovereignty rule. The first concerns the shooting down of a United States aircraft and the capturing of its pilot by the Soviet Union. The aircraft was shot down while flying in Soviet national airspace. The second incident involved the shooting down of another United

[124] Ibid., p. 1656.
[125] Ibid.
[126] Ibid.
[127] SC/RES/138 Question relating to the case of Adolf Eichmann (1960), [Resolution 138].
[128] Schmitt and Vihul, *supra* note 50, p. 1659.
[129] Ibid., p. 1660-1661.

States aircraft and the capturing of its crew members by the Soviet Union. Unlike the first aircraft, this aircraft was shot down while flying in international airspace. While the downing of the first aircraft was not protested by the US government, the second incident was strongly remonstrated. The different reactions by the US government towards the two incidents is said to be explained by the different locations of the shoot-downs. The fact that the first aircraft was shot down while flying in Soviet territorial airspace and the absence of protests by the US government indicates that the US recognised that the sovereignty of the Soviet Union had been violated by the aerial intrusion.[130]

In 2001, a US military surveillance aircraft collided mid-air with a Chinese fighter jet. Following the collision, the US aircraft entered into Chinese territorial airspace for an emergency landing. China claimed that the US had violated its sovereignty by entering into its territorial airspace and landing on a Chinese military airport without permission. The US concurred that unconsented entrance into another state's territorial airspace indeed constituted a violation of international law. However, in this specific case, the wrongfulness of entering Chinese airspace was precluded because the American aircraft was in distress. Supposedly, the US government's argument indicates that absent distress, the American aircraft would have violated China's sovereignty.[131]

State practice in support of the existence of the violation of sovereignty rule can also be found in the maritime domain. One example is the capturing and detaining of fifteen British Royal Navy personnel by Iranian forces in 2007. The Royal Navy was conducting a search of a merchant vessel in the Persian Gulf when Iranian forces intercepted. Iran captured and detained the crew on the basis that it was operating in Iranian territorial waters without permission, thus violating its territorial sovereignty. The United Kingdom government on the other hand claimed that Iran had acted unlawfully because the incident took place in what the UK claimed to be Iraqi territorial waters.[132]

Another example is the 2016 incident in the Persian Gulf involving Iran and the US. Iranian forces captured ten US Navy personnel and two riverine boats that had entered Iranian territorial waters. Iran stated that the entry into Iranian territorial waters was illegal. However, shortly after negotiations with the US government, Iran released the boats and the personnel. The US did not voice any protests against the actions of Iran. Rather, Secretary of State John

[130] Ibid., p. 1656.
[131] Ibid., p. 1657.
[132] Ibid., p. 1657-1658.

Kerry thanked the Iranian authorities for their cooperation, suggesting that the US understood that the entry into Iranian waters constituted a violation of Iran's territorial sovereignty.[133]

As evident from this account, there is ample state practice supporting the assertion that sovereignty is a primary rule susceptible to violation. It merits noting however that all of the examples above are from other domains than the cyber domain. Nevertheless, when interpreting sovereignty in cyberspace, they may prove to be useful by way of analogy.

5.2.2 Opinio Iuris

Expressions of *opinio iuris* in support of the existence of the violation of sovereignty rule can, *inter alia*, be found in states' national cyber security strategy documents, states' declarations of international law in cyberspace, and in the statements of senior government officials.

There is a great deal of expressions of *opinio iuris* that support the assertion that the principle of sovereignty is a rule susceptible to violation. Starting with the US, Schmitt and Vihul highlight that in the late 1990s, the US DoD released a document in which it stated that "[a]n unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory".[134] The question at the time was not whether cyber operations could violate another state's sovereignty, but at what point they did. That cyber operations could violate another state's sovereignty was taken as a normative given.[135]

Further, the former US State Department Legal Adviser Harold Koh held a speech in 2012 on international law in cyberspace. Koh expressed that the US took the position that established principles of international law are applicable in the cyber domain and that states conducting cyber operations in other states must take into account the sovereignty of those states. This view was reiterated by Koh's successor Brian Egan, who added that the threshold at which a cyber operation violates another state's sovereignty must be determined by state practice and *opinio iuris*. Both Koh and Egan treated the principle of sovereignty as distinct

[133] Ibid., p. 1658.
[134] As cited in Ibid., p. 1640.
[135] Ibid.

from the prohibition on use of force and the prohibition on coercive intervention, which suggests that it operates as an independent and binding rule. Further, in 2014, the US reiterated its view with respect to sovereignty in cyberspace in its submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (UNGGE).[136] The UNGGE is the main state-level forum addressing questions of how international law applies to cyberspace.[137]

States' national cyber security strategy documents are often written in very general, cautious and sweeping formulations. Nevertheless, they have proven to serve as a useful tool when examining the *opinio iuris* of states.[138] For instance, two Chinese national cyber security strategy documents reveal that China is convinced that sovereignty functions as a binding rule of international law in cyberspace.[139] The 2017 document states that China's goal is to "resolutely safeguard the country's sovereignty (…) in cyberspace" and that "[u]pholding sovereignty in cyberspace (…) reflects governments' responsibility and right to administer cyberspace in accordance with law".[140] Furthermore, the 2016 document states that "[n]o infringement of sovereignty in cyberspace will be tolerated" and that China will "oppose all actions [that] subvert [their] national regime or destroy [their] sovereignty through [cyberspace]".[141] The fact that China is so keen to defend its sovereignty implies that the official Chinese view is that sovereignty is not merely a principle but a rule susceptible to violation. If sovereignty could not be violated in cyberspace, why would China feel the need to defend it at all?

France's Strategic Review of Cyber Defence from 2018 and its Declaration on International Law in Cyberspace from 2019 leave no doubt as to whether France views sovereignty as a guiding principle or as a rule with operative effect. The 2018 document states

[136] Ibid., p. 1663-1664.

[137] Geneva Internet Platform Digital Watch Observatory, https://dig.watch/processes/un-gge, last visited 4 December 2019.

[138] Väljataga, Ann – Tracing *opinio juris* in National Cyber Security Strategy Documents (NATO CCDCOE, 2018), p. 4-5, [Väljataga].

[139] China, National Cyberspace Security Strategy (27 December 2016), unofficial translation available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/, original Chinese text available at http://www.cac.gov.cn/2016-12/27/c_1120195926.htm, last visited 4 December 2019, [China NCSS 2016]; China, International Strategy of Cooperation on Cyberspace (1 March 2017), unofficial translation available at http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm, last visited 4 December 2019, [China ISCC 2017].

