UPPSALA
UNIVERSITET

Department of Law
Spring Term 2020

Master's Thesis in Public International Law
30 ECTS

Due Diligence in Cyberspace

An Assessment of Rule 6 in the Tallinn Manual 2.0

Author: Maja Bergwik
Supervisor: Olle Mårsäter

List of Abbreviations

EIA	Environmental impact assessment
ICJ	International Court of Justice
ILA	International Law Association
ILC	International Law Commission
ICT	Information and Communication Technology
ITLOS	International Tribunal on the Law of the Sea
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
PCIJ	Permanent Court of International Justice
UN GGE	United Nations Group of Governmental Experts
UNCLOS	United Nations Convention on the Law of the Sea

Table of Contents

1 Introduction

1.1 Cyberspace and international law

States and non-State actors have become increasingly reliant on digital technology, such as computers and the networks that link them. States are heavily dependent on the use of cyberspace. As cyberspace becomes a more important part of everyday life, there is an increasing need for regulation in that area. Cyberattacks and kinetic attacks can, at times, have similar consequences, for example harm to life, bodily harm, and destruction of property.[1] The increase in cyber operations targeting States' administrations, the economic sector and critical infrastructure is one of "the most pressing and potentially dangerous" threats for national and international security.[2] While these cyber operations fall beneath the threshold of an armed attack, they can have a damaging impact. This raises issues about the obligations of States in this area and how international law can deal with this new threat. Already, efforts to regulate cyberspace can be seen in both regional and international contexts, especially on the area of cyber security.[3]

Cyberspace enjoys some unique features which are not inherent in physical territory. First of all, cyberspace has a borderless character. Secondly, actors in cyberspace have a significant level of anonymity. Finally, cyberspace is easily accessible for many actors. All of these qualities of cyberspace amount to a thriving environment for non-State actors.[4] Because of the special character of cyberspace, it has been under a lot of dispute whether international law applies in cyberspace or not.

For example, Barlow expressed in 1996 that legal concepts do not apply to cyberspace and that it "does not lie within [governments'] borders".[5] These arguments assume that cyberspace is different from other spaces in that it is not territorial and that it is borderless.[6] However, the consequences of having no rules in cyberspace would be that cyberspace becomes a "lawless land". It would be a legal void, where all kinds of actions

[1] Efrony & Shany p. 584.
[2] Bannelier-Christakis p. 3.
[3] See for example Commission (EC) and High Representative of the European Union for Foreign Affairs and Security Policy, '*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*' (joint communication) JOIN(2013) 1 final (7 February 2013) and Alexander Klimburg (ed.), *National Cyber Security Framework Manual* (NATO CCD COE 2012).
[4] Buchan p. 429.
[5] Barlow.
[6] See the discussion about this in Chapter 2.1.

could take place. Considering that the use of cyberspace to perform malicious cyber operations is becoming more common, not regulating does not seem to be a feasible option. In order to maintain peace and security, which is essential for international law, regulation is highly necessary.

What most authors conclude is that it is no longer disputed that cyberspace is subject to international law.[7] There is nothing that would exclude cyber operations from the application of international law. Instead, the discussions have now shifted to *how* international law should be applied in cyberspace. It is the scope and the content of international law which has obtained different reactions and remains unsettled.

International law and its applicability in cyberspace have been discussed in different fora. For example, a number of prominent international lawyers attempted to facilitate the regulation of cyber operations by international law by developing the Tallinn Manual 2.0 on the international law applicable to cyber operations (Tallinn Manual 2.0).[8] A Group of Governmental Experts (UN GGE) was established by the United Nations in 2004 to strengthen the security of global information and telecommunications systems.[9] The UN GGE were successful in releasing two consensus reports (in 2013 and 2015)[10], before failing to reaffirm the applicability of international law to cyberspace in 2017.[11]

Customary law is slow to develop, while advancement in the field of cyberspace is happening quickly. One might say that public international law is struggling to keep up. As an example of the way international law is not adjusted to cyberspace, there is a traditional understanding of an armed attack which does not at the moment support cyberattacks from hackers or non-State actors to States.[12] Considerable difficulties exist in applying international law to cyberspace.

At the center of the discussion lies the issue of State responsibility. State responsibility generally requires that the unlawful act can be attributed to a State. Attributing cyber acts to States is difficult because of the special features of cyberspace and because many of

---

[7] See for example Tsagourias, *The legal status of cyberspace* p. 13 and Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 3. See also Chapter 2.3. for a more in depth discussion.
[8] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*
[9] A/RES/58/32, *Developments in the field of information and telecommunications in the context of international security* (8 December 2003) p. 2 para. 4.
[10] A/68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 June 2013) (UN GGE 2013 Report) and A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (22 July 2015) (UN GGE 2015 Report).
[11] Väljataga.
[12] Arias p. 2.

the actors in cyberspace consist of non-State actors. Therefore, it has been suggested that attribution is not prepared to deal with these cyber operations.[13]

However, there might be another option to attribution to ensure the responsibility of States. Rule 6 in the Tallinn Manual 2.0 describes the due diligence principle and states that it is applicable to cyber operations.[14] Due diligence is a principle in customary international law, developed through case law. The principle infers an obligation on States to not allow knowingly their territories to be used for acts contrary to the rights of other States.[15] One of the consequences of the rule being applicable to cyber operations is that the State being targeted with the attack may be able to use countermeasures to stop the attack. It is therefore important for States to know whether this rule applies in cyberspace or not, and, if it does, to what extent.

1.2 Purpose of the study

The purpose of this study is to examine whether the obligation of States to not allow knowingly its territory to be used for acts contrary to the rights of other States applies to activities conducted in cyberspace. In order to do this, the due diligence principle, as formulated in Rule 6 of the Tallinn Manual 2.0., will be assessed.

1.3 Delimitation

Due diligence is a rule concerned with State responsibility. Therefore, individual criminal responsibility will not be of interest in the study. Neither will the responsibility of international organizations. Attribution, which is essential for the determination of State responsibility, but not relevant for the due diligence principle, will be discussed only in order to understand the problems of State responsibility relating to cyberspace.

Jus ad bellum and jus in bello will not be covered here. The due diligence principle applies both for peaceful cyber operations and for cyber operations which amount to the use of force by States and it is therefore not of interest in this study to discuss the rules about use of force. Furthermore, issues relating to self-defense are outside the scope of the study since self-defense refers to the right of a State to use force in response to an armed attack. However, countermeasures will be addressed because they may be allowed

[13] See Chapter 3.5 for a discussion about this.
[14] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 30.
[15] Compare *Corfu Channel case*, Judgment of April 9th, 1949: ICJ Reports 1949, p. 4, p. 22.

if the due diligence principle is applicable. Other consequences of State responsibility will not be discussed.

Cyberspace is a technical area, but the technical aspects of cyber operations will be covered only in order to understand the problems of cyber operations and how due diligence works in relation to this.

Due diligence is sometimes referred to with other names, for example the obligation of vigilance, the obligation of prevention, and the duty of prevention. I have decided to refer to it as simply due diligence, which is the terminology adopted in the Tallinn Manual 2.0.[16]

While the examination of the applicability of the due diligence principle is the focus of the study, the scope and the content of the principle will also be discussed in order to understand it.

1.4 Method and material

1.4.1 The dogmatic method and public international law

To examine the due diligence principle in cyberspace, I have used a dogmatic approach. There are many different definitions of the dogmatic method, but the main feature is that it attempts to analyze what the established law is, and to interpret the content of the legal sources in question.[17] At the same time, this is a study of public international law. Public international law differs from domestic law as regards the method and the sources used. In international law, there is no "single body" creating laws which are binding upon all States. [18] Neither is there a court system similar to the domestic court systems, that is able to interpret and extend the law in a comprehensive way. Furthermore, the sources of international law are different from the sources of domestic law.

Article 38(1) of the Statute of the ICJ[19] contains the most widely recognized authoritative and complete declaration of the sources of international law.[20] The article states that

[16] See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 31 for a discussion about the terminology.
[17] See Lehrberg p. 201 and Hjertstedt p. 167.
[18] Shaw p. 49.
[19] United Nations, *Statute of the International Court of Justice* (18 April 1946).
[20] Shaw p. 50.

> [t]he Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting States;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

The sources of international law are thus: treaties, custom, general principles, judicial decisions and academic writings. The article is written as an instruction to the Court, but it is considered to be the general list of sources of international law. As stated in the article, judicial decisions and academic writings are subsidiary to the other sources.

Treaties are based on the customary international law principle *pacta sunt servanda*, i.e. that agreements are binding.[21] Some treaties have a general relevance, so called law-making treaties, while others function more like contracts and apply only between two or a few States.[22] Articles 31 and 32 of the Vienna Convention on the Law of the Treaties[23] lay down the general rules of interpretation of treaties. Article 31(1) states that a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

The second source of international law mentioned in Article 38 of the Statute of the ICJ is international custom. Customary rules should constitute general practice accepted as law. From this it is possible to deduce two elements to customary rules – general practice and *opinio juris*.[24] General State practice is the actual behavior of States. *Opinio juris* is the belief of States that such behavior is, in fact, law.

