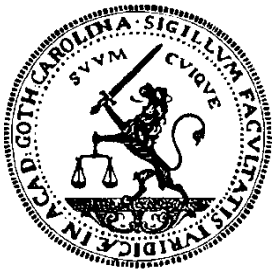

FACULTY OF LAW
Lund University

Jasmin Öykü Özdemir

Attribution of cyber operations in International Law

A study of the ILC Articles on Responsibility of States for Internationally Wrongful Acts, non-State actors and State liability in the 21st century

LAGF03 Essay in Legal Science

Bachelor Thesis, Master of Laws programme
15 higher education credits

Supervisor: Aurelija Lukoseviciene

Term: Spring term 2022

Contents

Summary

Attributing internationally wrongful acts to a particular State and liability is a complex problem in international law. The already unclear legal situation is further complicated when aspects of cyber operations are introduced with the rapid global technological development. To hold a State liable for the actions of non-state actors in cyberspace, we can only use secondary law and doctrine. The legal situation as it stands right now is based on doctrine and secondary law where the emphasis is placed on the technical evidence to hold a State accountable. It can thus be stated that there is a discrepancy between the legislation and reality. Additional problems are the nature of international law and its voluntariness. State liability for an internationally wrongful act is difficult because of the rules of evidence, which allow States to evade responsibility by supporting non-State actors without concrete links.

The purpose of this essay is to critically analyse and answer the research questions on how a non-State actor's actions can be traced to a State, and what main problems arise when an act is to be traced to the accused state. The essay also provides a summary of current law and tries to present possible solutions. The research questions that are answered are how international law can be used for State responsibility for cyber operations of non-State actors, and what are the most pronounced complications and solutions when attributing cyber operations to a State?

It can be stated that the threshold for state liability under Article 8 ARSIWA and thus the test of effective and overall control is extremely high. There is a discussion as to whether Article 8 and thus also Rule 17 of the Tallinn Manual 2.0 should be extended to include overall control.

Sammanfattning

Att härleda ett internationellt illegalt handlande till en viss stat och hålla denna ansvarig är ett komplext problem i folkrätten. Det oklara rättsläget kompliceras ytterligare när aspekter av cyberoperationer introduceras med den snabba globala teknologiska utvecklingen. Rättsläget som det ser ut just nu är baserat på doktrin och sekundärrätt, där vikt läggs vid den tekniska bevisningen för att statsansvar ska aktualiseras. Det kan således konstateras att det finns en diskrepans mellan lagstiftningen och verkligheten. Att hålla en stat ansvarig för en internationell illegal handling är svårt på grund av bevisreglerna, vilket gör att stater kan komma undan ansvar genom att låta cyberoperationer ske genom icke-statliga aktörer.

Syftet med uppsatsen är att kritiskt analysera och ge svar på hur en icke-statliga aktörs handlingar kan härledas till en stat, samt vilka huvudsakliga problem som uppstår när en handling ska härledas till den anklagade staten. Uppsatsen ger även en sammanfattning av gällande rätt och försöker presentera möjliga lösningar. Frågeställningarna som besvaras är hur folkrätten kan användas för statsansvar för icke-statliga aktörers cyberoperationer, vilka problem som uppstår under processen och vilka möjliga lösningar finns det?

Det kan konstateras att tröskeln för statsansvar enligt artikel 8 ARSIWA och därmed testen om effektiv och övergripande kontroll är synnerligen hög. En diskussion förs huruvida artikel 8 och därmed även regel 17 i Tallinn Manualen 2.0 bör utvidgas för att inbegripa övergripande kontroll. Detta hade utökat statsansvaret och möjliggjort folkrätten att hålla stater ansvariga för sina handlingar.

Abbreviations

ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts
CNA	Computer Network Attacks
DDoS	Distributed-Denial-of-Service
DoS	Denial-of-Service
ICJ	International Court of Justice
ILC	International Law Commission
ICTY	International Criminal Tribunal for the former Yugoslavia
NATO	North Atlantic Treaty Organization
SvJT	Svensk Juristtidning
UN	United Nations
UNGA	United Nations General Assembly

1 Introduction

1.1 Background

At the time of authoring this essay, no one can deny the fact that there is an ongoing war between Ukraine and Russia. It is at times like these that international law has its opportunity to show how conflicts can be resolved peacefully. However, not much has changed since the invasion started on the 24th of February 2022.[1]

As we, once again, witness the devastating consequences of war, one cannot deny the increased risk of cyber operations conducted by states such as Russia as an integral part of their military invasion of Ukraine. As the risk for cyber operations increases, the question of attribution arises. How can we hold a specific State liable for a malicious cyber operation or attack? Experts have raised concerns regarding Russian cyber operations on Ukraine and the possibility of these affecting other States.[2]

A clear example of how cyber operations and attacks have affected States previously is the NotPetya case, which is one of the most important and devastating cyberattacks. The attack spread worldwide and caused $10 billion in damages globally, which illustrates what kind of economic consequences cyber operations and attacks entail.[3]

The positioning of Russian troops along the Ukrainian border in the latter half of 2021 indicated Russia's intentions to invade Ukraine. Predictions were that cyberspace would play a significant role in the

[1] BBC (2022), 'Ukraine war in maps: Tracking the Russian invasion'.
[2] Gartzake, Erik & Kostyuk, Nadya (2022), 'Cyberattacks have yet to play a significant role in Russia's battlefield operations in Ukraine – cyberwarfare experts explain the likely reasons'.
[3] Greenberg, Andy (2018), 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'.

