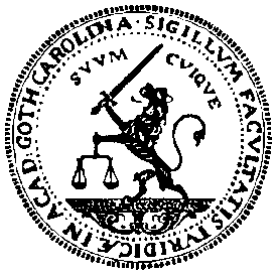

FACULTY OF LAW

Lund University

Tilda Cederlund

Cyber Sovereignty

The Application of the Principle of Sovereign Equality of States in Cyberspace and its Impact on Human Rights

LAGF03 Essay in Legal Science

Bachelor Thesis, Master of Laws program

15 higher education credits

Supervisor: Aurelija Lukoseviciene

Term: Autumn term 2023

Contents

Summary

The purpose of the essay is to examine different interpretations of the applicability of the principle of sovereignty on cyber operations which fall below the thresholds of the principle of non-intervention and the prohibition of the use of force. The essay also investigates how the applicability of the principle of sovereignty on these actions in cyberspace can affect the rights to freedom of expression and opinion.

The principle of sovereignty is particularly relevant when a cyber operation fails to reach the thresholds of a prohibited intervention or a use of force. To demonstrate the problematic nature of the uncertainty surrounding the principle of sovereignty in cyberspace, this essay will give an example of a situation which could be interpreted as falling short of both the aforementioned thresholds. Two opposing views of the applicability of the principle of sovereignty in cyberspace will be presented. Some scholars draw the conclusion that the principle is an independent rule of international law and that a breach of the principle can therefore be an internationally wrongful act and entail state responsibility. On the other side of the argument there are scholars who view the principle as an important guide for state's actions in cyberspace, however not binding for states.

The essay will conclude in an analysis of the problems presented above. The consequences to the human rights to freedom of expression and opinion will be demonstrated by applying both interpretations of the principle of sovereignty to the example presented in the essay. The essay reaches the conclusion that the principle of sovereignty is applicable in cyberspace, however that there is still disagreement in legal doctrine regarding what the applicability entails. Because of the harsh consequences the different interpretations of the principle of sovereignty can have on the human rights to freedom of expression and opinion, it is positive that states have started publicising their own interpretations of the applicability of international law in cyberspace. It could however be beneficial with more generally accepted

regulations on the area of cyberspace as well as further research on international law in cyberspace.

Sammanfattning

Uppsatsen siktar på att undersöka olika tolkningar av suveränitetsprincipens tillämpning på cyberoperationer som faller under trösklarna i våldsförbudet och non-interventionsprincipen. Vidare undersöks hur suveränitetsprincipens tillämpbarhet på dessa cyberoperationer kan påverka de mänskliga rättigheterna till yttrande- och åsiktsfrihet.

Suveränitetsprincipen blir särskilt relevant när en cyberoperation understiger de trösklar som finns i våldsförbudet och i principen om non-intervention. För att tydligt redogöra för problematiken som uppstår genom otydligheterna kring principen om statssuveränitet i cyberrymden kommer uppsatsen att belysa den med ett exempel på en cyber operation som kan anses understiga båda trösklarna.

Två motsatta tolkningar av suveränitetsprincipens applicering i cyberrymden presenteras. Å ena sidan kan tolkningen göras att principen är bindande för stater och att ett övertramp av suveränitetsprincipen i cyberrymden kan utgöra en internationellt felaktig handling. Å andra sidan kan en möjlig tolkning vara att principen snarare är en guide för stater i dess agerande i cyberrymden och att den således inte är bindande för stater.

Avslutningsvis går uppsatsen in på en analys av den problematik som presenterats i uppsatsen. Genom att applicera båda tolkningarna av suveränitetsprincipen i cyberrymden på det exempel som redogjorts för tydliggörs vilka svåra konsekvenser dessa kan få på två grundläggande mänskliga rättigheter.

Uppsatsen kommer fram till att principen om statssuveränitet är applicerbar i cyberrymden men att det finns osämja i doktrin angående vad begreppet ’applicerbar’ innebär. På grund av de svåra konsekvenser de olika tolkningarna av principen kan få för mänskliga rättigheter är det positivt att flera stater har börjat offentliggöra sina ståndpunkter gällande folkrättens tillämpning i cyberrymden. Det hade eventuellt varit fördelaktigt om det

framtogs ett mer generellt accepterat regelverk samt vidare forskning på området.

Abbreviations

ARSIWA	Draft Articles on Responsibility of States for Internationally Wrongful acts
UN	United Nations
UDHR	Universal Declaration of Human Rights
UNGGE	United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
ICJ	International Court of Justice
NATO	North Atlantic Treaty Organization
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
US DOD	United States of America Department of Defence
USA, US	the United States of America
UNHRC	United Nations Human Rights Council
ICCPR	International Covenant on Civil and Political Rights
AJIL	American Journal of International Law
UK	the United Kingdom
ISIS	the Islamic State in Iraq and Syria
ICT	Information and Communication Technology

1 Introduction

1.1 Background

In the relatively short time it has existed, the internet has become the central global public forum and it has a profound part to play for freedom of expression.[1] The mechanics of holding an opinion have evolved with technology, and in this evolution significant vulnerabilities have been exposed. Today, opinions are often held digitally, using for instance hard drives, the cloud or e-mail archives.[2]

Hospital's ability to contact doctors, voters' ability to obtain reliable information about candidates and the ability to find government recommendations in a pandemic are all things which are threatened if the internet or telecommunications services are shut down.[3] Despite the effects an internet shutdown can have, not least on the right to freedom of expression and opinion, governments around the world continue to order internet shutdowns.[4] The digital landscape of today gives states a new capacity to interfere with the rights of both the citizens of the state in question as well as the citizens of other states through cyber operations.[5]

The right to freedom of expression and to hold an opinion are very relevant in the cyber context, and it is understandable that there is concern about some states' attempts to curtail the right through legal perspectives on how cyberspace should be regulated.