Shaw describes custom by saying that rules deciding what is allowed and what is not inevitably develop in all societies, even in primitive ones.[25] These rules emerge "almost

[21] Ibid p. 67.
[22] Ibid.
[23] United Nations, *Vienna Convention on the Law of Treaties*, Treaty Series, Volume 1155 (1969) p. 331.
[24] The ICJ in *Continental Shelf (Libyan Arab Jamahiriya/Malta),* Judgment, ICJ Reports 1985, p. 13, para. 27 expressed that the substance of customary law must be "looked for primarily in the actual practice and *opinio juris* of states".
[25] Shaw p. 51.

subconsciously" and are upheld by "the members of the group by social pressures and with the aid of various other more tangible implements."[26] He further states that

> [i]t reflects the consensus approach to decision-making with the ability of the majority to create new law binding upon all, while the very participation of States encourages their compliance with customary rules.[27]

State practice needs to be established, widespread and consistent.[28] It is a two-sided practice; "one State asserts a right, either explicitly or by acting in a way that impliedly constitutes such an assertion, and the State or States affected by the claim then react either by objecting or by refraining from objection".[29] If there is no protest regarding the claim, it is considered supported. However, if there is a protest "it excludes the claim".[30] As long as the State practice is widespread and consistent, it does not need to be the practice of every single State of the world.

Opinio juris is the belief that a State activity is legally obligatory.[31] States act in a certain way because they are of the belief that there is a legal obligation to do so. This has been confirmed, for example, by the ICJ in the *North Sea Continental Shelf* cases[32], where the Court stated that "[n]ot only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it".[33]

In some cases, it is rather difficult to point to a distinct line between treaty and custom. For example, a treaty provision could establish the foundation of a rule which, together with *opinio juris*, may lead to the formation of a binding customary rule for all States, not only the ones party to the treaty.[34] This was pointed out by the ICJ in the *North Sea Continental Shelf* cases where it was considered to be one of the established methods of creating new customary rules.[35] However, it is not just any provision that can constitute customary law. According to the Court, the specific provision has to be "of fundamentally

---

[26] Ibid.
[27] Ibid p. 52-53.
[28] International Law Commission, *Draft Conclusions on identification of customary international law*, Yearbook of the International Law Commission, Volume II, Part Two (2019) p. 3 conclusion 8.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] *North Sea Continental Shelf cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. The Netherlands*, Judgment, ICJ Reports 1969, p. 3 (20 February 1969).
[33] *North Sea Continental Shelf* para. 77.
[34] Shaw p. 68. Compare also article 38 of the Vienna Convention on the Law of the Treaties.
[35] *North Sea Continental Shelf* para. 71.

norm-creating character", meaning it must be able to establish the basis of a general rule of law.[36] Furthermore, a treaty rule may have been established with the purpose of codifying a customary rule.

This international legal method will be applied throughout the study when attempting to clarify the applicability of the customary rule of due diligence. One of the challenges when applying this method is to obtain material relevant to establish the scope of the customary rule.

1.4.2 The material and its relevance in this study

Due diligence is first and foremost a rule of international customary law. It has developed through international case law. Therefore, case law will primarily be used to understand the principle.

It is difficult to obtain information about State practice and *opinio juris* regarding cyberspace. The reason for this is mainly because State cyber practice is usually classified, and an extremely small number of States have made public statements regarding their view on cyberspace.[37] A few statements from States on the applicability of due diligence in cyberspace will be used in an attempt to establish State practice and *opinio juris*.

There are also a limited number of treaties on the area of due diligence and cyberspace. The few treaties that do deal with cyber operations are of very limited scope. Due diligence, on the other hand, can be observed in some treaties, mostly in the area of environmental law. These treaties of environmental law will be used as a comparison to due diligence in cyberspace. The main focus, although, will be on international customary law.

Furthermore, several non-binding sources will be used to examine the due diligence rule and international law in cyberspace overall. The focus of the thesis is Rule 6 in the Tallinn Manual 2.0 on the international law applicable to cyber operations. The Tallinn Manual 2.0 is one of the most recent and prominent efforts at an "objective restatement of the *lex lata*" concerning cyber operations.[38] As already stated, the Tallinn Manual 2.0 is not an official document or an official source of international law. It does not in any

[36] Ibid para. 72.
[37] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 3.
[38] Ibid.

way represent States' view on applicable law in cyberspace. However, it is an effort to assess what the law is (*lex lata*) and should be credited some weight in the discussion.

As was mentioned already in the introduction, the UN created a Group of Governmental Experts (UN GGE) in 2004. The group has released two consensus reports[39] which will also be used in the assessment of the due diligence principle in cyberspace. Although, of course, the reports are not similar to treaties, they do have considerable weight for cyber international law.

Furthermore, the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts[40] (the ILC Articles on State Responsibility) will be used in order to provide a background for the reader about the concept of State responsibility in public international law. Since the articles are not a treaty, they are not binding on any States. However, the United Nations Assembly commended the articles to member States in 2012 and they have also been repeatedly referred to by courts, tribunals, and other international bodies.

Finally, academic writings, which have made a big contribution to establishing the content of due diligence in cyberspace, will be used.

1.5 Outline of the thesis

The thesis will, in *Chapter 2*, introduce the concept of cyber operations. Cyberspace will be defined, as will cyber operations. Thereafter, it will be discussed whether public international law is applicable in cyberspace.

In *Chapter 3*, State responsibility is discussed. It will be explained what it is and when States can be held responsible for international acts. Attribution will be explained and discussed shortly, and the focus will be on the problems of attributing cyber operations to a State. Countermeasures will also be covered here.

Chapter 4 examines due diligence. There will be an assessment into the history of this customary rule. Due diligence in environmental law will be examined and the conclusions in this subchapter will be used in order to understand due diligence in cyberspace. It will

[39] A/68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 June 2013) and A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (22 July 2015).
[40] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, November 2001, Supplement No. 10 (A/56/10).

be discussed whether due diligence applies to cyberspace and what scope the due diligence principle has.

Chapter 5 covers countermeasures which may be used in certain cases as a response to a cyber operation. The chapter discusses how and when countermeasures can be used in relation to the due diligence principle.

Finally, *Chapter 6* will provide a discussion of the conclusions from the study, reiterate the most important parts from the previous chapters and discuss what future initiatives there are relating to due diligence in cyberspace.

2 Cyber operations and international law

2.1 What is cyberspace?

Cyberspace has been defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[41] It is generally held that cyberspace is "not a physical place" and that one of its characterizing features include anonymity.[42] It has been compared to the high seas, international airspace and outer space, because it is sort of a "global common".[43] However, at the same time, cyberspace would not exist without certain physical components. The physical layer consists of equipment (e.g. computers, integrated circuits, cables, communications infrastructure) which is generally located on the territory of a State.[44] Cyber infrastructure is defined by the Tallinn Manual 2.0 as "[t]he communications, storage, and computing devices upon which information systems are built and operate".[45] So while cyberspace in itself may be correctly referred to as *res communis omnium*, that is not true if one looks at the whole picture of cyberspace.

The Tallinn Manual 2.0 expressed this more clearly, by stating that the view that cyberspace is a *res communis omnium* may be useful in other contexts, but not in the legal one.[46] The International Group of Experts further held that cyber acts "occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives".[47] Additionally, while cyber acts may be international in that they cross multiple borders, they are still conducted by persons or entities which are subject to the jurisdiction of one or more States.[48]

The rules of State responsibility, including due diligence, refers to "territory". In relation to cyberspace, territory is to be understood as the territory connected to the physical aspect of cyberspace. For example, this could be where the computer is located, or where the individual conducting the act is located. The rules may also refer to the cyber

[41] Tsagourias, *The legal status of cyberspace* p. 15.
[42] Von Heinegg p. 9.
[43] Ibid.
[44] Ibid.
[45] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 564.
[46] Ibid p. 12.
[47] Ibid.
[48] Ibid.

infrastructure of a State, which consequently is part of the physical layer and within the State's territory. Therefore, the view adopted by the International Group of Experts in the Tallinn Manual 2.0 is the premise used in this thesis.[49]

It is also common to find references to ICTs, i.e. Information and Communication Technologies.[50] There is no commonly held definition of the term, but one definition is that ICTs are "[a]ny information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information".[51] A few examples of this are the internet, mobile communications devices, wireless networks, and other communication technologies.[52] ICT devices can be both the source of a misuse or the target of such.[53]

2.2 What is a cyber operation?

The due diligence rule in the Tallinn Manual 2.0 applies for all *cyber operations*.

According to the manual, cyber operations are a kind of *cyber activity*.[54] A cyber activity is defined as "[a]ny activity that involves the use of cyber infrastructure or employs means to affect the operation of such infrastructure". [55] Cyber operations are further defined as "employment of cyber capabilities to achieve objectives in or through cyberspace".[56] Perhaps the most commonly referred to cyber operations are *cyber attacks*. A cyber attack is defined in Rule 92 in the manual as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". According to Tsagourias, the term cyber attack is "used to describe a variety of harmful activities taking place in the cyberspace".[57] The NATO Glossary of Terms and Definitions[58] provides a definition of one type of cyber attacks, namely computer network attacks (CAN). These sorts of attacks are actions "taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer

[49] See Chapter 4.5.4 for a further discussion about territory and infrastructure in relation to the due diligence principle in cyberspace.
[50] This is for example the terminology primarily used in the UN GGE reports.
[51] United States of America, *National Initiative for Cybersecurity Careers and Studies Explore Terms: A Glossary of Common Cybersecurity Terminology* (28 November 2018).
[52] See for example Australia, *Cyber Security Strategy* (2009) p. 1 and Austria, *Austrian Cyber Security Strategy* (2013) p. 22.
[53] UN GGE 2013 Report p. 6 para. 5.
[54] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 564.
[55] Ibid.
[56] Ibid.
[57] Tsagourias, *Cyber attacks, self-defence and the problem of attribution* p. 229.
[58] Voitasec p. 125.

network, or the computer and/or computer network itself". A mere intrusion into a computer system is not included in the term cyber attack.[59] Rather, it is to be considered as cyber espionage, which is not prohibited under public international law.[60]

However, Voitasec explains that currently there is no widely recognized definition of cyber attacks.[61] Neither is there a legal definition of the term cyber operation. In other words, it is not entirely established what acts are included in the aforementioned terms. For the purposes of this study, however, it is not necessary to establish exactly the content of the terms cyber operations or cyber attacks. Since the due diligence principle as formulated in the Tallinn Manual 2.0 is concerned with cyber operations, that term, which is unquestionably wider than the term cyber attack, will be used throughout the study.