conflict. However, it is now clear that these hypotheses were incorrect. Cyber operations have not replaced the military invasion and of what is known at this moment cyber operations are not a part of the military invasion.[4]

The United States (U.S) and the United Kingdom (U.K) have stated that Russian military hackers were behind attacks that affected banks and government websites in Ukraine before the invasion. The Ukrainian government have attributed other attacks to a Belarusian hacking group. According to the Cyber Peace Institute, the latest cyberattack against Ukraine was on the 19th of April 2022 but there is uncertainty regarding the attribution of the act to a State.[5]

We also have to bear in mind that there have been cyberattacks launched against Russia which illustrates that States who are accused of conducting cyber operations can also be affected.[6]

1.2 Purpose, research questions and delaminations

This essay aims to investigate how cyber operations conducted by non-State actors can be attributed to a State within the framework of international law. This essay will try to answer how the International Law Commission's (ILC) Articles on Responsibility of States for Internationally Wrongful Acts (2001) (ARSIWA) are applied to cyber operations and if there are any obstacles within international law when attributing such operations to a State. Additionally, this essay will give an outline of the regulation of State responsibility and the analysis will

[4] Gartzake, Erik & Kostyuk, Nadya (2022), 'Cyberattacks have yet to play a significant role in Russia's battlefield operations in Ukraine – cyberwarfare experts explain the likely reasons'.
[5] Cyber Peace Institute, (2022), 'UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects'.
[6] Burges, Matt (2022), 'Russia Is Being Hacked at an Unprecedented Scale'.

evaluate valid law and the current legal framework. This paper will also discuss the potential complications that arise with the test of attribution.

The research questions are the following:

- What are the possibilities to identify State liability within international law for a non-State actor's conduct of malicious cyber operations?
- What are the most pronounced complications and solutions when attributing a cyber operation to a specific State?

This paper will only analyse the question of attributability of non-State actors' conduct of cyber operations to a specific State. Furthermore, this essay will give an outline of State responsibility and the applicability of international law on cyber operations. The valid law for the essay will therefore be the Articles of State responsibility, as the research question aims to identify how we hold a State accountable for an internationally wrongful act and if a cyber operation is such. The rules of International Humanitarian Law will not be addressed further. In conclusion, this paper will give an outline of State responsibility and how cyber operations conducted by non-State organisations can be attributed to a specific State.

1.3 Method and materials

The legal dogmatic method consists of the reconstruction of the legal system and valid law. In contrast to other methods, the legal dogmatic method is internal to a legal system. To identify the legal system a certain kind of exercise of power must exist to facilitate the identification of the system.[7] The term legal dogmatics is used as a denomination for a subject which in combination with legal history,

[7] Jareborg, SvJT (2004) p. 3.

sociology and philosophy have been considered to constitute jurisprudence.[8]

According to Korling and Zamboni, the method symbolises the scientific interpretation of applicable law and is thus used thoroughly by lawyers and scholars in the legal field to solve questions of interpretation and application of valid law. The method marks the original activity at the crossroads between application and science. Its purpose is problem-solving in the established sources within valid law.[9]

The method will be used when seeking answers in the established sources of international law to answer the research questions of this paper. The recognized sources in international law include treaties, general customary law, general principles of law, judicial decisions, and legal doctrine.[10] The source that regulates State responsibility is ARSIWA, which has the aim to codify applicable rules of State responsibility. ARSIWA is customary law and is thus a part of the recognized sources.

The Tallinn Manual is a doctrinal description of how the articles in ARSIWA can be applied to cyber operations. The manual is adopted by the International Group of Experts and is meant to reflect customary international law. The "rules" in the manual are accompanied by "commentary" that describes their legal basis and differences of opinions among the experts.[11] These rules are non-binding, but they allow us to regulate cyber operations.[12]

The method is used to answer and analyse whether international law ARSIWA applies to cyber operations. It will also be used to give an

[8] Olsen, SvJT (2004) p. 105.
[9] Korling and Zamboni (ed.) (2013), p. 21–25.
[10] Statue of the International Court of Justice, Art. 38 (1).
[11] Schmitt (2017) p. 79 – 82.
[12] Schmitt (2011) p. 34.

overview of the legal framework in international law. International law will therefore be analysed according to *de lege lata,* the law as it is and *de lege ferenda,* the law as it should be. To give a normative discussion valid international law will be critically analysed and solutions and conclusions will be presented on the matter. One of the purposes of the method is to answer precisely how a norm should be interpreted when it is applied in a certain context, which motivates why it should be used in this paper.[13]

1.4 Structure

Initially, this paper will give an explanation of vital terminology within cyber technology. Then, the aim is to give an outline of the valid law for State responsibility. The articles on State responsibility will be explained to later be used in the part case studies. This essay will give the reader an understanding of cyber operations that have occurred and how the question of attributability has or has not been answered in these various cases. The fourth part of this essay will analyse the usage of international law on cyber operations and try to give novel solutions to the problem of attribution. The last part of this essay will conclude the various arguments in a discussion and conclusion.

[13] Korling and Zamboni (ed.) (2013), p. 21–25.