[140] Ibid., China ISCC 2017.

[141] China NCSS 2016, *supra* note 139.

that "[t]he principle of sovereignty applies to cyberspace".[142] It then goes on to state that apart from constituting violations on the principle of non-intervention and the prohibition on the use of force, cyber operations can also constitute violations of sovereignty.[143] In the 2019 document then, France reiterates that depending on the gravity, effects, or intrusion of a cyber operation, it may violate the prohibition on the use of force, the non-intervention principle, or the victim state's sovereignty.[144] Note that in both the 2018 and the 2019 documents, France treats violations of sovereignty separate from coercive interventions and uses of force. This is indicative of the French view that sovereignty is an autonomous binding norm. Moreover, the 2019 document holds that "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related [(information and communication technology)] activities".[145] Again, note that France distinguishes state sovereignty from norms and principles that flow from state sovereignty, such as the principle of non-intervention and the prohibition on the use of force. It is clear that the French *opinio iuris* is that state sovereignty is a binding rule of international law rather than merely a foundational principle.

The Netherlands is another major supporter of the violation of sovereignty rule. As recently as in September 2019, the Dutch government stated in a letter to its parliament that "states have an obligation to respect the sovereignty of other states and to refrain from activities that constitute a violation of other countries' sovereignty. Equally, countries may not conduct cyber operations that violate the sovereignty of another country".[146] In the document, the notions of state sovereignty, non-intervention, and use of force are dealt with separately, demonstrating that the Netherlands considers state sovereignty to be an independent rule distinct from other rules that stem from the principle of sovereignty.

---

[142] France, Strategic Review of Cyber Defence (February 2018), as cited and translated in Delerue, François; Géry, Aude – France's Cyberdefence Strategic Review and International Law (Lawfare, 23 March 2018), available at https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law, last visited 4 December 2019.

[143] Ibid.

[144] France, Declaration on International Law in Cyberspace (September 2019), as referred in Roguski, Przemyslaw – France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I (Opinio Juris, 24 September 2019), available at https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/, last visited 4 December 2019, [Roguski].

[145] Ibid.

[146] The Netherlands, Appendix: International Law in Cyberspace (September 2019), p. 2, available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, last visited 4 December 2019.

Russia has also expressed support for the assertion that state sovereignty is a binding norm. Together with the Chinese President Xi Jinping, Russia's President Vladimir Putin issued a statement in 2016 announcing that China and Russia "[j]ointly advocate respect to and oppose infringements on every country's sovereignty in information space".[147] The fact that the word 'infringements' was used indicates that Russia views state sovereignty as a rule susceptible to violation.

The common denominator in the aforementioned expressions of *opinio iuris* is that the principle of state sovereignty applies in cyberspace and that it operates as a substantive and binding norm, not simply as an underlying principle from which other binding norms derive.

Apart from state practice and *opinio iuris*, which are central elements of customary international law, the existence of a certain rule in customary international law can also be supported by decisions and statements by international courts and international organisations. The following sections will thus present evidence by international courts and international organisations that speak in favour of the violation of sovereignty rule being part of customary international law.

5.3 Evidence in International Judicial Decisions

As mentioned above (Subsection 1.4.2.1), decisions of international courts can reinforce customary international law. Should a court find a certain rule to exist as part of customary international law, then there is "persuasive evidence to that effect".[148] Additionally, court decisions can influence the subsequent practice of states because of their value as precedents, and thus indirectly contribute to the crystallisation of customary international law.[149]

Schmitt and Vihul start their review of the case law in support of the existence of the sovereignty rule with the *Lotus* case from 1927.[150] In the judgment, the PCIJ pronounced that "the first and foremost restriction imposed by international law upon a state is that – failing

[147] Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, as cited in Väljataga, *supra* note 138, p. 7. Full statement available at https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm, last visited 4 December 2019.

[148] ICRC, *supra* note 23, p. xl.

[149] Ibid.

[150] S.S. Lotus (France v. Turkey), Judgment No. 9, 1927, PCIJ, Series A. – No. 10.

the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another state".[151] From this excerpt, Schmitt and Vihul argue that it is possible to conclude that a state which, without consent, acts in the territory of another state is in breach of its duty to respect that state's sovereignty.[152] This implies that state sovereignty is a primary rule of international law.

In 1928, the Permanent Court of Arbitration stated in the *Island of Palmas* case that "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[153] From this excerpt, Schmitt and Vihul contend that since sovereignty gives states the exclusive right to exercise state functions, the corollary of that right must be that other states are under an obligation to respect it.[154]

This thread continued in the *Corfu Channel* case.[155] In short, the case involved a dispute between the UK and Albania, which arose out of an incident in the Albanian territorial waters of the Corfu Channel. British warships passing through the channel struck mines and suffered heavy damage from the explosions. Three weeks after the explosions, the UK sent more warships to the area in question in order to conduct minesweeping operations. With respect to these operations, Albania accused the UK for having violated its sovereignty by sweeping mines in Albanian territorial waters without prior consent from the Albanian authorities.[156] And indeed, the Court stated that "between independent States, respect for territorial sovereignty is an essential foundation of international relations. (…) [T]o ensure respect for international law, (…) the Court must declare that the action of the British Navy co stituted [*sic*!] a violation of Albanian sovereignty".[157] According to Schmitt and Vihul, this is a clear exhibition that the principle of sovereignty is an autonomous primary rule of international law.[158]

[151] Ibid., p. 18.
[152] Schmitt and Vihul, *supra* note 50, p. 1651.
[153] Island of Palmas (United States of America v. The Netherlands), Arbitral Award, 1928, PCA, Case Nr. 1925-01, p. 8.
[154] Schmitt, Michael N.; Vihul, Liis – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in Cyberspace: *Lex Lata Vel Non?* (The American Journal of International Law Unbound, Vol. 111, 2017) p. 216, [Schmitt and Vihul Symposium].
[155] Corfu Channel (United Kingdom v. Albania), Judgment, ICJ Reports 1949, p. 4, [Corfu Channel].
[156] Ibid., p. 12-13.
[157] Ibid., p. 35.
[158] Schmitt and Vihul Symposium, *supra* note 154, p. 215.