When discussing cyber operations and the due diligence principle, certain terms will be used. *The target State* refers to the State being targeted with the cyber operation, i.e. the State whose rights are being affected. *The territorial State* is the State in whose territory the cyber operation is being operated from or where the cyber infrastructure is located, i.e. the State that has the due diligence obligation. *The author* of the cyber operation means the individual or group which is conducting the cyber operation in question.

It is important to point out that it is no longer only teenage hackers that are behind these cyber operations, but all from States and criminal or terrorist organizations to individuals with ideological motives.[62] Cyber operations can be used to "delete, alter, or corrupt software and data resident in computers" which consequently could affect physical infrastructures which are operated by computers[63]. Roscini gives examples of potential consequences of malicious cyber operations:

> a cyber operation could go as far as to disable power generators, cut off the military command, control, and communication systems, cause trains to derail and aeroplanes to crash, nuclear reactors to melt down, pipelines to explode, weapons to malfunction, banking systems to cripple.[64]

Cyber threats are a concern for the international community and therefore it is important to know whether international law applies in cyberspace.

---

[59] Von Heinegg p. 16.
[60] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 5.
[61] Voitasec p. 125.
[62] Roscini p. 2.
[63] Ibid.
[64] Ibid.

2.3 The applicability of international law to cyberspace

As has already been noted, cyberspace enjoys certain particular features. Cyberspace is borderless, actors in cyberspace can be significantly anonymous, and it is easily accessible for many actors, including non-State actors. Because of the special character of cyberspace, there has been discussions in the legal doctrine whether public international law applies to cyberspace or not. While one view[65] is that cyberspace is not within any borders, and therefore it cannot be subjected to legal concepts, the most generally held view is that international law is in fact applicable to cyberspace. If nothing else, if there were no rules applicable to cyberspace, cyberspace would become a lawless land. This would mean that non-State actors and State actors alike could perform all sorts of acts without legal consequences. Regulation is necessary in order to prevent a legal void, and to ensure the maintaining of peace and security.

Furthermore, it was highlighted in Chapter 2.1 that cyber operations do not only occur in cyberspace. They are highly associated with territory, since either the authors behind the cyber operation, or the technology used, are located on the territory of one or more States. Therefore, it is only reasonable that the territorial States must apply international law as usual.

The introduction of the Tallinn Manual 2.0 concludes that existing international law applies to cyber operations and that this is a view most States agreed on, and which has been acknowledged by NATO and the UN GGE.[66] Rule 1 of the Tallinn Manual 2.0 further states that the principle of State sovereignty applies in cyberspace.[67] Sovereignty is part of the foundation of international law and is included, for example, in the UN Charter.[68] Sovereignty itself is highly connected to the concept of territory.[69]

Furthermore, Rule 4 of the Tallinn Manual 2.0 states that a State must not conduct cyber operations that violate the sovereignty of another State.[70] It is prohibited in international law to prevent or disregard another State's exercise of its sovereignty, and this is true also for cyber operations.[71]

The first consensus report released by the UN GGE in 2013 was highly proclaimed since it stated plainly that international law is applicable to cyberspace. At the same time,

[65] See for example Barlow.
[66] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 3.
[67] Ibid p. 11.
[68] See the United Nations, *Charter of the United Nations*, 1945, 1 UNTS XVI art. 2(1).
[69] Shaw p. 352.
[70] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 17.
[71] Ibid.

however, it is clear from the second consensus report, in 2015, that there are many different views among the States on international law and the scope of its application. Furthermore, when concluding the last round of deliberations in 2017, it became clear that the UN GGE would not be able to reach consensus and could therefore not release a third consensus report. The task given by the General Assembly was to continue to study "how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States".[72] Although there are obvious difficulties in the limitations of international rules in cyberspace, and States do not fully agree on the scope, it cannot be doubted that the UN GGE did reach consensus on the applicability of international law in cyberspace.

It must be concluded from the above that international law is indeed applicable to cyberspace.

[72] A/RES/70/237, *Developments in the field of information and telecommunications in the context of international security* (23 December 2015).

3 State responsibility

3.1 Introduction

In order to understand the due diligence principle and how it works, some understanding of State responsibility is needed. State responsibility is a central principle of public international law. It rests on the foundation that States are sovereign and equal. The principle stipulates that international responsibility occurs between two States, when one State commits an internationally unlawful act against the other State.[73] State responsibility attempts to answer three questions, namely, if there has been a breach of an international obligation by a State, what the consequences are for such a breach, and who may seek reparation or respond to the breach.[74]

The International Law Commission adopted draft articles on State responsibility on 9 August 2001 (the ILC Articles on State Responsibility). According to Shaw, the Draft Articles are considered to have a particular weight to them, since the General Assembly in a resolution[75] annexed the text of the articles and commended them to governments, which is an unusual procedure.[76] Crawford describes the ILC Articles on State Responsibility as the "modern framework for State responsibility".[77]

3.2 The elements of State responsibility

Article 1 of the ILC Articles on State Responsibility forms the foundation for State responsibility:

> Every internationally wrongful act of a State entails the international responsibility of that State.

The term "internationally wrongful act" is aimed to include all wrongful acts of a State, regardless of if it originates from a positive action or from an omission or a failure to act. According to the Commentary, there are as many cases where State responsibility has

[73] Shaw p. 566.
[74] Crawford & Olleson p. 443.
[75] A/RES/56/83, *Responsibility of States for internationally wrongful acts* (12 December 2001).
[76] Shaw p. 568. There was even talk about turning them into a convention.
[77] Crawford p. 45.

become relevant because of an omission as cases where the wrongful act arises from a positive obligation.[78]

Article 1 is the general rule of State responsibility, which is commonly supported by practice.[79] Article 2 states that the internationally wrongful act of a State must be attributable to the State and must constitute a breach of an international obligation of the State. The principle in Article 2 has been confirmed by case law.[80]

Attribution will be covered in Chapter 3.4. According to Article 12 in the ILC articles on State Responsibility, there is a breach of an international obligation when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character. In other words, what is a breach depends on what the international obligation is.[81]

One may notice that any preconditions about "fault" by the State or "damage" suffered by an injured State is missing from article 1.[82] There has been a debate in the legal literature whether some kind of fault is required or whether it is an "objective responsibility".[83] Case law generally support the latter.[84] However, Crawford & Olleson holds that whether fault is necessary depends on if the relevant primary obligation includes it at a necessary condition.[85] The same could be said about the question of whether some kind of harm or damage is necessary.[86] The *Rainbow Warrior* case[87] established that "damage" is generally not a requirement determining an internationally wrongful act.[88]

According to Article 42 of the ILC Articles on State Responsibility, a State is entitled as an injured State to invoke the responsibility of another State if the obligation breached is owed to that State individually or to a group of States, including that State, or the international community as a whole. Furthermore, the breach of the obligation must specifically affect the injured State or is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.

---

[78] ILC Articles on State Responsibility p. 35.
[79] Shaw p. 569
[80] Ibid.
[81] Crawford & Olleson p. 447.
[82] Crawford p. 49.
[83] Crawford & Olleson p. 462.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] *Rainbow Warrior Case*, (New Zealand v. France) (1990) 82 I.L.R. 500.
[88] Ibid p. 267 para. 109.

In the Eritrea-Ethiopia Claims Commission it was established that "clear and convincing" evidence is required to support claims of State responsibility.[89] The ICJ has stated that claims against a State involving "charges of exceptional gravity" has to be accompanied by evidence that is "fully conclusive".[90]

3.3 Attribution

States are legal entities. As such, they cannot act themselves. Article 2 of the ILC Articles on State Responsibility declares that in order for an act or omission to amount to an internationally wrongful act, the conduct in question must be attributable to the State. This element of State responsibility is necessary since the State, as a single entity, is not the one acting. Instead, it is a State organ or a person or a group which acts on behalf of the State. A State is normally only responsible for the acts of its organs or officials.[91] The rules of attribution, which are included in Chapter II of the ILC Articles on State Responsibility, aim to establish a connection between these agents and the State itself.

There are three general attribution standards.[92] Article 7 of the ILC Articles on State Responsibility states that the conduct of an organ or of a person or entity empowered to exercise elements of governmental authority shall be considered an act of the State under international law if acting in that capacity, even if it exceeds its authority or contravenes instructions.