2 Definitions in cyber technology

Cyber operations are the term to describe the reduction of information to the electronic format and the movement of the information between physical elements of cyberinfrastructure. Cyber operations can be categorised as computer network attacks, exploitation, or defence. CNAs include all cyber operations that have the aim "to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." A cyber operation is thus the encircling term for operations in cyberspace.[14]

Schmitt defines a cyberattack as a cyber operation that can either be offensive or defensive, to cause injury or death to persons, damage, or destruction to objects.[15] This makes it clear that a cyberattack is a part of a cyber operation.[16] The term cyberattack is a term that is used to describe active hostile acts aimed at cyberinfrastructure, services applications, and users in general.[17] According to Marica Ericson, these terms have different definitions nationally, there are examples in the U.K and Germany.[18] There is therefore no common definition that has been agreed on by all states.[19] The term cyberattack refers to the acts or operations that are prohibited under Article 2(4) UN Charter or article 51 UN Charter.[20]

[14] Melzer (2011) p. 5.
[15] Schmitt (2017) p. 415-418.
[16] Ibid.
[17] Ericson (2020) p. 38.
[18] Ibid.
[19] Ibid.
[20] Ibid. p. 39.

Cyber acts include cyberattacks and cyber operations. The European Commission defines cyber acts as criminal acts committed online through electronic communication networks and information systems and categorizes them as cybercrime.[21]

Schmitt states that cyber-related acts are used to distinguish the fact that a State may bear responsibility for acts that are attributable to it. These acts can be other than cyber operations. An example is a State's cyberinfrastructure being available to non-State actors or other States. This means that the State fails to take the required measures to prevent the conduct of cyber operations from its territory.[22]

As this essay will discuss the attributability to a State the term that will be used when describing the State's responsibility is cyber operations. The term shall be used as the general term as this essay focuses on the States and how they conduct cyber acts as part of operations. When referring to specific cases and an isolated act the term cyber attacks will be used.

[21] European Commission, 'Cybercrime'.
[22] Ericson (2020) p. 84 – 88.

3 Valid law

3.1 Definition of non-State actors

A State organ can be defined as the main medium in which States act. With the State's increased usage of cyberspace in both peace and wartime, specific organs of the State devoted to such activities have developed. All activity conducted by an organ of a State is attributable to that State. A State organ is interpreted broadly in ARSIWA, in particular article 4 where a State organ is described as an organ that includes any person or entity which had that status by the internal law of the State.[23]

Rule 17 in the Tallinn Manual 2.0 defines a non-State actor as including both individuals and groups.[24] Groups are considered as non-State actors under the rule whether they are incorporated, unincorporated, hierarchical, or not, organised, or unorganised and whether they possess domestic legal personality or not.[25] As for individuals the term incorporates individual hackers e.g., "informal groups like Anonymous, criminal organisations engaged in cybercrime, legal entities such as commercial IT services, software and hardware companies and cyber terrorists or insurgents."[26]

[23] Articles on State Responsibility, Art 4; Delerue (2020) p. 115.
[24] Schmitt (2017) p. 95.
[25] Ibid.
[26] Ibid.

3.2 Cyber attribution

When examining cyber attribution there is both a technical and a legal aspect. Various difficulties of attribution are established when attributing a malicious cyber operation to a specific State. The scope of this essay is not to evaluate how technical evidence is assessed or collected, but the technical attribution must be addressed to explain legal attribution and to give an outline of the framework.[27]

3.2.1 Technical attribution

Technical attribution plays a vital part in legal attribution as it answers questions concerning the origin of an attack. Firstly, the relationship between the hacker and the responsible State must be determined. The facts that need to be established are the geographic origin of the attack and the identity of the people responsible. However, to establish these facts we need to overcome technical and evidentiary obstacles. An example is the cyberattacks on Estonia in 2007, where the reports showed that the attacks originated from at least 177 countries, and Estonia was one of those itself.[28]

This illustrates the difficulty in determining from where and by whom an action is conducted. A clear example is IP addresses (Internet Protocol addresses) and how these can be modified (IP spoofing) to give the illusion of the act being conducted elsewhere.[29]

A cyber operation can thus be conducted in State A, but the IP address shows us the opposite. The Internet and how it operates to make the identification process difficult and it is widely agreed that there is a difficulty determining the technical attribution. Furthermore, scholars

[27] Tsagourias and Farrell (2020) p. 942
[28] Schmitt (2017) p. 569.
[29] Payne and Finlay (2017) p. 559-561.

argue that the problem of cyber attribution is impossible to solve. Dienstein, argues that the solution is nothing more than the development of technology.[30]

3.2.2 Legal attribution

The legal attribution is divided into direct and indirect attribution to a State.[31] According to Eric Mejia, direct attribution holds States liable for acts or omissions of individuals exercising the State's machinery of power and authority.[32] These acts can be attributed to the State even if the acts exceed the authority given by the State.[33] Indirect attribution includes acts or omissions of non-State actors that are generally not attributable to the State.[34] However, there is a possibility to hold States responsible if it fails to exercise "[...] due diligence in preventing or reacting to such acts or omissions."[35]

There is a difficulty when assessing the technical attribution of a cyberattack. Furthermore, it shall be stated that this complicates matters for the legal attribution as this attribution relies on the evidence that the technical attribution provides. We must decide the standard required, and propose a proof of the relationship between the hacker, the State and the control that the State exercises over the hacker. This makes it difficult to attribute a cyber operation to a specific State. Without technical attribution, we cannot answer these questions. To attribute a non-State organisation's act to a State, we will have to use the overall and effective control tests, established in the *Nicaragua* and *Tadic* cases.[36]

[30] Payne and Finlay (2017) p. 559-561.
[31] Meija (2014) p. 118.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Ibid. p. 562-564.