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p. 5

[2] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p.8

[3] Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/50/55, p. 2, para 1

[4] Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/50/55, p. 5, para 19.

[5] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p. 3

According to ARSIWA, every internationally wrongful act conducted by a state entails responsibility for that state.[6] An internationally wrongful act by a state is an action or omission that is both attributable to the state and that constitutes a breach of an international obligation of that state.[7] Most States agree that cyber operations which amount to a use of force in accordance with article 2(4) of the UN Charter or a breach of the principle of non-intervention are violations of international law.[8]

What happens when a cyber operation falls below these thresholds? Such an operation could very well impact the human rights to freedom of expression and opinion. Can such operations be allowed? There are several different views on how states should act in cyberspace. One of the key points of disagreement is the concept of sovereignty. Some argue that the principle of sovereign equality of states is applicable and binding for states in cyberspace, and therefore that a cyber operation which breaches the sovereignty of another state can be wrongful. Others argue that the concept of sovereignty while it is a useful principle, is not legally binding for states.

1.2 Purpose and research questions

This essay aims to investigate the different interpretations of the application of the principle of state sovereignty on cyber operations which fall below the thresholds of the principle of non-intervention and the prohibition of the use of force. The essay also investigates how the applicability of the principle of sovereignty on these actions in cyberspace can affect the right to freedom of expression and opinion.

To achieve this purpose, the following questions will be answered:

- How can sovereignty be defined in the context of cyberspace?

[6] ARSIWA, art. 1
[7] ARSIWA, art. 2
[8] Corn & Taylor, Sovereignty in the age of Cyber, p. 208

- Is the principle of sovereign equality of states binding to states in cyberspace?

- How can different perspectives of the applicability of sovereignty in cyberspace affect the right to freedom of expression and the right to hold an opinion?

1.3 Delimitations

This essay will be written from an international law perspective. The sources will therefore be those of relevance to international law. The essay will not focus on questions in other legal areas which may arise when discussing sovereignty in cyberspace, such as for instance the protection of immaterial rights.

Human rights other than those mentioned above will not be explored in any depth. This is not because no other rights can be affected by different legal approaches to cyber space. On the contrary, several of the rights in the UDHR, such as for instance the rights to education, to freedom of association and assembly, to health, to work and to social and economic development could be equally affected.[9] However, in writing this essay there was the matter of space and time allotted to be considered.

The rights to freedom of expression and freedom of opinion were chosen because the impact of different interpretations of international law in cyberspace is very clear regarding these rights and it is mostly these rights that are discussed when concerns about the consequences of different regulations are discussed.

As mentioned in the background of this essay, the essay will be examining cyber operations which fall below the thresholds of use of force and non-intervention.

[9] Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/50/55, p. 3 para 7.

The question of attribution will not be examined in this essay, even though it is very relevant to establish state responsibility, especially in the context of cyber operations. The reason for this is that the subject of attribution of cyber operations is large and deserves a more in-depth exploration than the scope of this essay can offer.

The failure of the UNGGE in 2017 will not be accounted for since there is not enough space in the essay for a proper account.

1.4 Method and material

The method used in this essay will be the legal dogmatic method. Briefly explained, the method consists of trying to scientifically recreate a legal system. It is most frequently used to recreate *de lege lata* however there is nothing hindering a legal dogmatic argumentation from broadening the perspective to *de lege feranda.*[10] More concretely the legal dogmatic method is about finding answers in the generally accepted legal sources. These can be written law, legal practice, preparatory work, and doctrine.[11]

Since this essay will have an international law perspective, it is of certain importance to give an account of the sources used in international law. The ICJ utilises several sources when deciding disputes of international law, which can be found in article 38.1 of the ICJ statute. The main sources are international conventions, international customary law, and general principles of law recognised by civilised nations. Subsidiary to these sources the court also may apply judicial decisions and doctrine from highly qualified publicists.[12]

This essay will be examining questions regarding sovereignty in cyberspace. One difficulty with this subject is that there are very few treaties that directly deal with cyber operations, and the few that exist are of limited scope. There is also a lack of *opinio juris* on the subject and state cyber practice is often

[10] Jareborg, p. 4
[11] Nääv & Zamboni, p. 21
[12] ICJ Statute, art. 38.1

classified.[13] Some reports to the general assembly will be used, as well as general assembly resolutions. The essay will however, due to the subject at hand, mostly be using reports and resolutions from the human rights council and the high commissioner for human rights. Because of the lack of treaties and *opinio juris* the essay will place a larger focus on doctrine and international customary law. In doing so the Tallinn Manual 2.0 will be used to a rather large extent.