The second standard according to Article 8 of the ILC articles on State Responsibility is that the conduct of a person or group of persons shall be considered as an act of State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct. In the *Nicaragua* case, the ICJ stated, regarding the level of control necessary, that "it would in principle have to be proved that [the State in question] had *effective control* of the military or paramilitary operations in the course of which the alleged violations were committed".[93]

---

[89] *Final Award – Ethiopia's Damages Claims between the Federal Democratic Republic of Ethiopia and the State of Eritrea*, Eritrea-Ethiopia Claims Commission (17 August 2009) para. 35. Compare also Shaw p. 567.
[90] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, ICJ Reports 2007, p. 43, para. 209. [hereinafter *Bosnian Genocide*].
[91] See Articles 4 and 5 of the ILC Articles on State Responsibility.
[92] Tsagourias, *Cyber attacks, self-defence and the problem of attribution* p. 236.
[93] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, p. 14 para. 115 [emphasis added] [hereinafter the Nicaragua case].

Finally, Article 9 of the ILC Articles on State Responsibility provides that the conduct of a person or a group of persons shall be considered as an act of the State under international law if the person or group was in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority.

This is not a complete examination of the rules of attribution, but it presents the foundation of attribution and explains the main ways of attributing acts. The main reason for introducing the rules of attribution in this study is to explain the difficulties in relation to cyber operations. This will be done in the next chapter.

3.4 The problems of attribution in cyberspace

As has been explained in the previous chapter, attribution is one of the conditions for establishing the responsibility of States. However, with the particular features of internationally wrongful acts in cyberspace, it is not that simple. Cyber operations produce both technical and legal challenges to public international law. It has been described as being "more art than science".[94] Attribution is an issue which is often discussed in the international legal doctrine, but it is still a highly underdeveloped part of international cyber law.

Attribution attempts to identify the source of the cyber operation, which is an important matter, for example in order to respond properly to the cyber operation.[95] However, identifying the actor behind the cyber operation is just one of several issues of attribution in cyberspace. Chircop describes it as a three-level problem.[96]

First, the computer or computers used in the cyber operation must be identified. This is not technically impossible, since every computer has an IP address which is unique to it. The IP address can in certain circumstances be used to obtain the exact position of the computer. However, the actor of the cyber operation may be able to mask the IP address so that it is not trackable. Not only that, but if the actor uses a network modification technique, it can make it seem as if the computer is in a different location to where it in fact is.[97]

[94] Banks p. 1493.
[95] Tsagourias, *Cyber attacks, self-defence and the problem of attribution* p. 230.
[96] Chircop p. 646.
[97] Ibid.

The second part of the problem, which is perhaps even more daunting, is that it is necessary to identify the person, or the group, operating the computer. Attribution attempts to establish the connection between the State and an *actor*. Of course, even if the location of the computer was identified, this does not automatically mean that the person behind the act can be identified.[98]

Finally, the last part of the problem is that, even if the computer location is established and the person operating the computer identified, there must be a sufficient legal nexus between the actor and the State.[99] The ICJ stated in *Bosnian Genocide* that it had to find a "sufficiently direct and certain causal nexus between the wrongful act […] and the injury suffered".[100] The wrongful act in the case was the breach of the obligation to prevent genocide.[101]

Tsagourias adds another issue to the ones described already. It is possible that the cyber operation is performed by multi-stage cyber attacks, which means that there are several computers at different locations (or even different jurisdictions) and that they are operated by different people.[102] Naturally, this complicates matters even more. Moreover, cyber operations can emerge rapidly and are therefore challenging to foresee. Tsagourias further states that attribution is important for the counteraction to be effective but also lawful.[103]

All of these issues explained above consequently lead to the difficulty of holding States responsible for cyber operations. Without being able to infer responsibility on States, the risk is that actors will have free reigns in cyberspace. Furthermore, States will not be able to use countermeasures in order to protect themselves against the attack.

3.5 Countermeasures

The international legal system is based on consent and the fact that States are sovereign and equal. However, it does happen that States perform internationally wrongful acts. If that happens, the targeted State may be able to use non-forcible measures against the State breaching the international rule. These non-forcible measures are referred to as countermeasures.

[98] Ibid.
[99] Ibid.
[100] *Bosnian Genocide* para. 462.
[101] Ibid.
[102] Tsagourias, *Cyber attacks, self-defence and the problem of attribution* p. 233.
[103] Ibid p. 230.

Article 22 of the ILC Articles on State Responsibility provides that the wrongfulness of an act is precluded if and to the extent that the act constitutes a countermeasure. In the *Gabcikovo-Nagymaros Project* case, the ICJ stated that a countermeasure has to meet certain conditions in order to be justifiable.[104] First, the countermeasure must be taken in response to a previous international wrongful act of another State and must be directed against that State.[105] Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it.[106] In the view of the Court, an important consideration is that the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.[107] Furthermore, the Court stated that another condition for the lawfulness of a countermeasure is that its purpose must be to induce the wrongdoing State to comply with its obligations under international law, and that the measure must therefore be reversible.[108]

Countermeasures are dealt with in Chapter II of the ILC Articles on State Responsibility. Article 49 states the object and limits of countermeasures and the first paragraph provides that an injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under the draft articles. Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures and shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligation in question. Obligations not affected by countermeasures are covered in Article 50 which makes it clear that countermeasures shall not affect the obligation to refrain from the threat or use of force as embodied by the UN Charter[109], obligations for the protection of fundamental human rights, obligations of a humanitarian character prohibiting reprisals and other obligations under peremptory norms of general international law.

Countermeasures in relation to the due diligence principle will be further discussed in Chapter 5.

---

[104] *Gabcikovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, ICJ Reports 1997, p. 7, para. 83.
[105] Ibid.
[106] Ibid.
[107] Ibid para. 84.
[108] Ibid para. 87.
[109] Article 2(4) of the UN Charter.

4 Due diligence

4.1 Introduction

There are two different ways in which States can be held responsible. The first one is by attribution. The problems of attribution in cyberspace have already been explained in previous chapters. The second way is where the State fails to satisfy the due diligence principle. If attribution in cyberspace has been considerably discussed by academics, the due diligence principle in cyberspace has received significant less attention. Furthermore, military responses to cyber attacks has gained much more focus than situations below the threshold of use of force, both in academic and political debate.

This disproportional focus does not mirror the reality, which is that there are no cyber operations which have actually been at the level of an armed attack, and it is much more common with peacetime cyber operations.[110] It is also a fact that many of the authors of cyber operations are private individuals or international organizations. These subjects are generally not able to be held responsible for acts contrary to international law and it is, usually, not possible to attribute the acts to a State. However, the State may still have international responsibility for these acts, if the State failed in some obligation to prevent the act in question. In that case, responsibility is the consequence of a State's own failings, not the direct result of the actions of private individuals.[111] Attribution and due diligence have previously been referred to as direct and indirect responsibility. [112]

Due diligence is a general obligation, which assumes its meaning depending on the context and in relation to another specific international norm. The due diligence principle in *Corfu Channel* is rather simplistic in its expression compared to the formulation in the Tallinn Manual 2.0 for example. This chapter will examine the history of due diligence, its development in environmental law, and the applicability and scope of due diligence in the field of cyberspace.

4.2 The history of due diligence

As has already been stated, due diligence refers to the obligation of States to ensure that their territory is not being used to affect the rights of a third State. In the 17th century,

[110] Geiss & Lahmann p. 657.
[111] Crawford & Olleson p. 456.
[112] Hessbruegge p. 268.

Grotius established the foundation of the concept of due diligence.[113] However, it would take until the 19th century before due diligence began to assume its current form and to impose a duty on States.[114] In the early days, because of the increased movement of people across territorial borders, due diligence became important for the protection of aliens.[115] For example, Justice Moore observed in the *SS Lotus Case* that "it is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people".[116]

The concept of State sovereignty also emerged stronger during the 19th century and led to a requirement of States to protect "the security of other States in times of peace and war".[117] The principle of sovereignty is well-established in international law and means that States are prohibited from violating the sovereignty of another State. The principle of sovereignty is expressed, for example, in Article 2(1) of the UN Charter. Due diligence is derived from this principle. In the *Island of Palmas* case (1928), territorial sovereignty was interpreted as including an obligation to protect within the territory the rights of other States.[118] Max Huber, the arbitrator in the case, stated that "[t]erritorial sovereignty … involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war".[119] If a State enjoys the right to exercise sovereignty over objects and activities within its territory, necessarily there needs to be a corresponding legal obligation.

The term due diligence was not included in the ILC Articles on State Responsibility. The commentary to Art. 2 states that

> Whether responsibility is 'objective' or 'subjective' in this sense depends on the circumstances, including the content of the primary obligation in question. The articles lay down no general rule in that regard. The same is true of other standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for

[113] International Law Association, *Study Group on Due Diligence in International Law,* First Report (7 March 2014) p. 2.
[114] Ibid.
[115] Ibid.
[116] *SS Lotus (France v Turkey),* 1927 PCIJ (Ser. A), No 10 para 269.
[117] ILA Study Group, First Report p. 2.
[118] *Island of Palmas Case (or Miangas),* United States v. Netherlands, Award, II RIAA 829, ICGJ 392 (PCA 1928), Permanent Court of Arbitration (4 April 1928) p. 839.
[119] Ibid.

> reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation.[120]

What this suggests is that the ILC Articles on State Responsibility do not control whether the primary rule in question requires an element of fault or lack of diligence before it can be considered a breach.[121] Furthermore, the Commentary held that States are not responsible for the acts of private individuals if they are, for example, seizing an embassy (which the rules of attribution make clear), but "it will be responsible if it fails to take all necessary steps to protect the embassy from seizure, or to regain control over it".[122] From this it is clear that the Commission did indeed consider the obligation of due diligence.