3.3 State responsibility - law of attribution

3.3.1 Articles on Responsibility of States for Internationally Wrongful Acts

In this part of the paper, State responsibility will be examined in general terms to apply it to cyber operations conducted by non-State actors. Initially, an act must be an internationally wrongful act for a State to be liable. State responsibility is the rules that include the principles of governing, when and how States can be liable for the breach of an international obligation and the consequences that follow the violation.

ARSIWA is a set of provisions and commentary of secondary rules adopted by the ILC and the UNGA in 2001. According to James Crawford, the ILC's recommendations are a compromise between the members of the Commission that wanted ARSIWA to serve the international legal order as evidence of international law and the others that wanted ARSIWA to be an international convention.[37]

Initially, article 1 ARSIWA establishes the core of the document, in that every internationally wrongful act of a State entails that State's responsibility. There are two requirements for the applicability established in article 2 of the regulation. Firstly, attributability and secondly, a breach of an international obligation. At first, the regulation in article 1 may seem obvious, but it does not give clarity on general preconditions for responsibility in international law. [38]

Furthermore, it does not state anything regarding which State has conducted an internationally wrongful act, or anything about the damages it causes to the affected State. Additionally, article 1 does not identify the States or other international legal persons that have

[37] Crawford (2013) p. 39–42.
[38] Ibid, article 1-2 ARSIWA.

international responsibility. Crawford explains this as an "objective correlative" of the commission of an internationally wrongful act.[39]

As stated previously, article 2 ARSIWA sets out the constitutive element of an internationally wrongful act. To qualify as an internationally wrongful act, two conditions need to be fulfilled. Firstly, a breach of an international obligation needs to have occurred and secondly, this breach must be attributable to the State under international law.[40]

Chapter II of ARSIWA manages the attribution of conduct to a State. It is stated in article 4 that the conduct of any State organ is attributable to the State through its obligations under international law. Even in article 4, there is a requirement of attribution, and it can either be through active or passive action. [41]

Article 5 handles persons or an entity that are empowered to exercise governmental authority. Article 6 describes the situation when the conduct of an organ is placed at the disposal of another state. By article 7, a State is considered responsible even if persons or entities that are empowered to exercise governmental authority exceed its authority or contravene instructions. Articles 8 and 9 deal with cases where attributability is made through analogy with the concept of agency.[42]

[39] Crawford (2013) p. 39–42.
[40] Ibid.
[41] Ibid.
[42] Ibid.

3.3.2 State responsibility applied to non-State actors

As the research question is how we can attribute a cyber operation conducted by non-State actors to a specific State, article 8 is relevant. Article 8 states the following: if a group of persons was acting under the control, instruction of, or under any direction of the State, these actions can be attributable to the State. However, to attribute such actions to a State we need to look at how article 8 functions and how the requirement "direction" and "control" are interpreted and used as two ways of attributing the actions or conducts to a State.[43]

The general rule is that cyber operations conducted by private groups and people are not attributable to a State, thus we cannot hold the State accountable for malicious acts as such. However, there may arise situations where such acts can be attributable to a specific State through article 8 ARSIWA.[44]

Article 8 ARSIWA provides us with the scope that the conduct of a group of persons or a person should be considered an act attributable to a State if the person or group of persons are acting under the State's instructions, direction, or control. If one of these three requirements is fulfilled, that State is considered the conducting State of the cyber operation.[45]

Therefore, article 8 deals with two circumstances: firstly, private persons acting on the instructions of the State while carrying out the act and secondly, the more general situation where private persons acting under the State´s direction and control. Furthermore, it is of importance

[43] Articles on State Responsibility, Art. 8.
[44] Ibid.
[45] Articles on State Responsibility, Art. 8.; Tallinn Manual 2.0 (2017) p. 95. S*ee also* UN GGE 2013 Report para. 23; UN GGE 2015 Report, para. 28.

that we take into consideration that both cases need a real link between the people conducting the act and the State machinery.[46]

When it comes to cyber operations, we will have to look at the Tallinn Manual 2.0, a legal doctrine based on the articles in ARSIWA.[47] Rule 14 establishes the fact that a State bears international responsibility for a cyber-related act that is attributable to that state. It also must constitute a breach of an international legal obligation.[48] We can thus say that an internationally wrongful act is an "[...] action or omission that both: (1) constitutes a breach of an international legal obligation applicable to that State; and (2) is attributable to the State under international law."[49] This article has a customary character that has been confirmed by the ICJ through cases like *Tehran Hostages* and generally through the *Nicaragua* case.[50]

Rule 17 reflects article 8 in ARSIWA and is interpreted with the commentary and the doctrines of *effective* and *overall control*. This rule articulates the legal standard where a State may, either by specific directions or by exercising control over a group, assume responsibility for their conduct. Each case is regarded individually and dependent on its facts.[51]

This concludes that the actions of a non-State actor must be under the instructions, direction, or control or if the State acknowledges and adopts the operations as its own. To assess if the non-State actor is under the control of the State we must apply the tests of effective and overall control.[52]

[46] Articles on State Responsibility, Art. 8. para 1 of commentary.
[47] Schmitt (2017) p. 30–35; Nicaragua (Judgement) paras. 386-394.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Ibid p. 94
[52] Ibid. p. 96.