The Tallinn Manual 2.0 is not an official document. The manuals were written by an international group of experts at the invitation of the NATO CCD COE.[14] The rules in the manuals are intended to reflect international customary law as applied in the cyber context.[15] Supposing the rules in the manuals accurately articulate customary international law, the manual is legally binding for states (except for possible persistent objectors). However far from all states agree to the interpretations in the manual, and it is unclear whether the rules reflect international customary law. Even still, the manuals have become an important material which states refer to when discussing cyber operations.[16]

The first Tallinn Manual, published in 2013, addressed the most severe cyber operations. The second manual, published in 2017, continued by considering the rules of international law governing cyber incidents which fall below the thresholds of the use of force or armed conflict.[17] It is the second manual which will be referenced further on in this essay.

1.5 Disposition

Initially, this essay aims to give a definition of some essential terms which will be used in the essay. This is done to give a greater understanding of the material moving forward.

[13] Schmitt, p. 3
[14] Schmitt, p. 1
[15] Schmitt, p. 4
[16] Wiktorin, s. 52
[17] Schmitt, p. 1

The essay will thereafter move into further exploration of the human rights to freedom of expression and freedom to hold an opinion in the context of cyberspace. This discussion will lead to a review of a discussion in doctrine concerning the principle of sovereignty in cyberspace as well as Sweden's national position on the topic.

The essay will conclude, in the final chapter, with an analysis of the various perspectives and arguments.

2 Discussion

2.1 Definitions

Several of the terms required to understand the topic of this essay lack a legal definition. To move forward it is therefore important to investigate the use of these terms and their meaning.

2.1.1 What is cyberspace?

During most of human history our worldview was divided into land and sea. This changed in the early 20th century, first with the addition of aerospace and then outer space to the areas we had the ability to explore and utilize. Cyberspace is different in the way that it is an invisible, non-physical space which makes it challenging to regulate. [18]

Since there is no legal definition of cyberspace, it is necessary to look to military definitions. The US DOD defines cyberspace as:

> A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[19]

Large parts of the infrastructure and systems of society today are decidedly dependent on cyberspace for their continuing functionality. These dependencies make our systems vulnerable to outside intervention.[20] It is therefore relevant and important to examine how and if the principles of international law are applicable to cyberspace.

[18] Ericson, p. 35–36
[19] DOD Dictionary, page 55
[20] Ericson, p. 36

2.1.2 Cyber attacks and cyber operations

The term cyber attack will be used as a term with a specific meaning. A cyber attack is defined in the Tallinn Manual 2.0 as a cyber action, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[21] A cyber attack can therefore be understood as an operation which breaches the prohibition of use of force under article 2(4) of the UN Charter.[22]

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[23]

There is a consensus that actions in cyberspace which result in death, injury, significant destruction, or that represent an imminent threat thereof, constitute a use of force.[24]

To fully understand the concept of a cyber attack it is also important to define the term cyber operation. As was the case with the term cyberspace, there is no legal definition of the term cyber operation. Going forward, the term will be used to describe acts in cyberspace which do not amount to cyber attacks.

Article 2(7) of the UN Charter is usually interpreted as dealing with the prohibition against intervening in the internal affairs of other states, that is to say, the principle of non-intervention.[25] The principle of non-intervention is defined by the ICJ in *Nicaragua*. The court found that the principle of non-intervention prohibits direct or indirect intervention by states in internal or external affairs of other states. A prohibited intervention subsequently must concern matters which each state normally is permitted by the principle of sovereignty to decide freely on. According to the court intervention is wrongful when it uses coercion. The element of coercion is said to define and

[21] Schmitt, p. 415
[22] Ericson, p. 39
[23] UN Charter, Article 2(4)
[24] Corn & Taylor, Sovereignty in the Age of Cyber, p. 208
[25] Wiktorin, p. 57

form the very essence of prohibited intervention.[26] However, it is important to remember that not all acts qualify as 'coercive', only acts of a certain magnitude that are intended to force a policy change in the target state would breach the principle.[27] Similarly to acts in cyberspace which breach the prohibition of the use of force, there is a general agreement that cyber operations which amount to a prohibited intervention violate international law.[28]

2.1.3 Sovereignty in cyberspace: physical, logical, and social layer

There is a generally agreed upon definition of the principle of state sovereignty in the Island of Palmas arbitral award from 1928.[29] Sovereignty in the relations between states is defined as signifying independence. The arbitration adds that independence regarding a part of the globe is the right to exercise, to the exclusion of other states, the functions of a state in that area.[30]

Article 2(1) of the UN Charter declares that the UN is based on the principle of the sovereign equality of all members.[31] The rules in article 2(4) and (7), are interpreted as signifying that states have supreme authority within its territory and is protected from the intervention of other states.[32]

The legal right to assert control over cyberspace and the internet is essential for the argument of sovereignty in cyberspace.[33] Rule 1 of the Tallinn manual contains the general principle of sovereignty in cyberspace. The rule declares that the principle of sovereignty applies in cyberspace.[34]

[26] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, (1986), p. 107-108, para 205
[27] Jamnejad & Wood, p. 348
[28] Corn & Taylor, Sovereignty in the Age of Cyber, s. 208
[29] Schmitt, p. 11
[30] *Island of Palmas case (Netherlands, USA)*, (1928), p. 838
[31] UN Charter, art. 2(1)
[32] Delerue, p. 202-203
[33] Ericson, p. 109
[34] Schmitt, p. 13