Due diligence saw the biggest development in practice in the field of environmental law during the second half of the 20th century.[123] Since due diligence was not included in the ILC Articles on State Responsibility, the Commission included the concept in other contexts.[124] Perhaps the most prominent one is in the Draft Articles on the Prevention of Transboundary Harm.[125] The Commentaries to the Draft Articles expressed that the duty to take "preventing or minimization activities measures is one of due diligence".[126]

Case law has repeatedly referred to the notion of due diligence. For example, in the *Trail Smelter Arbitration* case (1941)[127], which concerned an environmental dispute between the United States and Canada, the Tribunal stated that

> under the principles of international law, as well as the law of the United States, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.[128]

The Tribunal accepted a due diligence standard in order to limit transboundary damage. There was not much international precedent for the Tribunal to use in its assessment. Instead, the Tribunal turned to domestic decisions for inspiration and it refers to the

[120] ILC Articles on State Responsibility p. 34.
[121] Koivurova para. 7.
[122] ILC Articles on State Responsibility p. 39.
[123] ILA Study Group, First Report p. 5. See more about environmental law in Chapter 4.3.
[124] Ibid.
[125] See more about due diligence and environmental law in Chapter 4.3.
[126] ILA Study Group, First Report p. 5.
[127] *Trail Smelter Arbitration*, United States v. Canada, 3 UNRIAA 1905 (1938 and 1941).
[128] Ibid p. 1965.

decisions of the Supreme Court of the United States as the basis of its conclusions.[129] The Tribunal held that the Dominion of Canada, according to international law, was responsible for the conduct of the Trail Smelter.[130] It further decided that the Trail Smelter should be required to refrain from causing any damage through fumes in the State of Washington and to fix the indemnity of such damage.

The Tribunal's decision has, however, received some criticism. It is claimed that the Tribunal analogized from domestic decisions in order to "create" an international principle.[131] While this may be true to a certain extent, it is important to remember that the obligation of due diligence existed already as a concept before the case. The Tribunal only expanded on the content of due diligence by referring to domestic decisions. One might claim that the international principle formulated in the case should be restricted to the specific circumstances of the case, or that it should simply be considered a principle of environmental law. This discussion will be continued in Chapter 4.3 when the development of due diligence in environmental law is examined.

Nevertheless, the notion of due diligence can be seen outside of environmental case law. If there was ever any doubt about the application of the due diligence principle outside of the environmental area, that doubt was erased by the ICJ in the *Corfu Channel* case. In 1949, the ICJ in the *Corfu Channel* case tried the State responsibility regarding the laying of mines in Albania's territory by an unnamed third party. The Court held Albania responsible because of the State officials' knowledge of the activity and their omission to warn shipping in the area. The Court stated that it is "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[132] The Court identified it as a general and well-recognized principle. *Corfu Channel* has been said to best articulate the general principle of due diligence.[133]

Furthermore, in its Advisory Opinion to the UN General Assembly on the *Legality of the Threat or Use of Nuclear Weapons*[134], the ICJ stated that "[t]he existence of the general obligation of States to ensure that activities within their jurisdiction and control

[129] Miller, Trail Smelter Arbitration para 7.
[130] *Trail Smelter Arbitration*, United States v. Canada, 3 UNRIAA 1905 (1938 and 1941) p. 1965.
[131] Miller para. 7.
[132] *Corfu Channel case*, Judgment of April 9th, 1949: ICJ Reports 1949, p. 4, p. 22.
[133] Chircop p. 649.
[134] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, p. 226 [hereinafter *Nuclear Weapons Advisory Opinion*].

respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment".[135]

The rise of transnational terrorism has further raised the attention of the doctrine of due diligence. The UN Security Council has repeatedly, in 1999 and in 2000, demanded that the Taliban (at that point, the Afghanistan's government), take appropriate effective measures to ensure that the territory under its control is not used for terrorist installations or camps, or for the preparation or organization of terrorist acts against other States or their citizens.[136]

There are many references to due diligence in the sources of international law, although the term itself is at times absent. This is especially true for international treaty law.[137] There are exceptions, such as the 2011 Council of Europe Convention on Preventing and Combatting Violence against Women[138], which explicitly includes due diligence in article 5. Despite these rare exceptions, it is fair to say that the term is not in frequent use. Nonetheless, due diligence is an essential feature of international law. It is also particularly well suited as a tool for responding to complicated legal situations of responsibility in newer, more complex, areas such as cyberspace.[139]

According to an ILA study group on due diligence, the principle "is now clearly a part of customary international law, and reflects cornerstone concepts of international law (including State sovereignty, equality, territorial integrity, and non-interference)".[140] They explain the particular position of due diligence in international law by describing its desirable features; it is a concept by which States can observe specific behavioral standards, or intend to accomplish specific outcomes, but without specifying the exact result or timeframe by which this is supposed to occur.[141] It is generally true, that the more general a legal concept is, the easier it can stand the test of time. Therefore, it is not surprising that due diligence remains a prominent standard of influential law and that its use has spread, and is still spreading, to other areas of international law besides environmental law.

---

[135] Ibid p. 242.
[136] UN SC Res. 1267 (15 October 1999); UN SC Res. 1333 (19 December 2000).
[137] ILA Study Group, First Report p. 6.
[138] *Council of Europe Convention on preventing and combating violence against women and domestic violence*, CETS No. 210 (11 May 2011).
[139] International Law Association, *Study Group on Due Diligence in International Law*, Second Report (July 2016) p. 2.
[140] Ibid p. 5.
[141] Ibid.

4.3 Due diligence in environmental law

Due diligence has seen the most development in the field of environmental law. Because of this, the use of due diligence in environmental law serves as a good yardstick when assessing the due diligence principle in the cyber context. Therefore, the application and scope of due diligence in environmental law will be examined in this chapter.

In environmental law, due diligence obligations have been included in a number of international treaties. For example, Article 192 of the United Nations Convention on the Law of the Sea (UNCLOS) states that "States have the obligation to protect and preserve the marine environment".[142] Article 194(2) of UNCLOS states that "States shall take all measures necessary to ensure that activities under their jurisdiction and control are so conducted as not to cause damage by pollution to other States and their environment". Shaw says that "[t]he test of due diligence is in fact the standard that is accepted generally as the most appropriate one".[143] At the same time, he concludes that what exactly due diligence means, is not obvious. In some cases, such as the due diligence obligation prescribed for in UNCLOS, the measures are specified and there are references to other relevant treaties.[144] But at other times, the matter is more uncertain.[145] Nonetheless, the prevention of transboundary harm is a key component in international environmental law. Due diligence is necessarily a huge part of this.

Article 3 of the ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities[146], adopted in 2001, states that States "shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof".

The Commentary to the Draft Articles further adds that:

> The obligation of the State of origin to take preventive or minimization measures is one of due diligence. It is the conduct of the State of origin that will determine whether the State has complied with its obligation under the present articles. The duty of due diligence involved, however, is not intended to guarantee that significant harm be totally prevented, if it is not possible to do so. In that eventuality, the State of origin is required … to exert its best

[142] UN General Assembly, *Convention on the Law of the Sea* (10 December 1982) [hereinafter UNCLOS].
[143] Shaw p. 621.
[144] Ibid.
[145] Ibid.
[146] International Law Commission, *Draft articles on Prevention on Transboundary Harm from Hazardous Activities, with commentaries*, Yearbook of the International Law Commission, Volume II, Part Two (2001).

> possible efforts to minimize the risk. In this sense, it does not guarantee that the harm would not occur.[147]

The Commentary, therefore, besides confirming that due diligence is an obligation of conduct, clarifies that the State is not obligated to do more than what is possible. The State simply has to do its best to prevent the transboundary harm. Even if the State fulfills its due diligence obligation, it is not a guarantee that there will be no harm. UNCLOS similarly clarifies in Article 194(1) that States only need to use "the best practicable means at their disposal and in accordance with their capabilities". Although, this is not stated directly in relation to the due diligence obligation, but in the paragraph regulating prevention of pollution from any source. It is reasonable to assume that the State have a stricter obligation when the source is in fact from within their own jurisdiction or control. What is clear from the treaties and the case law is that there is a standard of reasonableness included in the due diligence obligation. What States need to do in order to fulfill its obligation is expressed in different ways depending on the context. Terminology used is, for example, that States should use all appropriate measures, use all measures necessary, or use all the means at their disposal. What is also implied, and sometimes directly expressed, is that States are not obligated to do more than they are able to do.

The cause of an environmental damage to a nearby State is often a private company. The *Trail Smelter Arbitration* case, mentioned above, is one example of this. The case concerned a private company in Canada which was located close to the border with the United States of America. The company polluted the environment in the United States and a Tribunal was established to resolve the dispute between the States and led to the reference by the Tribunal to the standard of due diligence.[148] Because the actor was a private company, the State responsibility rules of attribution could not be used. Instead, the State responsibility was based on the obligation of States to not permit the use of its territory in a manner injurious to other States.

As recent as 2010, the ICJ in its *Pulp Mills on the River Uruguay* case confirmed that "the principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory" before going on to cite the Court's fundamental statement in *Corfu Channel*.[149] The Court went on to state that a State is "obliged to use

[147] Ibid para. 7.
[148] See Chapter 4.2.
[149] *Pulp Mills on the River Uruguay (Argentina v Uruguay)*, ICJ Reports 2010, p. 14, para. 101 [hereinafter *Pulp Mills*].

all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State.[150] Note that, similarly to the *Trail Smelter Arbitration* case, the Court included "damage" as a criterium for due diligence to apply.