3.3.3 The tests of effective and overall control

The ICJ, ICTY and ILC have made different approaches to the question of attributability of internationally wrongful acts conducted by non-State actors and the term "control" by article 8 ARSIWA. In the *Nicaragua* case, the tests of *effective* and *strict control* are introduced. The case arose to the ICJ because of the activities of the guerrilla insurgency in 1981 by the group *Contras* against the government in Nicaragua.[53]

The main question for the Court was to answer how the actions of this non-State actor could be attributable to the U.S as the supporting State.[54] Two situations were distinguished. Firstly, persons that are supported, financed and armed by a State organ and acting under its control.[55] Secondly, persons that were armed and financed by a State, but with some independence in the conduct of the operations.[56] The non-State actor in the *Nicaragua* case was the latter.[57] The court addressed the attributability to the U.S by establishing the fact that even if the involvement of the U.S was not fully proven, military personnel of that State took a "[...] direct part in the operations, agents of the U.S participated in the planning, direction, support, and execution of the operations."[58]

The three alternative prerequisites: control, direction and instruction are supposed to be understood disjunctively according to the Commentary. However, the ICJ tends to treat the prerequisite control and direction together. The term effective control summarises the scope of the concept, and the two terms are referring to the continuing process of exercising authority over activity such as a cyber operation.[59]

[53] Delerue (2020) p. 131.
[54] Ibid. *See also* Nicaragua (Judgement) paras. 386-394.
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] Ibid. p. 96.

When determining whether the conduct was conducted "under the direction or control" of a State, the attributability will only be attained if the State was directing or controlling the specific operation and additionally if the operation was an integral part of the operation.[60]

Hence, ICJ has developed the term *effective control* through *Nicaragua* and the *Genocide* cases. The key issue in the *Nicaragua* judgement was the degree of control that must be exercised by the State for the act to be attributable. In conclusion, for effective control to be fulfilled the proof must be beyond any doubt which demands a thorough technical attribution.[61]

In the *Tádic* case, the ICTY had to decide if the Bosnian-Serb forces were *de facto organs* of the Federal Republic of Yugoslavia. The question of an agency relationship between a group and a State was addressed.[62]

The applicability of the *overall control* depends on if the State has given specific instructions to the non-State actor.[63] This establishes the core of the test, and it applies to the two degrees established by the Tribunal.[64] The Chamber distinguished two degrees of control, the first depending on if it concerned "private individuals" and the second about an "organised and structured hierarchical group."[65]

According to Antonio Cassese, this is the effective control test established in the *Nicaragua* case, but it has been applied incorrectly by the Chamber to the relationship of agency. The Chamber used both the

[60] Delerue (2020) p. 131.
[61] Ibid.
[62] *Tádic* (Appeals Chamber) para 87; Delerue (2020) p. 120.
[63] Ibid.
[64] Delerue (2020) p. 121.
[65] Ibid.

"strict control" and "effective control" test, thus constructing the overall control test. However, scholars point out that the overall control test applied to an organised and hierarchical group is not derivable to the ICJ's judgements.[66] As Delerue points out, this test "[...] requires a lower degree of control than the test applied by the ICTY for private individuals and is lower than the two tests of the ICJ."[67]

The test of overall control has been overruled by the ICJ in the *Bosnian Genocide* case. By rejecting the test of overall control, the ICJ has decided that the usage of the effective control test is more suitable for attributability. When it comes to the usage of the precedent in terms of cyber operations, a discussion can be conducted on whether the overall or effective control test is more appropriate, and which should be used.[68]

Scholars argue that the degree of control required by the ICJ is too strict and provides a high threshold to apply to and keep up with innovative technology. However, there is a risk of lowering the threshold significantly by applying the overall control test because there is still an aspect of State sovereignty within international law.[69]

The Chemical Weapons Convention could be used as a model for a future convention on cyber operations, as it is stated in article 1 that States those are a part of the convention can not engage in military preparations to use chemical weapons, or assist or encourage such activity. This entails the States to make sure that there is no usage of Chemical weapons in their territory.[70]

---

[66] Cassese (2007) p. 651 f.
[67] Delerue (2020) p. 122.
[68] *Bosnian Genocide* (Judgement) paras 406–407; Delerue (2020) p. 141.
[69] *Bosnian Genocide* (Judgement) paras 406–407; Delerue (2020) p. 141. *See also* Shackelford and Woltag.
[70] Chemical Weapons Convention art. 1.

4 Case studies

We will now examine previous cases of cyberattacks that might have been conducted through a State's sponsorship, and thus can be attributed to a specific State. It can be stated that most State-sponsored cyber operations are conducted by non-State actors, which activates the question of attribution. The rules on State responsibility apply to the question of attributability on cyber operations.[71] As stated above, the Internet and its characteristics on how it operates makes it difficult to apply ARSIWA, particularly when it comes to attribution. The following sections of the paper are based on generally accepted understandings of international law.

4.1 Estonia (2007)

In 2007 various cyber operations were conducted against Estonia and the Estonian government accused Russia of being responsible. Estonia admitted that they had no evidence that Russia had any involvement. However, members of the Russian Parliament and youth groups that worked closely with the Kreml, have confirmed that they had conducted cyber operations against Estonia.[72]

In this case, there has only been one person identified and that has now been convicted as the perpetrator of the cyber operations that blocked the websites of Estonian parties. Delerue divides these cyber operations into two parts, the first part lasted from 27 to 29 April 2007 and consisted of DoS attacks against government and media websites. The second part took place from 30 April to 18 May 2007 and consisted of more coordinated and refined cyber operations with more harmful consequences.[73]

[71] Delerue (2020) p. 144.
[72] Ibid. p. 146-151.
[73] Ibid.