Furthermore, as Phil Spector, another author of the Tallinn Manual 2.0 notes, Judge Alejandro Alvarez elaborated on the principle of sovereignty in his individual opinion to the *Corfu Channel* case.[159] Judge Alvarez noted that "[b]y sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations on them".[160] Essentially, Judge Alvarez reiterated and clarified the reasoning expressed in the *Island of Palmas* case; rights conferred upon states by sovereignty must be shouldered by corresponding obligations imposed on other states to respect those rights.

In the *Nicaragua* case, after having found that the US had violated the prohibition on the use of force and the principle of non-intervention, the ICJ went even further and explicitly concluded that the US had also violated the sovereignty of Nicaragua. While acknowledging that the principle of sovereignty to a certain extent overlaps with the principle of non-intervention and the prohibition on the use of force, the Court treated the principle of sovereignty separately.[161] According to Schmitt and Vihul, this demonstrates that "sovereignty enjoys independent valence" and thus supports the assertion that sovereignty is an autonomous primary rule.[162]

The final case invoked by Schmitt and Vihul in support of the sovereignty-as-rule approach is *Certain Acitivities*.[163] In this case, the ICJ found that "by excavating three [channels] and establishing a military presence on Costa Rican territory, Nicaragua ha[d] violated the territorial sovereignty of Costa Rica".[164] The Court noted that it had come to this conclusion without also having to establish a use of force.[165] Accordingly, Schmitt and Vihul claim that this case leaves no doubt as to the self-standing and legally binding nature of the principle of sovereignty.[166]

---

[159] Spector, Phil – Symposium on Sovereignty, Cyberspace and, Tallinn Manual 2.0: In Defense of Sovereignty, in the Wake of Tallinn 2.0 (The American Journal of International Law Unbound, Vol. 111, 2017) p. 220, [Spector].

[160] Corfu Channel, *supra* note 155, p. 43 (Individual Opinion by Judge Alvarez).

[161] Nicaragua, *supra* note 81, para. 212-213, 251.

[162] Schmitt and Vihul, *supra* note 50, p. 1654.

[163] Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, ICJ Reports 2015, p. 665, [Certain Activities].

[164] Ibid., para. 229.

[165] Ibid., para. 96-97.

[166] Schmitt and Vihul, *supra* note 50, p. 1655.

The thread running through the aforementioned cases is that sovereignty confers rights and imposes duties upon states, and that it operates independently from the principle of non-intervention and the prohibition on the use of force. In other words, the cases speak in favour of the violation of sovereignty rule being part of customary international law.

5.4 Evidence in International Fora

As stated above (Subsection 1.4.2.1), although international organisations are not states, they sometimes have legal personality and can accordingly contribute to the creation of customary international law independently of their member states.[167] It is therefore important to examine what support there is for the existence of the violation of sovereignty rule in various international organisations and groups.

Schmitt, Vihul and Spector point out that the UNSC and the UNGA have supported the existence of the violation of sovereignty rule.[168] For instance, the aforementioned Resolution 138 of the UNSC, concerning the abduction of Eichmann, stated the unlawfulness of violating "the sovereignty of a Member State".[169] Furthermore, Spector mentions UNSC Resolutions, 1244 (Yugoslavia), 1272 (Indonesia), and 1808 (Georgia), as further examples of affirmations of sovereignty being a primary rule.[170]

With respect to the UNGA, its 1970 Declaration on Friendly Relations is said to be "perhaps the most significant general pronouncement of law bearing on the existence of [the violation of sovereignty] rule".[171] The declaration holds that "the purposes of the United Nations can be implemented only if States enjoy sovereign equality and comply fully with the requirements of this principle in their international relations".[172] From this excerpt, Schmitt and Vihul conclude that the principle of sovereignty can be violated by certain state actions. Hence, "sovereignty is more than an underlying principle; it must have operative effect".[173]

[167] ICRC, *supra* note 23, p. xli.
[168] Schmitt and Vihul, *supra* note 50, p. 1665; Spector, *supra* note 159, p. 220.
[169] Resolution 138, *supra* note 127, preamble.
[170] Spector, *supra* note 159, p. 220, n. 7.
[171] Schmitt and Vihul, *supra* note 50, p. 1666.
[172] GA/RES/2625 (XXV) Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (1970), preamble.
[173] Schmitt and Vihul, *supra* note 50, p. 1666.

Further the 2013 Report of the UNGGE distinguished sovereignty from other norms and principles that derive from it, such as the non-intervention principle and the prohibition on the use of force. It held that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities".[174] The language is recognised from the 2019 French Declaration on International Law in Cyberspace cited above (Subsection 5.2.2). This distinction indicates that the principle of sovereignty is an independent rule separate from the other two.[175] In its 2015 Report, the UNGGE reiterated the distinction between state sovereignty on the one hand and the principle of non-intervention and the prohibition on the use of force on the other.[176] In addition, Schmitt and Vihul argue that the fact that this distinction was made in a context of the regulation of cyber operations, the UNGGE admitted that sovereignty is a rule applicable in cyberspace.[177]

[174] GA/DOC/A/68/98 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (2013), para. 20.

[175] Schmitt and Vihul, *supra* note 50, p. 1667.

[176] GA/DOC/A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (2015), para. 27-28.

[177] Schmitt and Vihul, *supra* note 50, p. 1667.

6 The Arguments Against the Existence of a Primary Rule on Violations of Sovereignty in Cyberspace

6.1 Introduction

On the other end of the spectrum are the sovereignty-as-principle-only supporters. They oppose the claim that Rule 4 of the Tallinn Manual 2.0, which prohibits certain cyber operations below the thresholds of unlawful intervention and unlawful use of force, is reflective of customary international law. According to them, contemporary customary international law does not prohibit states from conducting cyber operations below the thresholds of unlawful intervention and unlawful use of force. It is argued that with respect to cyberspace, the principle of sovereignty is just that: a baseline principle rather than a primary rule prohibiting certain cyber operations. In recent years, two states in particular appear to have confessed themselves to the sovereignty-as-principle-only school, namely the US and the UK. Seeing as these states have so clearly rejected the idea of a primary rule on violations of sovereignty in cyberspace, this chapter will explore their various arguments.