A relevant question is whether the principle adopted in the environmental case law can be extended to other areas of international law. It is possible, for example, to argue that the *Trail Smelter Arbitration* case had some specific circumstances and that the principle should be limited to these. Perhaps it should simply be considered a principle of environmental law, or even limited to cases dealing with fumes. However, this argument does not stand considering that the obligation of due diligence existed already prior to the *Trail Smelter Arbitration* case, and that, since then, it has been developed both in environmental law and in other areas of international law.

It is also true that due diligence is a flexible concept, which has to be adapted due to the specific circumstances in every case. States are required to "take preventive action in relation to foreseeable harm, that is, when they possess scientific evidence that significant transboundary damage is likely."[151] The due diligence standard varies according to context. There is not one standard of due diligence which applies to all primary rules.[152] This was confirmed by the *Seabed Mining Advisory Opinion.*[153] The *Seabed Mining Advisory Opinion* (2011)[154] concerned the Republic of Nauru and the Kingdom of Tonga who both put forward applications for approval of a plan of work for exploration in the area reserved for the conduct of activities by the Seabed Mining Authority. The Area means the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction.[155] The Council of the International Seabed Authority submitted the Advisory Opinion to the Seabed Disputes Chamber and requested that the Chamber rendered an advisory opinion on certain questions of, *inter alia*, legal responsibilities and obligations of States. The Chamber therefore had the opportunity to add to the case law of due diligence. It stated that due diligence is a variable concept and that it may change over

[150] Ibid.
[151] ILA Study Group, First Report p. 26.
[152] ILA Study Group, Second Report p. 20.
[153] ILA Study Group, First Report p. 26.
[154] *Responsibilities and obligations of States with respect to activities in the Area,* Advisory Opinion, 1 February 2011, ITLOS Reports 2011, p. 10 [hereinafter the Seabed Mining Advisory Opinion].
[155] See UNCLOS art. 1 para. 1(1).

time "as measures considered sufficiently diligent at a certain moment may become not diligent enough in light, for instance, of new scientific or technological knowledge".[156]

Furthermore, the standard of due diligence may depend on the risk of the activities. In *Pulp Mills*, the Court found that "it may now be considered a requirement under general international law to undertake an environmental impact assessment where there is a risk that the proposed industrial activity may have a significant adverse impact in a transboundary context, in particular, on a shared resource".[157] The use of environmental impact assessments (EIAs) was further elaborated in the dispute concerning *Certain Activities Carried out by Nicaragua*[158], where the ICJ emphasized that in order to prevent significant transboundary harm, the due diligent obligation triggers the procedural obligations to carry out an EIA and, if the EIA confirms a risk of significant harm, to notify and consult the potentially affected State.[159]

The Court's instructions on what a State should do to fulfill the obligations can be divided into three steps. The first step is to assess whether there is a risk of transboundary harm. The second step is, if the State establishes that there is such a risk, to carry out an EIA. The content of the assessment is up to the State to decide for each case.[160] Finally, if there is a confirmed risk of significant transboundary harm by the EIA, "the State planning to undertake the activity is required … to notify and consult in good faith with the potentially affected State, where that is necessary to determine the appropriate measures to prevent or mitigate the risk".[161] In other words, the three steps are risk ascertainment, risk assessment, and notification or consultation. By contrast, if the State determines that no risk exists, there is no need to carry out an EIA or to notify or consult the affected State. However, these steps have also been criticized for oversimplifying the obligation of due diligence. In her separate opinion, Judge Donoghue stated that "the Judgment could be read to suggest that there is only one circumstance in which the State of origin must notify potentially affected States", i.e. when a need to do an EIA has been established.[162] The due diligence obligation, however, might not be limited to this one circumstance. It is, for example, possible to imagine a scenario in which a State is aware

[156] *Seabed Mining Advisory Opinion* para. 117.
[157] *Pulp Mills* para 204.
[158] *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* and *Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment, ICJ Reports 2015, p. 665 [hereinafter *Certain Activities Carried Out by Nicaragua*].
[159] Ibid para. 104.
[160] Ibid.
[161] Ibid.
[162] Ibid, Separate Opinion of Judge Donoghue p. 788, para. 21.

of a potential risk which warrants notifying potentially affected States, but where there is no need to do an EIA. The State might also need the input of a potentially affected State in order to carry out the EIA.

The damage needs to be established "by clear and convincing evidence", as emphasized by the tribunal in the *Trail Smelter Arbitration* case.[163] This is true for all issues regarding State responsibility, not only the due diligence principle.[164] The due diligence obligation also must be foreseeable for States.

The ICJ in the *Corfu Channel* case clearly stated that Albania "ought to or should have known".[165] This suggests that it is not enough to fulfil the due diligence obligation to claim that a State did not have actual knowledge. It must also be established whether the State had constructive knowledge.[166]

International environmental law has significantly helped in the understanding of the notion of due diligence. However, it remains unclear how much the particulars of due diligence in environmental law can be used to establish the content of the principle in other areas of international law. More specifically, the question for the following chapters is how our knowledge of due diligence so far can help in the assessment of the due diligence principle applicable to cyber operations.

4.4 The applicability of due diligence in cyberspace

As cyberspace was emerging, a pressing issue was whether international law, and, more specifically, the prohibition on violation of sovereignty applied to cyberspace as well. As has already been discussed, there is now a general consensus that it *does* apply to cyberspace. Does this mean that due diligence is also applicable in cyberspace?

According to the Tallinn Manual 2.0 – yes. The manual clearly states that it considers its rules to be reflecting the law as it is (*lex lata*).[167] The International Group of Experts in the Tallinn Manual 2.0 explains that new technologies are "subject to pre-existing international law absent a legal exclusion therefrom" and argue that this means that the due diligence principle applies in cyberspace. [168] The argument therefore goes that since due diligence is to be considered a general principle of international law, it is presumed

[163] *Trail Smelter Arbitration* p. 1965.
[164] See *Eritrea-Ethiopia Claims Commission* as referenced in Chapter 3.2.
[165] *Corfu Channel* p. 18.
[166] See a further discussion about constructive knowledge in Chapter 4.5.5.
[167] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 3.
[168] Ibid p. 31, with reference to the *Nuclear Weapons Advisory Opinion* para. 39.

that it is applicable to cyberspace unless State practice or *opinio juris* excludes it. At this moment, there is no such conclusive State practice or *opinio juris*. On the contrary, several States have expressed both that customary international law applies to cyberspace and that due diligence is among these customary rules.

For example, the White house stated, in its International Strategy for Cyberspace (2011), that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace".[169]

The French ministry of defense published a document in September 2019, describing its views on how international law applies in cyberspace.[170] France, by reference to the 2015 UN GGE consensus report, declared that sovereignty over computer systems on the State's territory creates a customary obligation of due diligence and that the duty means that the State should not "knowingly allow its territory to be used for internationally wrongful acts using ICT".[171]

In July 2019, the Dutch Minister of Foreign Affairs, in a letter[172] to the parliament, explained the view of the Government on international law's applicability in cyberspace. The Annex to the letter, referring to *Corfu Channel*, and noting that not all countries agree that due diligence is an obligation in its own right in international law, clearly states that the Netherlands views the principle as an obligation in its own right.[173] Violating the principle therefore constitutes an internationally wrongful act.[174]

Most State documents, however, stay quiet on the topic of due diligence obligations and avoid connecting it to the attribution problematics.[175] Nonetheless, Väljataga says that it is possible to detect notions of States' views on due diligence in these documents.[176] Partly by looking at national cyber security strategies, she draws a speculative conclusion that States "agree that cyber due diligence follows from cyber sovereignty" but that they "have not agreed on whether and how cyber due diligence can form the basis for state

[169] The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, 2011) p. 9.
[170] Roguski.
[171] Roguski.
[172] Minister of Foreign Affairs, *Letter to parliament on the international legal order in cyberspace + Appendix: International law in cyberspace* (26 September 2019).
[173] Ibid Appendix p. 4.
[174] Ibid.
[175] Väljataga, *Tracing* opinio juris *in National Cyber Security Strategy Documents* p. 8.
[176] Ibid.

responsibility".[177] At the same time, the strategy documents seem to recognize the obligations and responsibilities deriving from sovereignty.[178] Since due diligence is an obligation deriving from sovereignty, States still seem open to the fact that it is applicable to cyberspace, although the scope of its applicability is not clear.