The cyber operations, in this case, seem to have been coordinated through online forums and internet chat rooms. Delerue assumes that the attacks seem to have been disorganised and thus not constituted a single organised group. The conclusion is that it seems as if they were single individuals or informal groups that collected information on targets and conducted operations because they supported a cause.[74]

Given the nature of the attacks on Estonia, it makes it difficult to claim that the State had effective control over the online actions. The effective control would not be satisfied and thus, the operations would not be attributable to Russia. In this case, Russia did not exercise the degree of control as the U.S in the *Nicaragua* case, where the State arms, trains, and even funds the individual or group.[75]

The problem, in this case, lies in the technical proof, even if the Estonian government was able to technically prove that the source of the attack was in the Russian territory, they could not prove that there was governmental support.[76] In theory, a Russian government employee could act independently without any State interference. It could also be a citizen who conducted the attacks as well.[77] The overall control test encompasses a "[...] wider degree of control over the group without requiring specific instructions for each act [...]".[78]

Delerue states that we cannot identify everyone as an organised group in this case, but some of them might have belonged to such groups. Even if these people would have been organised in such groups it would still be difficult to say that the degree of control is not enough. Even if we would make a scenario that constitutes that Russia was sponsoring the operation it would not be enough to incite people to use the forums

[74] Delrue (2020) p. 146–151.
[75] Gerald (2009) p. 10.
[76] Ibid.
[77] Ibid.
[78] Ibid.

for conducting the attacks. In conclusion, this form of control and direction is below the threshold and does not fulfil the overall control test.[79]

4.2 Georgia (2008)

During the Russo-Georgian war of 2008, cyber operations in and through cyberspace occurred and came from both sides. The attacks consisted of computer network operations, to disable or degree the infrastructure. There was a hijacking of government computer systems the Georgian websites and some Russian media sites. These channels were subjected to large-scale DDoS. Russia was the accused State for the DDos against Georgia. Russia has not claimed responsibility for any of these activities, there is still uncertainty regarding if the operations were coordinated, encouraged, or officially tolerated by Russia.[80]

The coordination of the attacks that were conducted during the conflict has clear links to the Russian government, through forensic evidence. Because Russia denied any involvement we cannot move forward with public attribution, where other States openly attribute a cyber operation to a specific State. A conclusion is therefore that the requirement of proof in the effective control test is the main problem.[81]

It is not possible in this case to see whether Russia had exercised control over the non-State actors that conducted some of the malicious attacks. The main downfall of the effective control test is illustrated in this case. The requirement of proof causes conflict between the impossibility to provide a technical and strategic confirmation of the authorship when

[79] Delerue (2020) p. 147–149.
[80] Schapp (2009) p. 205.
[81] Connell and Vogler (2017) p. 17.

we have non-State actors involved. This inconsistency leads to the conclusion that this test causes impunity in cyberspace.[82]

If the overall control test would be applied to this case, we would have to look at the degree of control beyond a reasonable doubt. The forensic evidence that was presented in this case, could have been enough to prove the Russian government's influence and coordination over the hacker groups that conducted the cyber operations against Georgia.[83]

We must bear in mind that the overall control test only applies to organised groups, which complicates the liability of a State. As stated above, the overall control test has been overruled by the ICJ which gives us the indication that it should no longer be used. However, we cannot deny the fact that something needs to change to hold States responsible for their internationally wrongful acts in cyberspace.[84]

[82] Connell and Vogler (2017) p. 17.
[83] Delrue (2020) p. 150.
[84] Ibid.

5 Discussion and conclusion

Attributing malicious cyber operations committed by non-State actors to a specific State have both legal and technical difficulties. As stated, the question of attribution raises complex difficulties, however, it must be stated that international law does apply to cyber operations regardless of the difficulties of attribution. The process of identification of the non-State actor, which can consist of hacker groups or individuals, requires strenuous technical evidence of the chain between the group or individual and the accused State.

Such evidence can be found in the IP addresses or any form of data that serves value to the investigation. This data is stored on, received by, or transmitted by an electronic device such as a computer. As the legal attribution relies on the technical attribution, it is important that the injured State or any other States that wishes for responsibility provide technical evidence.

When assessing cyber operations and the applicability of international law we must keep in mind that the effective and overall control tests have nothing to do with technical attribution directly. The applicability of international law on cyber operations consists of the legal attribution that relies on technical attribution. ARSIWA is the ultimate document for State responsibility is secondary law and thus non-binding.

It can be stated that cyber operations are internationally wrongful acts when they constitute breaches in international law, and meet the requests in articles 1 and 2 ARSIWA. A clear example is the principle of non-intervention and the lack of respect for a State's sovereignty when conducting cyber operations to cause harm. If the States action constates a breach of an international obligation it is an internationally wrongful act which makes ARSIWA applicable. The cyber operations conducted against Ukraine are an example of when international law

should interfere with State liability. It must be stated that the circumstances regarding these attacks are not certain which makes it difficult to apply ARSIWA and the rules of the Tallinn Manual.