Sovereignty has both an internal and an external element. Internal sovereignty gives the state a right to independently decide on the political, social, cultural, economic, and legal order of the state.[35] In the context of cyberspace, internal sovereignty gives the state freedom to adapt any measure it regards as necessary or appropriate concerning cyber infrastructure, persons engaged in cyber activities or for that matter the activities themselves within the territory of the state. This applies with the exception of cases where the state is hindered from doing so by international law binding to the state, such as human rights law.[36]

The external aspect of sovereignty gives a state the right to be independent from other states in its international relations. In the context of cyberspace, this means a state is free to engage in cyber activities beyond the territory of the state and that the state is only subject to international law.[37]

There are three so-called layers of cyberspace which are included in the principle of sovereignty in cyberspace: the physical layer, the logical layer, and the social layer.[38]

The first layer is the physical layer which consists of devices, servers and other types of infrastructure physically placed in the territory of a state.[39]

The second layer is described as the logical layer. This layer consists of the actual data and code. It is in this layer that cyberspace becomes non-territorial. The data and code move between different points of connection in the physical layer. It can often travel between points in the physical layer which are situated in several different states. The fact that the logical layer is non-territorial does not mean the layer is excluded from state jurisdiction. States can still argue their jurisdiction over whatever passes through the physical

[35] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, (1986), p. 123, para. 263
[36] Schmitt, p. 13
[37] Schmitt, p. 16
[38] Schmitt, p. 13
[39] Ericson, p. 109

layer as well as the people in their physical territory. A person writing or communicating code in a state is under the jurisdiction of that state.[40]

The third and final layer of cyberspace is called the social layer. In this layer a state may regulate the cyber activities of both natural and legal persons within its own territory.[41] In this layer some states actively filter to prevent free information exchange, while others filter for crimes committed in cyberspace such as the spreading of child pornography.[42]

2.2 Human rights in cyberspace – freedom of expression and freedom of opinion

The UNHRC has found that individuals enjoy the same rights in cyberspace as they in the real world, and that the human rights should be equally protected by states regardless of if they are exercised online or offline.[43] This is reflected in the Tallinn Manual 2.0 which affirms international human rights law is applicable to cyber-related activities and that individuals possess the same international human rights regarding cyber related activities as they do otherwise.[44]

There is no definitive catalogue of customary international human rights law.[45] The UDHR has however been described as a 'common understanding' of the peoples of the world concerning human rights and it has been said to constitute an obligation for the members of the international community.[46]

The right to freedom of expression is found in article 19 of the UDHR.

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and

[40] Ericson, p. 109-110
[41] Schmitt, p. 14
[42] Ericson, p. 110
[43] UNHRC res. 47/16, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/47/16 (13 July 2021), p. 3, para 1
[44] Schmitt, p. 182, 187
[45] Schmitt, p. 180
[46] United Nations, International Conference on Human Rights, Final Outcome Document, A/CONF.32/41 (13 May 1968), p. 4, para 2

> to seek, receive and impart information and ideas through any media and regardless of frontiers.[47]

Furthermore, the rights to freedom of opinion and expression have been codified in several universal and regional agreements, such as for instance the ICCPR which, at the time of writing, 173 states are currently party to.[48] To the states which are not party to the ICCPR it still presents a standard for achievement and often reflect customary legal norm.[49] The right to freedom of opinion and expression can be found in article 19 of the ICCPR which largely echoes article 19 of the UDHR. Article 19.1 states that everyone has the right to hold opinions without interference and article 19.2 states that everyone has the right to freedom of expression which includes the freedom to seek, receive and impart all kinds of information regardless of frontiers. The rights in article 19.2 may be subject to restrictions, but only if the restrictions are provided by law and are necessary:

A) For respect of the rights or reputations of others;

B) For the protection of national security, public order, public health, or morals.[50]

Article 2.1 of the ICCPR gives each state party to the covenant an obligation to respect and to ensure the rights recognised in the covenant to all individuals within its territory and subject to its jurisdiction without any kind of distinction.[51] Restrictions to the rights given in the covenant must be permissible under the relevant provisions to the covenant and the state wishing to make a restriction must be able to demonstrate the necessity of the

[47] UDHR, article 19

[48] United Nations Human Rights High Commissioner, ICCPR Status of ratification interactive dashboard, 2023-12-29.

[49] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p. 6

[50] ICCPR article 19.3

[51] ICCPR, article 2.1

restriction. Moreover, a state may only take measures which are proportionate to the legitimate aim of the restriction.[52]

In the context of cyberspace states cannot partake in activities that violate the human rights of individuals in cyberspace.[53] With the exception of human rights that are absolute in nature, the obligations can however be subjected to certain limitations that are necessary to achieve a legitimate purpose, non-discriminatory and authorised by law.[54]

Absolute rights are the rights which may not be restricted by states for any reason. One such right is the right to hold opinions freely without interference. Although this right is often associated with freedom of expression, international human rights law has drawn a conceptual line between the two. This distinction is caused by the view that the ability to freely hold an opinion is a fundament to both human dignity and democratic self-governance and therefore the right is such a critical guarantee that no interference, limitations, or restrictions can be allowed.[55]