It was also affirmed by the UN General Assembly, already in 2001, that States should take preventive measures in cyberspace.[179] The UN General Assembly encouraged States to "ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies".[180]

Furthermore, the UN GGE's have expressed that principles of international law that "flow" from the principle of sovereignty are binding in the cyber context.[181] Since due diligence is a principle which derives from the principle of sovereignty, this statement should include due diligence. Additionally, the UN GGE included in its 2015 report the recommendation that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".[182]

At the same time, however, those who do not believe due diligence to be applicable in the context of cyber operations have used the UN GGE as an argument against its applicability.[183] In their reports, the Experts stated that States "should" observe the due diligence principle, rather than that they "must".[184] Nevertheless, according to the Tallinn Manual 2.0, the GGE's statements do not "definitively refute the existence of such a principle".[185]

While there is considerable evidence which points to the fact that due diligence should be considered applicable in the cyber context, it is a fact that not all States have accepted due diligence as customary law, especially not in cyberspace.[186] States are reluctant to credit the due diligence principle with a *lex lata* status. Considering that cyberspace still has to be seen as a new area of international law, this is not surprising. It is difficult, however, to draw any conclusions as to what States will say about the due diligence principle. Here it is relevant to point out that State practice must be widespread and

[177] Ibid p. 9.
[178] Ibid p. 18.
[179] A/RES/55/63, *Combating the criminal misuse of information technologies* (4 December 2000) p. 2.
[180] Ibid.
[181] UN GGE 2013 Report para 20.
[182] UN GGE 2015 Report para. 13(c). Compare also para. 28(e).
[183] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 31.
[184] UN GGE 2013 Report, para 23; UN GGE 2015 Report paras. 13(c), 28(e).
[185] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 31.
[186] Hankinson.

consistent, but that it does not need to be the practice of every State in order to be a customary rule. Considering the few statements that do exist, or have been made public about due diligence, it is not enough to establish such State practice or *opinio juris*.

Although it cannot be predicted whether State practice and *opinio juris* will confirm or deny the applicability of due diligence to cyberspace, the argument of this thesis is that the principle should be treated as applicable to cyberspace. This also follows the prerequisite of the Tallinn Manual 2.0. Due diligence is a general principle of international law which so far has been adapted to different areas of law. Because it is such a flexible concept, as pointed out already in the examination of the principle in the area of environmental law, it can easily be adapted to fit in the cyber context. It is my view that due diligence will be applicable, in one way or another, in cyberspace. The main question to be answered is what the content of the applicable principle will be.

4.5 The scope of due diligence

4.5.1 General notes about the scope

Rule 6 in the Tallinn Manual 2.0 describes the due diligence principle in cyberspace:

> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.[187]

The basis of this rule is the general international law principle that "States must exercise due diligence in ensuring territory and objects over which they enjoy sovereignty are not used to harm other States".[188] The International Group of Experts have used the commonly accepted definition in the *Corfu Channel* case when formulating the principle in the Tallinn Manual 2.0 and express that due diligence is the "standard of conduct expected of States when complying with this principle".[189]

The due diligence principle applies to all third party cyber operations. It does not matter if the cyber operation is carried out by a private person, a corporation, a non-State actor, or a State.[190]

[187] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 30.
[188] Ibid.
[189] Ibid.
[190] Ibid p. 32.

One of the concerns about the due diligence principle is that the principle would put an unreasonable burden on States. In this section, it will be shown that that is not the case. It will cover the different criteria of due diligence in order to understand the scope of the principle.

4.5.2 Internationally wrongful act and affecting a right

In order for the due diligence principle to come into play, the cyber operation needs to amount to an internationally wrongful act.[191] This may not seem so implausible, since it would not be reasonable for the target State to have to put an end to the cyber operation if the operation itself was not unlawful. The Tallinn Manual 2.0 provides an example regarding this.[192] If State A is monitoring State B's governmental databases by using cyber infrastructure in State C, State C does not have a due diligence obligation to terminate the operations. The reason for this is that the monitoring amounts to cyber espionage, and cyber espionage is not unlawful under international law.[193]

The International Group of Experts also held that the due diligence obligation only applies to a State "when the cyber operation that is being mounted from or through its territory would be unlawful under international law if it had been conducted by the territorial State itself".[194]

However, the matter becomes more complicated when including non-State actors in the due diligence scenarios. States are the only entities capable of performing acts amounting to internationally wrongful acts. Cyber operations conducted by non-State actors, which are not attributable to a State, are not considered internationally wrongful acts. It is, generally speaking, States, not non-State actors, that violate international law. The International Group of Experts nonetheless agreed that the due diligence principle applies also for cyber operations where the author is a non-State actor, provided that the cyber operation result in serious adverse consequences and affect a right of the target State.[195] This is consistent with the position taken in environmental law, where also the conduct of non-State actors activates the due diligence obligation.[196] Considering that

[191] Ibid p. 34.
[192] Ibid p. 35.
[193] See Rule 32 in Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 168.
[194] Ibid p. 35.
[195] See Chapter 4.5.3 regarding the "serious adverse consequences" criterium.
[196] See for example the *Trail Smelter Arbitration* case where it was the actions of a private company which made the due diligence obligation come into play.

there are many non-State actors in cyberspace (similar to in environmental law), it would not be reasonable to exclude these from the scope of the principle. What the International Group of Experts also concluded is that there is no convincing argument for excluding non-State actors from the due diligence obligation.[197] Especially since the due diligence principle is particularly well suited for these types of situations.

Besides having to amount to an internationally wrongful act, the conduct also needs to affect a right of the target State. It is not enough that it is a harmful cyber operation. One example of this is when the cyber operation violates the sovereignty of the target State. Since non-State actors cannot generally affect a right of a State, it has to be determined if the non-State cyber operation would breach an obligation that the territorial State owes the target State had the territorial State been the one conducting the cyber operation in question. An example provided by the Tallinn Manual 2.0 is if a private company publishes highly classified documents of the target State online.[198] The due diligence principle will not be applicable to this case since no international law right of the target State is affected. Naturally, the territorial State should not have to prevent the acts of a private company, when it would not be in breach of international law had it published the documents itself. This is true even if the publishing of the documents produces serious adverse consequences for the target State.

4.5.3 Serious adverse consequences

While the ILC Articles of State Responsibility does not include any prerequisites about fault or harm, this is not the case for due diligence in the field of cyberspace. Similarly to environmental law, cyberspace is somewhat concerned with transboundary harm. The harm is, of course, rather different, but the aim is the same. Cyber operations could potentially harm vital infrastructures in our society, such as hospitals and governmental entities.[199] The due diligence principle includes a form of harm for it to be applicable. The Tallinn Manual 2.0 holds that the due diligence principle applies only in situations when the cyber operation affects the rights of, and produce serious adverse consequences for, other States. The criteria "serious adverse consequences" was included in Rule 6 by analogy from the content of the due diligence principle in international environmental

[197] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 36.
[198] Ibid.
[199] See for example Bannelier-Christakis p. 3.

law.[200] In the *Trail Smelter Arbitration* case, it was stated that it needed to be "of serious consequence", and the ICJ in *Pulp Mills* held that the conduct had to amount to "significant damage" for another State. The threshold of the damage is not evident, but it is clear from the case law presented above that just any damage is not enough. The International Group of Experts concluded that it is not enough if the cyber operation is, for example, simply causing inconvenience or minor disruption, i.e. it is not enough that the conduct produces negative effects for the target State.[201]

States also seem to be accepting this standard, albeit it is of course too soon to tell. The Netherlands stated in its letter that it is "generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences".[202] Furthermore, it held that the precise threshold depends on the circumstances in each case and that physical damage is not a requirement.[203] This is also in line with both the Tallinn Manual 2.0 and the flexibility of the principle. The International Group of Experts states a major impact on the economy as an example of serious adverse consequences which do not consist of physical damage.[204]

The Tallinn Manual 2.0 also presents a potential problem occurring when the threshold of serious adverse consequences is used. If a hacker group in State A uses botnets[205] that are placed in several States in order to conduct operations against State B, the cyber operation may cause serious adverse consequences for State B.[206] However, this does not mean that the bots in the territory of one of the States alone produce serious adverse consequences. The issue here is whether the territorial States are violating the due diligence principle if they do not act to terminate the use of their territories by the hacker group. The International Group of Experts were split on how to treat this issue. While a few suggested that it would be a violation, it was pointed out by the majority that such a view would put the due diligence obligation in the perspective of the target State, rather than the territorial States. Instead, they claimed that due diligence "derives from the

[200] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 37.
[201] Ibid.
[202] Minister of Foreign Affairs, Letter to parliament on the international legal order in cyberspace + Appendix: International law in cyberspace (26 September 2019) p. 5.
[203] Ibid.
[204] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 38.
[205] Definition of botnet according to the Glossary in Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 563 is a "network of compromised computers, so-called 'bots', remotely controlled by an intruder, 'the botherder', used to conduct coordinated cyber operations, such as 'distributed denial of service' operations".
[206] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 38.

sovereign prerogatives of the territorial State".[207] A consequence of following the minority's line could also be that States might be held responsible for the omissions of other States. Nonetheless, the International Group of Experts agreed that as long as the harm suffered by a State meets the relevant threshold, it does not matter where that harm manifests.[208]

4.5.4 Territory and cyber infrastructure

According to the Tallinn Manual 2.0, the due diligence principle is applicable for activities on the sovereign territory of the territorial State.[209] However, in two cases, the obligation may extend extraterritorially.[210] The first case is when a State has control over a territory abroad without exercising sovereignty over it, which may be the case during military occupation for example. The second case is when a State has control over government cyber infrastructure abroad. This could be, for example, "a national mission network on a military installation in a foreign country, cyber infrastructure aboard sovereign platforms on the high seas or in international airspace, and cyber infrastructure in diplomatic premises".[211]

The author of the cyber operation is not necessarily located in the State bound by the due diligence obligation. The Tallinn Manual 2.0 describes the following scenario:

> As an example, consider a hacker group located in State A that carries out a destructive cyber operation against State B using cyber infrastructure located in State C. If State C knows of said usage and fails to take feasible measures to put an end to the operation, it is in violation of the due diligence principle.[212]

In this case, State C is the territorial State of the due diligence obligation, since the cyber infrastructure is located in State C.