Considering the circumstances, it is natural that Ukraine blames Russia for the cyberattacks against governmental and non-governmental websites that occurred shortly before the military invasion. If we were to assess these acts of cyber operations, we would have to use the rules in ARSIWA. As there is no binding treaty for cyber operations specifically, we will have to assess the applicability of the effective and overall control tests by analogy. The outcome would likely be as in the cases in Estonia and Georgia. The main issue here is the lack of technical evidence, to hold Russia or any other State responsible for cyber operations conducted by non-State organisations that State must have effective control.

As stated above, the effective control test introduced in the *Nicaragua* case requires proof that it is beyond a reasonable doubt. It must be that the State has ordered or supported the group or individual that conducted the cyber operation or attack. The high threshold makes it difficult for us to state that the State is liable. However, the thought behind the effective control test and the high threshold serves the purpose of legal certainty. If we were to lower the required proof this would dislodge the current order in the international community. This is counterproductive, even if we want internationally wrongful acts to be met with consequences, we cannot forget the purpose of international law which is the maintenance of international peace and security.

The overall control test could be an alternative. The issue is that the ICJ has overruled this doctrine in the Bosnian Genocide case, but nothing has been stated particularly regarding cyber operations. Nevertheless, the overall control test would lower the threshold, thus facilitating the process of attribution. As the required proof is beyond reasonable doubt

it would simplify the attribution process as seen in the case study of Estonia.

The consequences of the high threshold in the effective control test are that States can avoid liability by supporting non-State actors to conduct the malicious acts and making sure that there are no connections between the group and the State. This is possible due to the Internet and the way it operates, which complicates the legal and technical attribution. Even if the rules of State responsibility make it possible for the attribution of non-State actors' actions to a State, the question of liability remains unsolved as it is easy to get around the rules. Although we have examples of when States have been affected deeply by cyber operations, there is no case where a State has been held legally responsible for the non-State actors' acts.

A solution to the high threshold could be, as stated previously, to use the overall control test. However, I am not certain that this would make that much of a difference. If States can support non-State actors without having clear connections due to the technical aspects, adopting the overall control test may not solve the whole problem. Both tests, ARSIWA and the Tallinn Manual try to use existing principles and documents on a new phenomenon. The world has evolved technically, instruments and judgments that are used analogically do not reflect cyberspace and how it operates. Maybe the solution is new technology? If this is the solution, we will have to wait for it to develop which only benefits the hackers and States that deliberately want to harm other States without responsibility. This undermines international law and its significance, legislation cannot be postponed in a wait for new technology.

I believe that a way to move forward would be to either develop a new doctrine based on a case that has been risen e.g., the ICJ where the Court comes forward with a new approach tailor-made for cyber operations,

or an international treaty. However, the latter would be difficult as international law is the product of the voluntariness of the States. Even States that have been affected negatively by cyber operations would, in my opinion, not be ecstatic over ratifying a treaty that reduces voluntariness.

The main issue with international law is that there must be a mutual agreement between the States to develop new rules. As cyberspace is an immensely technical field, the solution to the problem of attribution needs to reflect and take that into account. A way to prevent the usage of cyberspace to conduct cyber operations would be to develop a convention such as the Chemical Weapons Convention where it is stated in article 1 that the States that are part of the convention will not develop or use chemical weapons, engage in any military preparations to use chemical weapons, or assist or encourage such activity.

If there could be a possibility for conducting a clear framework for the attribution and liability of cyber operations to States it would make it harder for States to engage in such activities. By having a clear convention on the matter, we would firstly, put pressure on States to comply with the rules and avoid using cyberspace for unpeaceful acts. Secondly, if rules would state that it is under every individual State to have responsibility for cyberspace within its territory it would oblige States to take liability for counteracting cyber operations. Lastly, adopting a new treaty or convention like the Chemical Weapons Convention would clarify valid law and liability.

There are discrepancies regarding the process of attribution. There is no uniform legislation to hold States liable for their actions in cyberspace, even if the articles on State responsibility apply to cyber operations and the Tallinn Manual gives clarity it is still secondary law and doctrine. It does not have the same significance as a treaty. However, the difficulties that occur when using the effective control test in the

process of attribution of cyber operations make it possible for States to avoid liability by making sure that there is no clear connection between the non-State actor and the State. A possible way to solve this problem is by using the *overall control* test, but this has its disadvantages as well.

The conclusion is therefore that we need to develop new technological and legal solutions to facilitate the process of attribution. If we have the aim of maintaining international peace and security, we need to consider cyberspace for future conflicts in general. As we have seen with the events before and during the invasion of Ukraine, cyber operations have caused damage and illustrated what kind of power it brings. The attacks against Ukraine have been destabilising, the attacks are in the grey area which makes it difficult for valid law to be applied and thus leaves us with uncertainty on how the law is applicable. There is a need for clarification of the rules and urgent efforts from States, civil society and academics to clarify valid law.

Furthermore, the main conclusion and answer to the research questions are that there is a framework consisting of ARSIWA, the Tallinn Manual, and the doctrine of effective and overall control. However, the attribution test is insufficient, as there has not been a State that has been held liable for its actions in supporting a non-State actor in cyberspace. This is because of the strict proof requirements, specifically in the effective control test. International law needs to learn a lesson from the invasion of Ukraine and try to develop new rules to prevent and hold States accountable for their internationally wrongful acts.

The character of international law is an obstacle as it is seemingly difficult for all States to agree on how to move forward, but doing something rather than doing nothing is a better way of approach. However, valid law is uncertain and there is a need for new and innovative legislation and technology. There is therefore one clear

conclusion, and that is that the test for State liability for non-State actors is ineffective.