6.2 The US' Position on Sovereignty in Cyberspace

As was demonstrated in the previous chapter, the US previously took the position that cyber operations could violate a state's sovereignty as a matter of law. The question was only at what point the sovereignty was breached. That position stands in stark contrast to the US' most recent assessment of sovereignty in cyberspace, which coincided with the election of President Donald Trump. In January 2017, the US DoD issued a memorandum in which it opposed the view that the principle of sovereignty operates as an independent and legally binding rule in cyberspace. It states that "[m]ilitary cyber activities that are neither a use of force, nor that violate the principle of non-intervention are largely unregulated by international law at this time".[178]

[178] As cited in Watts, Sean; Richard, Theodore – Baseline Territorial Sovereignty and Cyberspace (Lewis & Clark Review, Vol. 22, Issue 3, 2018), p. 828, [Watts and Richard].

Most prominent in articulating the US' current view on sovereignty in cyberspace are Colonel Gary Corn and Robert Taylor, two highly placed legal advisers within the US DoD. Corn and Taylor do not deny that international law applies to the cyber domain. For example, they agree that cyber operations can violate the prohibitions on intervention and use of force. Nor do they deny that international law, in general, prohibits violations of sovereignty. Rather, they claim that in the specific domain of cyberspace, there is no independent rule prohibiting violations of sovereignty. According to them, cyber operations that fall below the thresholds of unlawful intervention and use of force are not prohibited by international law. They claim that "[b]elow these thresholds, there is insufficient practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace".[179] They further state that "[w]hile [the] principle of sovereignty (…) should factor into the conduct of every cyber operation, it does not establish an absolute bar against [them]".[180]

To support their claim, Corn and Taylor point to the differences in how sovereignty is viewed and applied in different circumstances and different domains. As illustration, they refer to the practice of espionage in other states' territories. Corn and Taylor claim that while espionage might be unlawful under a state's domestic laws, it is not under international law. They base this on the fact that states have long engaged in espionage activities in the territories of other states, "subject only to the risk of diplomatic consequences or the exercise of domestic jurisdiction (…) if discovered and caught".[181] Corn and Taylor mean that as long as the espionage activity stays below the thresholds of prohibited intervention and use of force, it is not violating an international norm. Thus, it is claimed that the same would apply for espionage activities conducted in cyberspace.[182]

To further support their claim, Corn and Taylor point to the domains of outer space, air and the seas. With respect to outer space, they hold that "objects in orbit are beyond the territorial claims of any nation, and outer space – including outer space above another state's territory – is available for exploitation by all".[183] The contrast is very striking with respect to the aerial domain, where "any unconsented entry into the airspace of another state is regarded

[179] Corn and Taylor, *supra* note 18, p. 208.
[180] Ibid.
[181] Ibid., p. 209.
[182] Ibid., p. 209-210.
[183] Ibid., p. 210.

as a serious violation of international law".[184] Lastly, with respect to the maritime domain, Corn and Taylor state that whether an entry into or transit through another state's territorial waters is permissible will depend on the facts and circumstances in the specific case. Based on these examples, Corn and Taylor conclude that "[t]he fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace".[185]

Another argument used to support their claim that sovereignty does not prohibit cyber operations below the thresholds of unlawful intervention and use of force is that such a rule would set up hurdles to states engaging in counter-terrorism cyber operations. Corn and Taylor write that states that wish to disrupt the cyber infrastructure of terrorist organisations like ISIS would have to either seek authorisation from the UNSC or from the host state. Seeing as "[t]he nature of cyber operations (…) often require high degrees of operational security and the flexibility to act with speed and agility", a primary rule on violations of sovereignty would make these operations ineffective.[186] Accordingly, Corn and Taylor conclude that the principle of sovereignty does not preclude the US from conducting cyber operations against the cyber infrastructure of terrorist organisations located in other states. This is the case as long as the cyber operation "is focused solely against the individual accounts or facilities of terrorists or terrorist organizations widely recognized as such, and when the cyber actions will generate only *de minimis* effects on nonterrorist infrastructure within the host state".[187]

6.3 The UK's Position on Sovereignty in Cyberspace

In May 2018, the UK for the first time officially presented its position on international law in cyberspace. During a speech at Chatham House, the UK's former Attorney General, Jeremy Wright, laid out his government's position on the applicability of international law in cyberspace. The UK takes the position that international law does apply to cyber operations. It

[184] Ibid.
[185] Ibid.
[186] Ibid., p. 211.
[187] Ibid., p. 211-212.

is stated that the fact that an act is carried out in cyberspace does not preclude it from being branded as an unlawful intervention, use of force, or armed attack.[188]

However, with respect to cyber operations that fall below the threshold of unlawful intervention, the UK adopts the position that these are currently not prohibited by international law. Like the US, the UK believes that the principle of sovereignty is a principle from which other binding norms stem, rather than itself constituting a binding norm. The UK states that it is not "persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law".[189]

Unfortunately, the UK's policy on sovereignty in cyberspace is rather laconic and does not engage in a discussion as to why it is not seeing the principle of sovereignty as a rule with operative force. It only states its lack of persuasion that sovereignty is a binding rule. However, although the UK does not present the rationale for its conclusion, it is probably based on the fact that the state practice that is used to support the existence of the rule originates from other domains than the cyber domain. If this is the case, the UK is not in favour of regulating this area of the cyber domain by way of analogy to other domains.

6.4 Evidence in International Judicial Decisions

The case law presented in Chapter 5 in support of the existence of the violation of sovereignty rule can, if seen through another lens, also support its non-existence. This is emphasised by Corn and Taylor, who argue that the principle of sovereignty does not stand as a rule on its own, but rather, it is attached to the already established rules of prohibited intervention and prohibited use of force. In making this argument, Corn and Taylor point out that the sovereignty-as-rule camp frequently refers to violations of a state's territorial sovereignty. This, they claim, "confuses the concept of territorial sovereignty, (…) with the more precise concepts of territorial integrity and the inviolability of borders protected through

[188] Wright, *supra* note 18.
[189] Ibid.

[Article 2(4) of the UN Charter]".[190] In order to violate the territorial integrity of a state, a higher degree of harm is required than that which is meant to be prohibited by the violation of sovereignty rule.