Traditionally there has been much less attention placed on the right to freely hold opinions than there has been to the right to freedom of expression. However, holding an opinion in the digital age is not as abstract a concept as it has once been. As mentioned in the introduction to this essay, the mechanics of holding an opinion has evolved with technology, and this evolution has unveiled significant vulnerabilities. Interference in the cyber context can involve targeted harassment of individuals and civil society organisations for the opinions they hold and can happen in many formats, such as targeted surveillance, online and offline intimidation, and criminalisation.[56]

[52] UN Human Rights Committee, General Comment No. 31 (80) The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/GC/34, 2004, p. 3, para 6

[53] Schmitt, p. 196

[54] Schmitt, p. 201-202

[55] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p. 8

[56] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, p.8-9

Regarding the requirement of necessity, it should be noted that states have some margin of appreciation. Nevertheless, measures which are necessary to achieve one legitimate aim may not be necessary for the purpose of achieving another such aim.[57] For instance, a blanket internet shutdown generally does not meet the requirements in article 19.3 ICCPR since it can affect many legitimate activities and even put people's safety at risk. However a more targeted shutdown can be permissible depending on the proportionality.[58]

2.3 Example – Sony Pictures Entertainment

In 2014 the American company Sony Pictures Entertainment was hacked. The hackers stole a significant amount of data from the company and demanded that Sony Entertainment cancel the release of the movie *The Interview* which was a satirical film about the assassination of the North Korean leader Kim Jong-un.[59]

The attack was allegedly sponsored by North Korea, according to United States officials.[60] The hacking of Sony Entertainment did not result in death, injury, or significant destruction; therefore, it can hardly be said to have amounted to a use of force in accordance with article 2(4) of the UN Charter.

In a statement after the attack Secretary Jeh Johnson of the US Department of Homeland Security said that the hack against Sony Entertainment "was not just an attack against a company and its employees. It was also an attack on our freedom of expression and way of life".[61] The freedom of expression and way of life in a state could be considered something a state is normally able to freely decide upon. However, it is unlikely that an operation such as this one against a private entertainment company would be regarded as directly or

[57] United Nations, Human Rights Council, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 2014, p. 9, para 27

[58] Human Rights Council Res. 47/16, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/47/16 (13 July 2021), p. 4

[59] Delerue, p. 239

[60] Delerue, s. 240

[61] Statement By Secretary Johnson on Cyber Attack On Sony Pictures Entertainment, 2014

indirectly aiming to coerce the United States.[62] It is therefore unlikely that the hack of Sony Entertainment would constitute a violation of the principle of non-intervention.

Is the act therefore allowed even if it would affect the freedom of expression of the citizens of the USA? The answer depends on whether one views the principle of sovereignty as legally binding or not.

2.4 Perspectives on sovereignty in cyberspace

According to the Tallinn Manual 2.0, the principle of sovereignty applies in cyberspace,[63] and states must not conduct cyber operations that violate the sovereignty of another state.[64] The interpretation of the principle of sovereignty presented in the manual is not entirely uncontroversial.

Two conflicting views will now be accounted for, using an AJIL unbound symposium as background.

There are scholars who are of the view that while sovereignty is an important principle of international law, it is not itself a binding rule for states. In the symposium this view is accounted for by Gary Corn and Robert Taylor, who have both served as lawyers for the US DoD.[65] Corn and Taylor argue that there is insufficient evidence of state practice and *opinio juris* to support the claim that the principle of sovereignty is an independent rule of international customary law.[66]

There are those who contest Corn and Taylor's interpretation of the principle of sovereignty. Michael Schmitt and Liis Vihul, the head and managing editor of the Tallinn Manual 2.0 project, argue that the principle of sovereignty is a safeguard for territorial integrity and inviolability. According to Schmitt and

[62] Delerue, p. 240
[63] Schmitt, p. 11
[64] Schmitt, p. 17
[65] Ginsburg, p. 205
[66] Corn & Taylor, Sovereignty in the Age of Cyber, p. 208

Vihul, disregard for another state's territorial integrity and inviolability can constitute an internationally wrongful act.[67]

Corn and Taylor view the principle of sovereignty as a guide for state interaction and argue that although the principle should be a factor to be considered in every cyber operation, it does not prevent cyber operations in another state if the effects do not rise to the level of an unlawful use of force or an unlawful intervention.[68]

Schmitt and Vihul contest that this view of the principle of sovereignty is internally inconsistent because the question of whether the principle of sovereignty protects a state from cyber activities is binary, it either does or does not. Corn and Taylor's interpretation of the principle as on the one hand not preventing a cyber operation against another state but on the other hand that it must be considered before a cyber operation is therefore inconsistent. Instead, Schmitt and Vihul conclude that if the principle of sovereignty requires states to consider the sovereignty of another state before a cyber operation, then the answer to the aforementioned question appears to be positive.[69]

Corn and Taylor claim that there is insufficient evidence of either state practice or *opinio juris* to support the idea that the principle of sovereignty is an independent rule of international customary law which regulates states' actions in cyberspace.[70] However, in the symposium, Phil Spector disagrees and contends that there are treaties, jurisprudence, and scholarly opinion which contradict this claim.[71] In response to the claim that the principle of sovereignty is only a background principle rather than a primary rule of international law, Spector refers to several sources including, inter alia, UN resolution on Friendly Relations which is understood to reflect international customary law.[72] According to the resolution the principle of sovereign