Bibliography

Literature

Crawford, James, *State Responsibility The General Part,* 1st ed., Cambridge: Cambridge University Press, 2013.

Delerue, François, *Cyber Operations and International Law,* 1st ed., Cambridge: Cambridge University Press, 2020.

Ericson, Marika, *On the Virtual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and War,* 1st ed, Uppsala: Uppsala universitet, 2020.

Gerald, T. Yap, *When is a Hack an Attack? A Sovereign State's Options if Attacked in Cyberspace: A Case Study of Estonia 2007,* Alabama: Air University Press, 2009.

Jareborg, Nils, 'Rättsdogmatik som vetenskap', *SvJT (Svensk Juristtidning)*, 2004.

Korling, Fredric and Zamboni, Mauro (ed.), *Juridisk metodlära,* 1st ed., Lund: Studentlitteratur, 2013.

Mejia, Eric. F, *Act and Actor Attribution in Cyberspace A Proposed Analytic Framework*, Vol. 8, No 1, Alabama: Air University Press, 2014.

Olsen, Lena, 'Rättsvetenskapliga perspektiv', *SvJT (Svensk Juristtidning)*, 2004.

Tsagourias, Nicholas, and Buchan, Russell (ed.), *Research Handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 2015.

Woltag, Johann-Christoph, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*, Cambridge: Intersentia, 2014.

Soft Law Documents

Schmitt, Michael N., and Vihul, Liis (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Cambridge: Cambridge University Press, 2017.

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, November 2011, Supplement No.10 (A/56/10), chp.IV.E1. [cit. Articles on State Responsibility; Commentary].

Reports

UN GGE*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General*, New York 24 June 2013, A/68/98 [cit. UN GGE 2013 Report].

UN GGE, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General*, New York 22 July 2015, A/70/174 [cit. UN GGE 2015 Report].

Other Reports

Melzer, Nils, *Cyberwarfare and International Law*, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2011.

Shackelford, Scott J. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Cambridge: University of Cambridge, 2010.

International Treaties and Conventions

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI [cit. Charter of the United Nations].

United Nations, Statute *of the International Court of Justice,* 18 April 1946 [cit. Statue of the International Court of Justice].

United Nations, *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and their Destruction,* 15 May 2015 [cit. Chemical Weapons Convention].

Electronic resources

Newspaper Articles

BBC, 'Ukraine war in maps: Tracking the Russian invasion', *BBC,* 16 May 2022. <https://www.bbc.com/news/world-europe-60506682> (accessed 17 May 2022).

Burges, Matt, 'Russia Is Being Hacked at an Unprecedented Scale', *WIRED*, 27 April 2022. < https://www.wired.com/story/russia-hacked-attacks/ > (accessed:19 May 2022).

Cyber Peace Institute, 'UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects', *Cyber Peace Institute,* 12 May 2022, <https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks> (accessed 10 May 2022).

Gartzake, Erik & Kostyuk, Nadya, 'Cyberattacks have yet to play a significant role in Russia's battlefield operations in Ukraine – cyberwarfare experts explain the likely reasons', *The Conversation,* 4 April 2022, <https://theconversation.com/cyberattacks-have-yet-to-play-a-significant-role-in-russias-battlefield-operations-in-ukraine-cyberwarfare-experts-explain-the-likely-reasons-178604> (accessed 2 May 2022).

Greenberg, Andy 'The Untold Story The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *WIRED,* 22 August 2018, < https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (accessed 2 May 2022).

Miller, Maggie, 'The world holds its breath for Putin's cyberwar', *Politico,* 23 Mars 2022,

<https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440> (accessed 27 April 2022).

Other Electronic Resources

Cassese, Antonio, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia', *The European Journal for International Law*, September 2007. < https://academic.oup.com/ejil/article/18/4/649/453762 > (accessed 3 May 2022).

Connell, Michael and Vogler, Sarah, 'Russia's Approach to Cyber Warfare', *The Centre for Naval Analyses (CNA)*, March 2017. <https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf > (accessed 3 May 2022).

European Commission, 'Cybercrime' <https://ec.europa.eu/home-affairs/cybercrime_en> (accessed 19 May 2022).

Healey, Jason, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks', Issue Brief. Washington, D.C.: Atlantic Council, 22 February 2012. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/> (accessed 16 May 2022).

Payne, Christian and Finlay, Lorraine, 'Addressing obstacles to cyber-attribution: a model based on state response to cyber-attack', *The George Washington International Law Review,* 2017. <https://gwilr.org/wordpress/wp-content/uploads/2017/05/ILR-Vol-49.3_Panye-Finlay.pdf > (accessed 18 May 2022).

Schmitt, Michael N, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law*

Journal, December 2012. <https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf> (accessed 15 May 2022).

Schaap, A.J, 'Cyber warfare operations: development and use under international law', *Air Force Law Review*, Winter 2009. <https://link.gale.com/apps/doc/A212035712/AONE?u=anon~23e5f8ad&sid=googleScholar&xid=6b73ea21> (accessed 16 May 2022).

Tsagourias, Nicholas and Farrell, Michael, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law*, 26 August 2020. <https://academic.oup.com/ejil/article/31/3/941/5897247?login=true> (accessed 2 May 2022).

Table of Cases

International Court of Justice (ICJ)

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia) International Court of Justice (ICJ), 11 July 1996.

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986.

International Criminal Tribunal for the former Yugoslavia (ICTY)

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.