First, Corn and Taylor claim that the facts and circumstances of the *Corfu Channel* case do not support the existence of a self-standing violation of sovereignty rule. With respect to the minesweeping operation that Albania claimed had violated its sovereignty, it was conducted "against the clearly expressed wish of the Albanian Government" and with "a large number of warships in the territorial waters of [Albania]".[191] Further, the Court likened the operation to a "manifestation of a policy of force".[192] These facts imply that the minesweeping operation violated a higher threshold than that purported by the violation of sovereignty rule.[193]

Second, Corn and Taylor refer to the *DRC v. Uganda* case to support their claim that sovereignty is not a self-standing primary rule.[194] In short, the Democratic Republic of the Congo (DRC) accused Uganda for having violated the prohibition on the use of force, the non-intervention principle, and the respect for the DRC's sovereignty by engaging in military activities, by occupying its territory, and by supporting rebel forces.[195] In its judgment, the ICJ found "that Uganda ha[d] violated the sovereignty, and also the territorial integrity of the DRC. Uganda's actions equally constituted an interference in the internal affairs of the DRC".[196] The usage of the phrase "territorial integrity" is extracted from Article 2(4) of the UN Charter, indicating a violation of a higher placed threshold. Furthermore, in its conclusions, the Court only stated that Uganda "violated the principle of non-use of force (…) and the principle of non-intervention", not mentioning a violation of sovereignty.[197] Thus, there is textual support for the view that the Court did not establish a violation of sovereignty independently from the violation of the prohibition on use of force and non-intervention. Simply put, this suggests that prohibited sovereignty-associated acts are limited to unlawful

[190] Corn and Taylor, *supra* note 18, p. 210.
[191] Corfu Channel, *supra* note 155, p. 33-34.
[192] Ibid., p. 35.
[193] Corn and Taylor, *supra* note 18, p. 210, n. 14.
[194] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005, p. 168, [DRC v. Uganda].
[195] Ibid., para. 24.
[196] Ibid., para. 165.
[197] Ibid., para. 345.

uses of force or unlawful interventions, i.e. there is no autonomous binding rule prohibiting violations of sovereignty.

To summarise, Corn and Taylor hold that the aforementioned cases "involved substantial military presence, de facto control of territory, and (…) violent operations, all of which implicate higher thresholds than the sovereignty-as-rule proponents assert".[198] Essentially, they mean that because these cases involved uses of force and interventions, sovereignty was only violated in the "broader sense".[199]

6.5 Evidence in International Fora

As mentioned above, the UNGGE Reports were used by the proponents of the violation of sovereignty rule in order to argue for its existence. Corn and Taylor, on the other hand, claim that "at no point has the [UNGGE] (…) identified sovereignty as a primary rule of international law" that prohibits certain low-intensity cyber operations.[200] They hold that the language of the reports is too "general and declaratory" to give rise to legally binding norms.[201]

[198] Corn and Taylor, *supra* note 18, p. 210, n. 14.

[199] Ibid.

[200] See Corn, Gary P.; Taylor, Robert – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Concluding Observations on Sovereignty in Cyberspace (The American Journal of International Law Unbound, Vol. 111, 2017) p. 282.

[201] Ibid.

7 Analysis of Sovereignty in Cyberspace – Underlying Principle or Primary Rule?

7.1 Introduction

There is common ground among both the proponents and the opponents of the existence of the violation of sovereignty rule that principles of international law apply to cyberspace and that there is a principle of sovereignty in international law. However, the proponents claim that the principle also functions as a rule and that violations of it constitute internationally wrongful acts whereas the opponents differentiate the principle from the rule, claiming that only the former exists in cyberspace. This chapter will assess the various arguments for and against the violation of sovereignty rule's existence. It will then analyse and conclude whether it currently forms part of customary international law. Finally, it will identify and analyse some practical benefits and risks of having such a rule.

7.2 Assessing the Arguments from Chapters 5 and 6 and Analysing the Status of Sovereignty in Cyberspace

When arguing against the existence of a primary rule on violations of sovereignty in cyberspace, Corn and Taylor emphasise that the principle of sovereignty is reflected differently in different domains. Referring to the long-standing practice of states engaging in espionage, they claim that as long as the espionage activity stays below the thresholds of unlawful intervention and use of force, it is not violating a rule of international law. By way of analogy, they argue that this also applies to cyberspace. This argument troubles me for two reasons. First, with respect to the lawfulness of espionage, Corn's and Taylor's rationale can be questioned. The fact that states have long engaged in the practice of espionage is not enough for the emergence of a customary rule allowing this practice. The long-standing practice must be accompanied by a sense of right (*opinio iuris sive necessitatis*), which is

absent in the case of espionage activities.[202] This lack of *opinio iuris* leads to the conclusion that the lawfulness of espionage is indeterminate.

Second, and more relevant to this thesis, Corn and Taylor are inconsistent in the sense that they apply analogic reasoning when such fits their agenda but argue strongly against it when it does not. As representatives of the US DoD, Corn and Taylor are of course concerned with advancing the interests of the US. And seeing as the US has great cyber capabilities, it is not surprising that Corn and Taylor are arguing for a broad leeway to engage in cyber espionage. However, the issue is that they are doing so by applying analogic reasoning while simultaneously claiming that the prohibition on violating another state's sovereignty in the various domains lacks analogous application for cyber operations. This contradiction strips Corn's and Taylor's argument of its value.

Recall that an unauthorised or unconsented law enforcement operation on the territory of a foreign state is a breach of Rule 4 because it usurps an inherently governmental function of that state. Corn and Taylor worry that this rule sets up hurdles for the US to conduct cyber operations against the cyber infrastructure of terrorist organisations located abroad. Leaning on this argument, they claim that the principle of sovereignty does not prohibit states from engaging in extraterritorial law enforcement operations. This is where their inconsistent application of analogic reasoning comes back to haunt them. If one recalls the reaction of the international community in the wake of the abduction of Eichmann, it clearly underscored how a state engaging in enforcement jurisdiction on the territory of another state without prior authorisation or consent acted unlawfully. If this rationale is to be applied analogously, an extraterritorial exercise of jurisdiction against the cyber infrastructure of a terrorist organisation would also be deemed as a violation of sovereignty of the state in which the infrastructure is located.

Moreover, although the objection that a primary rule on violations of sovereignty can complicate the carrying out of counter-terrorist cyber operations is legitimate, the fallacy of this argument is that it does not present evidence *de lege lata*. It is in fact an argument *de lege ferenda*, i.e. extraterritorial law enforcement operations should not be prohibited because that would tie the hands of those states wishing to carry out cyber operations to disrupt terrorist organisations. As such, this argument does not have bearing on the question of whether there

[202] Schmitt and Vihul, *supra* note 50, p. 1645.

currently exists a rule that prohibits certain low-intensity cyber operations as violations of sovereignty, which is a question of *lex lata* in its entirety.