[67] Schmitt & Vihul, p. 213-214
[68] Corn & Taylor, Sovereignty in the Age of Cyber, p. 208-209
[69] Schmitt & Vihul, p. 214-215
[70] Corn & Taylor, Sovereignty in the Age of Cyber, p. 208
[71] Spector, p. 222
[72] Spector, p. 220

equality of states entails that all states are equal members of the international community and that they have equal rights and duties. Sovereign equality includes the right for each state to enjoy full sovereignty, and each state has a duty to respect the personality of other states. The resolution also declares that the territorial integrity and political independence of a sovereign state are inviolable.[73]

The ICJ has also addressed violations of sovereignty, for instance in the Corfu Channel case. The court found that the UK had violated the sovereignty of Albania when carrying out a minesweeping operation in Albania's territorial waters.[74] Schmitt and Vihul especially note that the action by the UK only constituted a violation of sovereignty, not an unlawful intervention or a use of force. The violation of sovereignty was grounds enough for the court to be able to pass judgement.[75]

Corn and Taylor oppose the sources used by Schmitt, Vihul and Spector, and argue that they have looked to sources dealing with very different domains and activities in an attempt to discern a rule where there is no binding law. Corn and Taylor highlight the fact that the UNGGE, which is the only international body charged with the task of examining how international law applies to cyber operations, has never identified sovereignty as a primary rule of international law.[76]

Corn and Taylor use the example of cyber operations against ISIS to exemplify the difficulties that would occur if states seeking to interfere with terrorist cyber infrastructure were to be under an obligation to seek either consent from the state in question or authorisation from the security council before conducting the operation. ISIS has a strong presence online, using social media and the internet to communicate with its members. Followers of

[73] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625(XXV, p. 124

[74] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania*), p. 35

[75] Schmitt & Vihul, p. 215

[76] Corn & Taylor, Concluding Observations on Sovereignty in Cyberspace, p. 282

ISIS, both inside and outside ISIS-controlled territory can operate on servers around the globe, and the states that have these servers under their sovereign authority may never have knowledge of it. There is also the possibility that the state in question does not have the capability to counter ISIS presence in the cyber sphere. In that case, according to Corn and Taylor, the obligation to seek permission from the state or authorisation from the security council would impede efforts to disrupt terrorist cyber infrastructure. Because of the nature of cyber operations, the ability to effectively counter terrorists in the cyber sphere requires the flexibility to act quickly. It could therefore render response options unworkable if states had to operate through a consent model.[77]

Schmitt and Vihul find Corn and Taylor's example regarding ISIS concerning because it seems to imply that cyber operations in another state would be permissible if undertaken to counter terrorist activities. Such an approach could be damaging since definitions of the term "terrorism" could differ drastically depending on the state. An open-ended definition of the term could have devastating consequences for the right to freedom of expression.[78] For instance in China where the current definition of terrorism may be interpreted as attempting to punish thoughts or speech of terrorists.[79] The definition in the Chinese terrorism legislation could include nonviolent dissident activities and certain exercises of speech.[80]

Corn and Taylor conclude that it remains for states to consider the differentiation of what is lawful and what is not in the cyber sphere, outside of the established primary rules against use of force and unlawful intervention.[81]

In their concluding remarks, Schmitt and Vihul are concerned that some states argue for strong sovereignty rather than a free and open cyberspace. Schmitt and Vihul find this trend alarming for liberal democracies. The authors

[77] Corn & Taylor, Sovereignty in the Age of Cyber, page 211
[78] Schmitt & Vihul, p. 217
[79] Zunyou, p. 84
[80] Schmitt & Vihul, p. 217
[81] Corn and Taylor, Concluding Observations on Sovereignty in Cyberspace, p 282-283.

however find that Corn and Taylor take the opposition to sovereignty too far. Schmitt and Vihul argue that states, instead of denying the existence of the rule prohibiting violations of sovereignty, should work together to map the parameters of such a rule.[82]

In recent years, states have started publicly formulating interpretations of the application of international law in cyberspace. Sweden's position on the application of international law in cyberspace was released by the Government Offices of Sweden in July 2022. Sweden's views on the principle of sovereign equality of states largely reflect the interpretation in the Tallinn Manual. The principle is said to be fundamental for other norms, such as the prohibition of unlawful intervention and the use of force, as well as a rule in and of itself. According to the Swedish interpretation, the principle of sovereign equality also presents states with an obligation to respect the sovereignty of other states. If a state breaches this obligation the action would amount to a wrongful act and could therefore entail state responsibility.[83]

[82] Schmitt & Vihul, p. 218

[83] Government Offices of Sweden, 2022, Position Paper on the Application of international Law in Cyberspace, p. 2

3 Analysis

The aim of this essay was to investigate the different interpretations of the application of the principle of sovereignty in cyberspace within the framework of international law and how these interpretations can affect the right to freedom of expression and opinion. I will now attempt to answer the research questions posed in the introduction to this essay.

3.1 Sony Entertainment

The example of the hacking of Sony Entertainment is interesting because it could be an example of a cyber operation that does not reach either of the two thresholds presented in this essay. It is neither an unlawful use of force nor a prohibited intervention. It is therefore an example of the exact problem that the uncertainty regarding the application of the principle of sovereignty in cyberspace poses.