The strongest argument of the sovereignty-as-principle-only proponents derives from the *DRC v. Uganda* case.[203] Referring to this case, Corn and Taylor emphasise that the ICJ, while mentioning violations of sovereignty several times, never established such a violation independently from the unlawful use of force and unlawful intervention. Corn and Taylor mean that this suggests that there is no independent rule prohibiting violations of sovereignty. Rather, the DRC's sovereignty was violated "in the broader sense".[204] Be that as it may, it is important not to neglect the many cases in which the Court has explicitly established a violation of sovereignty independently from an unlawful use of force or intervention. Most prominent among these cases are *Corfu Channel* and *Certain Activities*, in which the ICJ found violations of Albania's and Costa Rica's sovereignties respectively without even dealing with the issues of unlawful intervention and unlawful use of force.[205] The fact that it sufficed for the Court to establish an internationally wrongful act on the grounds of sovereignty violations clearly shows the independent nature of the violation of sovereignty rule. Thus, in my opinion, the findings of the Court in these latter cases outweigh the conclusion drawn by Corn and Taylor from the *DRC v. Uganda* case.

Corn and Taylor opine that there is not sufficient evidence of state practice and *opinio iuris* to claim that cyber operations below the thresholds of unlawful intervention and unlawful use of force are wrongful acts. This is obviously not true. As was shown in Chapter 5, there is a plethora of expressions of *opinio iuris* explicitly concerning the unlawfulness of low-intensity cyber operations. And with respect to state practice, one must bear in mind that verbal acts count as much as physical acts. While it is true that disclosed cyber-specific state practice is sparse with respect to physical acts, a glance at the state practice in other domains might prove useful. It merits reiterating that in order to draw conclusions about the *lex lata* in cyberspace, the chosen method of this thesis allows for analogising the rationale of an existing rule in domains with sufficient state practice to the domain of cyberspace.

What permeates the state practice presented in Chapter 5 is the treatment of the principle of sovereignty as a self-standing binding rule with operative effect. Recall that in the physical land domain, the exercise of enforcement jurisdiction on the territory of another state was

[203] DRC v. Uganda, *supra* note 194.
[204] Corn and Taylor, *supra* note 18, p. 210, n. 14.
[205] Corfu Channel, *supra* note 155, p. 35-36; Certain Activities, *supra* note 163, para. 96-97, 229.

characterised as a violation of that state's sovereignty. Also recall that in the aerial domain, instances of aircrafts entering the territorial airspace of another state without permission have consistently been labelled as violations of sovereignty. And recall finally, that in the maritime domain, instances of vessels sailing through the territorial waters of a state have also been marked as violations of the sovereignty of that state. The thread running through all of these cases is that the principle of sovereignty has been treated as a rule susceptible to violation and distinct from other rules that derive from the principle of sovereignty. Essentially, what has occurred – and what is characteristic of the deductive method – is that a specific rule (the violation of sovereignty rule) has been inferred from an already existing general principle (the principle of state sovereignty). Now, by drawing an analogy from the domains of land, sea, and air, the rationale and the validity of the violation of sovereignty rule can be extended to also apply in the domain of cyberspace.

Apart from the state practice supporting the existence of a primary rule on violations of sovereignty, the expressions of *opinio iuris* from states like China, France, the Netherlands, Russia, and the US (pre-Trump) have been major contributions to the formation of the rule. They show that these states have firmly and unequivocally joined the sovereignty-as-rule camp. Bear also in mind that it is inevitable that some states will contribute to the establishment and formation of a customary rule more than others. This might be due to their status, power, wealth, or their close relationship to the subject. Accordingly, if one considers that four out of the five states just mentioned are permanent members of the UNSC and that all of them have highly developed cyber capabilities, it is telling that their practice and *opinio iuris* carry much weight.

It is difficult to pinpoint exactly when a certain behaviour crystallises into a customary rule of international law. The metaphor of building a house may serve as illustration. When has the construction reached a point where it can be called a house? "It is neither when the first foundation stone is laid nor when the last brush of paint has been applied, but somewhere between the two".[206] Taking into account the sensitivity of determining at what exact point a rule hardens into customary international law, it can in my opinion – in light of the presented state practice and *opinio iuris* on the subject, and in light of the method applied – be concluded that there currently exists a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. This conclusion

[206] Scharf, Michael P. – Accelerated Formation of Customary International Law (ILSA Journal of International and Comparative Law, Vol. 20, Issue 2, 2014), p. 329-330.

is considerably more substantiated in terms of legal evaluation than the opposite conclusion, which to a large extent is influenced and supported by policy and national security considerations.

With all this having been said, the scope of the violation of sovereignty rule is not entirely clear. For example, remember that the GoE of the Tallinn Manual 2.0 could not reach consensus on whether cyber operations that fall foul of the physical damage and loss of functionality thresholds violate the sovereignty of a state (Subsection 4.2.1.1), such as a cyber operation that affects only data or emplaces malware into a system without causing physical damage or loss of functionality.[207] This means that the scope of the rule is still under formation and subject to the practice and *opinio iuris* of states. In this regard, France appears to have taken a leading role by declaring its view that even such cyber operations that only affect data or emplace malware into a system – without causing physical damage or loss of functionality – can indeed constitute violations of sovereignty.[208] Whether the violation of sovereignty rule will in fact extend to cover also these cyber operations will depend on if other states follow suit. Thus, the question that should be asked is not whether customary international law prohibits certain cyber operations as violations of sovereignty; it does. Rather, the question is which cyber operations qualify as violations of sovereignty. This is a question that is up for states to decide either through state practice and *opinio iuris* or by adopting a treaty regulating the question.

Of course, states are pragmatical in their international relations in the sense that they generally act in a way that is in tune with their interests. This can explain why the US and the UK deny that the principle of sovereignty constitutes a primary rule in its own right which is susceptible to violation. By not recognising the violation of sovereignty rule, the US and the UK attempt to uphold the operational leeway in which they conduct cyber operations below the thresholds of unlawful use of force and unlawful intervention. Of course, by not recognising the rule, they are simultaneously rejecting the protection that it provides. But seeing as the US and the UK are some of the states with the highest developed cyber infrastructure in the world, they perhaps see the operational leeway that enables advancing of their national interests in cyberspace as outweighing the lack of protection that derives from the absence of a primary rule on violations of sovereignty.