The operation was conducted against a private company located in the USA, with the presumed purpose to stop the release of a film. The company is located in the USA, so the conclusion can be made that the operation infringed on the physical layer of cyberspace since the servers in all probability are located on American territory. However, even if they are not, it would still infringe on the logical layer since Sony Pictures Entertainment is an American company.

If interpreted, as an attack on the American freedom of expression and way of life but not, as presented in chapter 2.3, as a direct or indirect coercion against the United States, this could be viewed as a breach of the principle of sovereignty. The freedom of expression and way of life, or organisation of the state, is normally something which falls under the sovereignty of that state. Therefore, the hack is intruding on the sovereignty of the USA.

If one views the hacking of Sony Entertainment through both perspectives on the principle of sovereignty in cyberspace, the answer to whether it is an allowed cyber operation is drastically different depending on the perspective used.

In the perspective of the Tallinn Manual 2.0, as presented by Schmitt and Vihul, the operation against Sony Entertainment could be viewed as a breach of international law. If the act is attributed to another state and interpreted as wrongful it could give the target state several rights under international law.

Because the Swedish interpretation of existing international law in cyberspace is quite similar to the rules given in the Tallinn Manual 2.0 there is a high probability that a hack such as the one on Sony Entertainment in Sweden would similarly be viewed as a breach of international law.

However, if one instead views the situation above from the perspective of Corn and Taylor, the conclusion might be different. If the interpretation of the hack is accepted and it is not seen as a breach of either the prohibition of use of force or an unlawful intervention the question then is if the hack would be seen as an allowed cyber operation under international law. The answer, in this view, would in all probability be yes. Since Corn and Taylor argue that the principle of Sovereignty in cyberspace is not legally binding, an act under the threshold of article 2(4) or (7) of the UN charter would not be seen as wrongful. The targeted state, in this case the USA, would therefore not have the same rights according to Corn and Taylor in this scenario as it would in the view of Schmitt, Vihul and Spector.

3.2 The right to freedom of expression and the right to hold an opinion

The uncertainty surrounding the principle of sovereignty could be unfortunate seen from a human rights perspective. Both ways of viewing the principle of sovereignty in cyberspace could have consequences on several of the rights in the UDHR.

If one interprets the principle as a binding norm of international customary law, a breach of the principle (depending on the attribution to another state) could give the targeted state several rights in relation to the state conducting the cyber operation. However, such an interpretation could perhaps also give rise to some concern related to human rights, which even Schmitt and Vihul appear to concede in their concluding remarks.

It is important to recall that cyberspace has a profound role for the right to freedom of expression and opinion in the digitalized society of today. One reason for this, presumably, is the global nature of the internet, as a central global public forum. What then could a stronger sovereignty in cyberspace mean for the human right to freedom of expression and opinion in states where those rights are targeted by a strong desire for control? As previously discussed in chapter 2.1.3, internal sovereignty gives the state freedom to adapt any measure it regards as necessary or appropriate concerning cyber infrastructure, persons engaged in cyber activities or activities within the territory of the state. A stronger principle of sovereignty online could increase practice such as internet shutdowns and impede the rights to freedom of expression and opinion on the internet in states wishing to control the social layer of cyberspace. However, it is also important to remember the limitations posed in article 19.3 of the ICCPR regarding freedom of expression. A blanket internet shutdown might not meet the requirements, but a more targeted shutdown could. Further research on this topic could be useful in order to protect freedom of expression and opinion online

However, the interpretation presented by Corn & Taylor, could perhaps be seen as going too far in the opposite direction. If one views the principle of sovereignty as only a guide for states in their international operations and not as a binding rule of international law, a cyber operation in breach of the principle of sovereignty which does not amount to a use of force or a prohibited intervention could not be seen as an internationally wrongful act. This would entail that states are free in their international relations to conduct such cyber operations in other states as long as the operations do not amount to either threshold. This could have severe negative consequences for the

rights to freedom of expression and opinion, among other human rights, as has been accounted for in previous chapters.

The right to freedom of expression and the freedom to hold an opinion, especially in recent decades, has become increasingly interconnected with cyberspace. Not only that, but essential services today often rely on ICTs and the internet to function. Disruptions or shutdowns of these services therefore can lead to negative effects on several human rights. If a state, through a cyber operation which does not amount to a use of force, disrupts the internet in another state or region thereof there is no guarantee that this will result in a prohibited intervention, for instance if there is no element of coercion. This does not automatically mean that there would be no consequences for the targeted state. An internet shutdown which falls below the thresholds in article 2(4) and (7) of the UN Charter can still result in the limitation of people's right to freedom of expression or freedom to hold an opinion. States could stop the release of films, shut down blogs, digital meetings, and other forms of expression.

3.3 Is the principle of sovereignty legally binding in cyberspace?

The question does not have a straightforward answer. It can be said that there exists some consensus that the principle is applicable in cyberspace, there is however no harmony on the topic of what the applicability entails.

It would perhaps be positive if a more generally accepted approach was developed, such as mapping the parameters of the principle of sovereignty in cyberspace. This would generate common practices and provide states with more clear frames on how to conduct cyber operations abroad. It would also be positive if there were a generally accepted approach since it could provide accountability in the case of a wrongful cyber operation. A clear and common approach could presumably be positive for the targeted state because it could clarify what measures the state has available in response to the operation. However, in developing such a strategy it would be crucial that the unique

perspective of cyberspace, the internet's role as a central public forum and the rights to freedom of expression and opinion are central.