[207] Tallinn Manual 2.0, *supra* note 7, p. 21.
[208] Roguski, *supra* note 144.

7.3 Practical Benefits and Risks of a Primary Rule on Violations of Sovereignty

Cyber operations that do not qualify as unlawful interventions or uses of force can nonetheless have significant and undesirable effects. Take for example the exercise of cyber election meddling. In most cases of cyber election meddling, the aggressor state is affecting a matter falling under the targeted state's *domaine resérvé* but does not satisfy the second leg of the unlawful intervention test: coercion. In these cases, the cyber operation might very well be captured by the violation of sovereignty rule because it interferes with an inherently governmental function. Thus, the benefit of a primary rule on violations of sovereignty is that it can capture cyber operations that cause undesirable effects, but which absent such a rule would not have been prohibited because they would not cross the high thresholds of unlawful intervention or unlawful use of force. Taking into account that states face these undesirable low-intensity cyber operations on a daily basis, the existence of the violation of sovereignty rule is in tune with the rules-based international order.

Another benefit of having a primary rule on violations of sovereignty is that it helps the international community to work towards the overriding purpose of the UN – maintaining international peace and security – by reducing provocations of sovereignty in cyberspace. The approach that the principle of sovereignty only functions as a guiding principle rather than a binding prohibitive rule allows states to conduct cyber operations as long as they do not cross the unlawful intervention or unlawful use of force thresholds. Below these thresholds, states would be free to perform law enforcement functions through cyberspace on the cyber infrastructure located in another state, to interfere with the delivery of social services, or to interfere with the collection of taxes, just to mention a few examples. In such a state of affairs, the gloves are off. The risk of escalation of conflicts would surge and the realm of cyberspace would become increasingly unstable and disordered. Thus, the violation of sovereignty rule can have a cooling-off effect on states.

A third benefit of having a primary rule on violations of sovereignty is that low-intensity cyber operations can be condemned as internationally wrongful acts, resulting in the possibility to trigger the apparatus of state responsibility and to employ countermeasures. Without the violation of sovereignty rule, the targeted state would be unable to claim that it has been a victim of an internationally wrongful act, and thus to employ countermeasures. Of course, one could argue that if the violation of sovereignty rule did not exist in the first place

and if the targeted state's response would be held below the thresholds of unlawful intervention and unlawful use of force, the response would not in itself violate international law. The risk with this view is however, as was explained above, that conflicts can rapidly escalate and that even low-intensity cyber operations can be harmful.

The violation of sovereignty rule also entails certain risks which must not be neglected. It is a major concern for the international community that terrorist organisations, such as ISIS, use cyberspace to recruit members and incite violence. A troubling aspect of the violation of sovereignty rule in its purest form is that it can bar counter-terrorism cyber operations because such operations might usurp an inherently governmental function of another state. On the one hand, it is axiomatic that law enforcement functions reside at the heart of each state's sovereignty and must therefore be respected. But on the other hand, there is also a legitimate interest of countering acts of terrorism that threaten the territorial security of states and the well-being of citizens by e.g. disrupting or searching the cyber infrastructure of terrorist organisations located in foreign states.

A solution to this dilemma, which perhaps is already under way, is to develop a *lex specialis* regime of cyber sovereignty similar to that which has developed in the maritime domain. In the maritime domain, the territorial waters of coastal states are as a starting point inviolable. But exceptions such as innocent passage, transit passage, and archipelagic passage have developed through treaty law and customary law.[209] Considering the widespread interest of countering terrorism, it is not impossible that we might also see a *lex specialis* regime develop in cyberspace, allowing deviations from the main rule in order to undertake counter-terrorism cyber operations. Such an exception would however be entailed with great difficulty regarding its application, for interpretations of what the term 'terrorism' covers are greatly differing. Until a *lex specialis* regime allowing counter-terrorism cyber operations has hardened into international law, the *lex generalis* rule of respect for territorial sovereignty persists.

[209] Watts and Richard, *supra* note 178, p. 814; Schmitt and Vihul, *supra* note 50, p. 1645.

8 Closing Remarks

The main purpose of this thesis was to investigate whether there currently exists a rule of customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty.

After having explained the scopes of unlawful uses of force and unlawful interventions and related these to the scope of the violation of sovereignty rule, the thesis engaged in exploring the evidence and arguments for and against the existence of a primary rule on violations of sovereignty in cyberspace. These evidence and arguments originated from the practice and *opinio iuris* of states, as well as from decisions of international courts and statements in international fora.

Finally, after weighing and analysing the evidence and arguments and applying the chosen method, it was concluded that there currently exists a primary rule in customary international law that prohibits certain low-intensity cyber operations as violations of sovereignty. Once it was established that the principle of sovereignty functions as a prohibitive rule in cyberspace, the practical benefits and risks of the rule were identified and analysed. It was concluded that the future practice and *opinio iuris* of states will determine the exact shape and contours of the violation of sovereignty rule in cyberspace. Due to the widespread interest of combating terrorism, we might also see the emergence of a *lex specialis* regime providing exceptions to the *lex generalis* rule of inviolable sovereignty. But as of now, it is early days to claim that this possibility has crystallised to the point where it can be established as *lex lata*.

List of References

Treaties

Charter of the United Nations (1945).

Statute of the International Court of Justice (1945).

International Law Commission Report

Draft Articles on Responsibility of States for Internationally Wrongful Acts (International Law Commission, 2001).

UN Organs' Documents

United Nations Institute for Disarmament Research

Melzer, Nils – Cyberwarfare and International Law (UNIDIR Resources, 2011), [Melzer].

United Nations Security Council

SC/RES/138 Question relating to the case of Adolf Eichmann (1960), [Resolution 138].

United Nations General Assembly

GA/RES/2625 (XXV) Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (1970).

GA/DOC/A/68/98 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (2013).

GA/DOC/A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (2015).

Case Law

Permanent Court of Arbitration

Island of Palmas (United States of America v. The Netherlands), Arbitral Award, 1928, PCA, Case Nr. 1925-01.

Permanent Court of International Justice

Nationality Decrees Issued in Tunis and Morocco (France v. United Kingdom), Advisory Opinion No. 4, 1923, PCIJ, Series B. – No. 4.