The principle of sovereignty in cyberspace is a rather controversial subject and due to the fundamentally different approaches it is perhaps unlikely that such an approach will be presented in the near future. For the clarity of the international community, it is therefore positive that states have started publicly announcing their interpretations on the subject. It would be interesting to see more research on the subject in future, especially including the question of attribution to operations conducted in cyberspace.

Bibliography

International law sources

United Nations, *Charter of the United Nations*, (entered into force 24 October 1945) 1 UNTS XVI

United Nations, *Universal Declaration of Human Rights* (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

United Nations, *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

United Nations documents

United Nations International Conference on Human Rights, Final Outcome Document, para. 2, UN Doc. A/CONF.32/41 (13 May 1968), available from https://undocs.org/Home/Mobile?FinalSymbol=A%2FCONF.32%2F41&Language=E&DeviceType=Desktop&LangRequested=False (accessed 2023-11-24)

General Assembly resolution 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*, A/RES/2625(XXV), (24 October 1970), available from https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf (accessed 2023-12-29)

United Nations Human Rights Committee, General Comment No. 31 (80) The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/GC/34, (29 March 2004), available from https://digitallibrary.un.org/record/533996 (accessed 2023-12-12)

United Nations, Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for*

Human Rights, A/HRC/27/37 (30 June 2014), available from https://digitallibrary.un.org/record/777869 (accessed 2023-11-26)

United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* A/HRC/29/32 (22 May 2015), available from https://digitallibrary.un.org/record/798709 (accessed 2023-11-26)

United Nations, Human Rights Council, Resolution 47/16, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/47/16 (13 July 2021), available from https://digitallibrary.un.org/record/3937534 (accessed 2023-12-12)

United Nations, Human Rights Council, *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights: report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/50/55 (13 May 2022), available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/55/PDF/G2234155.pdf?OpenElement (accessed 2023-12-12)

Soft Law Documents

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, November 2001, Supplement No. 10 (A/56/10), cph.IV.E.1, available from https://www.refworld.org/docid/3ddb8f804.html (accessed 2023-12-29)

Judgements

Island of Palmas Case (Netherlands, USA), Reports of International Arbitral Awards, April 1928

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgement of 9 April 1949

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) Merits, Judgement of 27 June 1986

Literature

Corn, Gary & Taylor, Robert (2017), 'Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber'. *American Journal of International Law*, Unbound symposium, Cambridge University Press, p. 207-212

Corn, Gary & Taylor, Robert (2017), 'Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Concluding Observations on Sovereignty in Cyberspace' *American Journal of International Law*, Unbound symposium, Cambridge University Press, p. 282-283

Delerue, François, *Cyber operations and international law*, first paperback edition, Cambridge University Press, Cambridge, 2021 (2020)

Ericson, Marika, *On the Virtual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and War: Aspects of International and Swedish Domestic Law*, Uppsala Universitet, Uppsala, 2020

Ginsburg, Tom (2017), 'Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0'. *American Journal of International Law*, Unbound symposium, Cambridge University Press, p. 205-206

Jamnejad, Maziar & Wood, Michael (2009), ‘The Principle of Non-intervention’ *Leiden Journal of International Law,* Cambridge University Press, p. 345-381

Jareborg, Nils (2004) ‘Rättsdogmatik som vetenskap’, SvJT, s. 1-10.

Nääv, Maria & Zamboni, Mauro (ed.), Juridisk metodlära. Second edition, Studentlitteratur, Lund, 2018

Schmitt, Michael N. (ed.), Tallinn manual 2.0 on the international law applicable to cyber operations, Second edition., Cambridge University Press, Cambridge, 2017

Schmitt, Michael, Vihul, Liis (2017), ‘Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Select Sovereignty in Cyberspace: Lex Lata Vel Non?’*American Journal of International Law*, Unbound symposium, Cambridge University Press, p. 213-218

Spector, Phil (2017), ‘Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Select Sovereignty in Cyberspace: Select In Defense of Sovereignty, in the Wake of Tallinn 2.0’*American Journal of International Law*, Unbound symposium, Cambridge University Press, p. 219-223

Wiktorin, Johan (ed.), *Cyberförsvaret: en introduktion*, Kungl. Krigsvetenskapsakademien, Stockholm, 2022

Zhou, Zunyou, *Fighting Terrorism According to Law: China’s Legal Efforts against Terrorism*, in Michael Clarke (ed.), *Terrorism and Counter-Terrorism in China: Domestic and Foreign Policy Dimension*s, (2018; online edition, Oxford Academic, 21 Feb. 2019),

Other materials

Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment, December 19 2014, Available from

https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment (accessed 2023-11-14)

Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington DC: The Joint Staff, 2021, Available from: https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477-1.pdf (accessed 2023-12-14)

Government Offices of Sweden, Report from Ministry of Foreign Affairs, *Position Paper on the Application of international Law in Cyberspace*, July 2022, available from https://www.government.se/reports/2022/07/position-paper-on-the-application-of-international-law-in-cyberspace/ (accessed 2023-12-08)

United Nations Human Rights High Commissioner, ICCPR Status of ratification interactive dashboard, available from https://indicators.ohchr.org/ (accessed 2023-12-29)