S.S. Lotus (France v. Turkey, Judgment No. 9, 1927, PCIJ, Series A. – No. 10.

International Court of Justice

Corfu Channel (United Kingdom v. Albania), Judgment, ICJ Reports 1949, p. 4, [Corfu Channel].

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, ICJ Reports 1986, p. 14, [Nicaragua].

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, p. 226.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005, p. 168, [DRC v. Uganda].

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, ICJ Reports 2015, p. 665, [Certain Activities].

National Cyber Security Strategies and other Official Government Publications

China, National Cyberspace Security Strategy (27 December 2016), unofficial translation available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/, original Chinese text available at http://www.cac.gov.cn/2016-12/27/c_1120195926.htm, last visited 4 December 2019, [China NCSS 2016].

China, International Strategy of Cooperation on Cyberspace (1 March 2017), unofficial translation available at http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm, last visited 4 December 2019, [China ISCC 2017].

China and Russia, Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development (June 2016), available at https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm, last visited 4 December 2019.

France, Strategic Review of Cyber Defence (February 2018), available at http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf, last visited 4 December 2019.

France, Declaration on International Law in Cyberspace (September 2019), available at https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf, last visited 4 December 2019.

The Netherlands, Appendix: International Law in Cyberspace (September 2019), available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, last visited 4 December 2019.

United Kingdom, Wright, Jeremy – Cyber and International Law in the 21st Century (Speech at Chatham Royal Institute of International Affairs, 23 May 2018), available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, last visited 4 December 2019, [Wright].

United States, Department of Defense: Law of War Manual (Office of the General Counsel of the Department of Defense, June 2015, updated December 2016), available at https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual

%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190, last visited 4 December 2019.

Literature

Books

Abass, Ademola – Complete International Law: Text, Cases, and Materials (Oxford University Press, 2012).

Doswald-Beck, Louise; Henckaerts, Jean-Marie; International Committee of the Red Cross – Customary International Humanitarian Law: Volume I: Rules (Cambridge University Press, 2005), [ICRC].

Evans, Malcolm D. (ed.) – International Law (Oxford University Press, 2019).

Finkelstein, Claire; Govern, Kevin; Ohlin, Jens David (eds.) – Cyber War: Law and Ethics for Virtual Conflicts (Oxford University Press, 2015), [Finkelstein et al.].

Harrison Dinniss, Heather – Cyber Warfare and the Laws of War (Cambridge University Press, 2012).

Henriksen, Anders – International Law (Oxford University Press, 2017).

Jennings, Robert; Watts, Arthur (eds.) – Oppenheim's International Law: Volume I. Peace. Introduction and Part 1 (Longman, 1992).

Ruys, Tom – 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice (Cambridge University Press, 2010), [Ruys].

Schmitt, Michael N.; Vihul, Liis (eds.) – Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), [Tallinn Manual 2.0].

Shaw, Malcolm N. – International Law (Cambridge University Press, 2017), [Shaw].

Journal articles

Buchan, Russell – Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? (Journal of Conflict and Security Law, Vol. 17, Issue 2, 2012), p. 211-227, [Buchan].

Corn, Gary P.; Taylor, Robert – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber (The American Journal of International Law Unbound, Vol. 111, 2017), p. 207-212, [Corn and Taylor].

Corn, Gary P.; Taylor, Robert – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Concluding Observations on Sovereignty in Cyberspace (The American Journal of International Law Unbound, Vol. 111, 2017), p. 282-283.

Crootoft, Rebecca – Autonomous Weapon Systems and the Limits of Analogy (Harvard National Security Journal, Vol. 9, Issue 2, 2018), p. 51-83.

Dev, Priyanka R. – "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response (Texas International Law Journal, Vol. 50, Issue 2/3, 2015), p. 381-401.

Efrony, Dan; Shany, Yuval – A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice (The American Journal of International Law, Vol. 112, Issue 4, 2018), p. 583-657.

Ruys, Tom – The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)? (The American Journal of International Law, Vol 108, Issue 2, 2014), p. 159-210.

Scharf, Michael P. – Accelerated Formation of Customary International Law (ILSA Journal of International and Comparative Law, Vol. 20, Issue 2, 2014), p. 305-341.

Schmitt, Michael N.; Vihul, Liis – Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in Cyberspace: *Lex Lata Vel Non?* (The American Journal of International Law Unbound, Vol. 111, 2017), p. 213-218, [Schmitt and Vihul Symposium].

Schmitt, Michael N.; Vihul, Liis – Respect for Sovereignty in Cyberspace (Texas Law Review, Vol. 95, Issue 7, 2017), p. 1639-1676, [Schmitt and Vihul].

Spector, Phil - Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: In Defense of Sovereignty, in the Wake of Tallinn 2.0 (The American Journal of International Law Unbound, Vol. 111, 2017), p. 219-223, [Spector].

Talmon, Stefan – Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion (European Journal of International Law, Vol. 26, Issue 2, 2015), p. 417-443.

Watts, Sean – Low-Intensity Cyber Operations and the Principle of Non-Intervention (Baltic Yearbook of International Law, Vol. 14, Issue 1, 2015), p. 137-161, [Watts].

Watts, Sean; Richard, Theodore – Baseline Territorial Sovereignty and Cyberspace (Lewis & Clark Review, Vol. 22, Issue 3, 2018), p. 771-840, [Watts and Richard].

Internet sources

Delerue, Francois; Géry, Aude – France's Cyberdefence Strategic Review and International Law (Lawfare, 23 March 2018), available at https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law, last visited 4 December 2019.

Gellman, Barton – Cyber-Attacks by Al Qaeda Feared (The Washington Post, 27 June 2002), available at https://www.washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/, last visited 4 December 2019.

Geneva Internet Platform Digital Watch Observatory, available at https://dig.watch/processes/un-gge, last visited 4 December 2019.

Roguski, Przemyslaw – France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I (Opinio Juris, 24 September 2019), available at https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/, last visited 4 December 2019, [Roguski].

Väljataga, Ann – Tracing *opinio juris* in National Cyber Security Strategy Documents (NATO CCDCOE, 2018), available at https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf, last visited 4 December 2018, [Väljataga].

I, Sam Safi, was registered on this course for the first time in the autumn semester 2019. I have not been re-registered, nor have I participated in any previous examination.