There was some discussion among the International Group of Experts whether the due diligence principle should apply to transit States or not.[213] A transit State is a State through which only data transits, e.g. through a fibre optic cable. Although hesitantly, they concluded that it did apply if the transit State had knowledge of the cyber operation, if

[207] Ibid.
[208] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 39.
[209] Ibid p. 32
[210] Ibid.
[211] Ibid p. 33.
[212] Ibid p. 32.
[213] Ibid p. 33.

the cyber operation reaches the relevant threshold of harm and the transit State is able to take feasible measures to effectively terminate the operation. Bannelier-Christakis adds to this and states that there is "no legal reason" that transit States do not have to abide by the due diligence obligation.[214] If a State has knowledge of a terrorist group that is going to cross its territory to attack a third State, the State has a duty to act and to prevent this attack. There is no reason that this should not be the case for illegal cyber attacks.[215] At the same time, however, it is unlikely that a transit State could be held responsible for violating the due diligence principle, mostly due to the rapidity of transit in cyberspace, but also because it would be extremely difficult to prove that the transit State had knowledge of these actions.[216] The International Group of Experts came to the same conclusion, even stating that it is unlikely that a transit State would even know of or be able to identify the cyber traffic transiting their cyber infrastructure.[217] However, if they do have the knowledge and the ability to prevent the cyber operation, they have an obligation to do so.

4.5.5 Knowledge

A State does generally not have an obligation to prevent harm if the State does not have *knowledge* of the situation which obliges action.[218] The ICJ in the *Corfu Channel* case made it clear that the obligation to notify shipping of the existence of mines was dependent on the State having obtained knowledge of that fact in sufficient time before the date when the vessels were struck by the mines.[219] It would not be reasonable to hold a State responsible for something it was not aware of. The Court further stated that "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known" about the circumstances.[220] In other words, States do not have an absolute knowledge of everything that is happening on their territory. However, it may be reasonable to ask of a State to "use best effort to gain knowledge of activity within its territory or jurisdiction".[221]

[214] Bannelier-Christakis p. 6.
[215] Ibid.
[216] Ibid.
[217] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 34.
[218] ILA Study Group, Second Report p. 12.
[219] *Corfu Channel* p. 22.
[220] Ibid p. 18.
[221] ILA Study Group, Second Report p. 12.

Whether it can be considered reasonable or not, however, does depend on the circumstances of each situation.

The Tallinn Manual 2.0 states that as soon as the territorial State has knowledge of the cyber operation, the State must take all reasonably available measures to stop that cyber operation.[222] The International Group of Experts stated that it is "a constitutive element in the application of this Rule".[223] There is nothing controversial about the due diligence applying for *actual knowledge*. The Tallinn Manual 2.0 gives an example of a State having actual knowledge when its intelligence agencies have detected a harmful cyber operation from within its territory or if the State has received credible information about such a cyber operation.[224] The main problem here is, of course, proving that the State had such knowledge.

A more difficult question is whether due diligence is applicable also in cases of *constructive knowledge*, i.e. when States should have known about a cyber operation. The International Group of Experts concluded that the rule includes constructive knowledge.[225] This means that if the State did not know about the cyber operation in question, but objectively *should have known* about it, the due diligence obligation still applies. Turning to case law, it seems to agree that the principle would be applicable to certain cases of constructive knowledge. The ICJ in the *Corfu Channel* case clearly stated that Albania "ought to or should have known".[226] This definitely seems to include constructive knowledge in the due diligence principle.

Determining whether the State should have known about the cyber operation is another issue. On this point, the International Group of Experts stated that there is a range of factors at play.[227] For example, they held that it is more likely that the State will meet the "should have known" standard if the State's governmental cyber infrastructure is being used, rather than if a private infrastructure is being used.[228] Likewise, if the cyber operation is of the type that is generally always detected, it is easier to ascribe the State to have had constructive knowledge.[229] The International Group of Experts were very clear, however, that in some cases, especially concerning more difficult cyber operations,

[222] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 43.
[223] Ibid p. 40.
[224] Ibid.
[225] Ibid p. 41.
[226] *Corfu Channel* p. 18.
[227] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 41.
[228] Ibid.
[229] Ibid.

it might be unreasonable to expect the State to have known about it.[230] Once again, the principle shows that it is not being unreasonable in what is required of States.

4.5.6 Reasonableness and the flexibility of the due diligence principle

In the introduction to this chapter, it was stated that the due diligence principle does not impose an unreasonable burden on States. This has already been made clear from the way it is defined and the content of the principle. However, it deserves to be highlighted that it is a principle of reasonableness and flexibility. In fact, due diligence is often described as providing a "reasonable" standard of conduct.[231] It is a flexible concept, and it only prescribes that States act in a duly diligent manner. It does not care about the end result. It is an obligation of conduct, not of result.[232] This is not uncommon for international law since it tends to focus on the behavior of States instead of the outcomes of their behavior.[233] The obligation simply means that a State is required to take all measures it could reasonably be expected to take. This is in line with the due diligence principle in environmental law as well, as the Commentary to the Draft Articles on Transboundary Harm, for example, conclude that States do not need to do more than what is possible. It has further become clear from the examination of the principle in environmental law that the principle is easily adapted and that it depends on the context what is required of States.

What is reasonable is undoubtedly difficult to determine, but it is safe to say that the due diligence principle suggests that States have different obligations depending on the circumstances, including the level of (economic) development of a State. It should also imply that States have much discretion in choosing the means to prevent the cyber operation. Other factors that may be important for the test of reasonableness are, for example, control over territory, the degree of the risk and the existence (or absence) of bona fide acts.[234] The ICJ's judgment in the *Tehran Hostages* case further supports that States only have to take appropriate steps to prevent harm of a third State if it has "the means at [its] disposal to perform [its] obligations".[235] Additionally, it is clear already from the Commentary to the ILC Articles on State Responsibility that obligations of prevention, which due diligence must count as, "are usually construed as best efforts

[230] Ibid.
[231] See for example the ILA Study Group, Second Report p. 8.
[232] Bannelier-Christakis p. 11.
[233] ILA Study Group, Second Report p. 2.
[234] ILA Study Group, Second Report p. 47.
[235] *United States Diplomatic and Consular Staff in Tehran*, Judgment, ICJ Reports 1980, p. 3, para. 68.

obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur".[236]

Another way of expressing the reasonableness standard is to understand it as a requirement of conduct which would be the standard by any reasonable State in the prevailing circumstances.[237] Although the standard of reasonableness does not have any clear content or criteria, general guidelines from other areas of international law, such as international environmental law, can be used to establish the scope of the principle.

The Tallinn Manual 2.0 also includes reasonableness throughout their commentary on Rule 6. For example, the International Group of Experts states that "[i]f it is unreasonable to expect the territorial State to have known of the operation in the attendant circumstances and to have been able to terminate it, this Rule will not have been breached".[238] The reasonableness is further elaborated on in Rule 7 about compliance with the due diligence principle, which states that

> [t]he principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.[239]

Rule 7 clarifies that the territorial State must take all reasonably available measures in order to prevent or stop the attack.

The ILA Study Group on Due Diligence also expressed that "it is well-established that developing States may not be able to control the activities in their territory in a similar manner to developed States, and that this will affect the evaluation of whether they have breached their due diligence obligation".[240] Developing States may therefore be permitted to use less diligence than developed States. It is clear that the capabilities of a State are taken into consideration when applying the due diligence principle.

Naturally, the flexibility and the lack of definitions is also combined with problems. Reasonableness involves a standard for the measures taken related to what could be expected of a State. It is difficult to define what is reasonable and to set up requirements of what is expected of States. Nonetheless, it can be concluded that due diligence will not become an unreasonable burden for States.

---

[236] ILC articles on State Responsibility p. 62.
[237] Geiss & Lahmann p. 653.
[238] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 41.
[239] Ibid p. 43.
[240] ILA Study Group, First Report p. 27.

4.5.7 The measures adopted

Another question is what exactly States need to do in order to fulfil their due diligence obligation. Since this is an area still in development, there is no clear answer to this question. Due diligence seeks to answer the question of whether States have taken reasonable measures to prevent the injury to other States.[241] A State will not be said to have violated the due diligence principle simply by not adopting legislation or protecting its cyber infrastructure. It has already been stated that due diligence necessitates some sort of harm. Article 14(3) of the ILC Articles on State Responsibility state that "[t]he breach of an international obligation requiring a State to prevent a given event occurs when the event occurs". Similarly, if a State has knowledge of a cyber operation, and the means to stop it, but chooses not to, it will still not be in breach of its due diligence obligation if the cyber operation does not cause serious adverse consequences for another State. The fact that the territorial State did not take any measures does not matter if there are no consequences.

The ILA study group on due diligence generally stated that the degree of due diligence varies depending on the primary rule in question.[242] It is yet to be ascertained the degree of due diligence in relation to cyber operations. Nonetheless, a few things can be, and have already been, said regarding the scope of the principle. For example, there seems to be an evolving consensus amid scholars and State legal advisers that there is no obligation of States to monitor cyber activities on their territory or to prevent the wrongful use of their cyber infrastructure.[243] The International Group of Experts concluded that the due diligence principle does not include an obligation to prevent and therefore there is no obligation for States to monitor cyber activities on their territory.[244] However, this is not undisputed. Bannelier-Christakis concluded, on the contrary, that due diligence does imply "not only an obligation *to react* but also *to prevent*".[245] Here it is worth pointing to the *Alabama* case, where the Tribunal found that "[t]he British government failed to use due diligence in the performance of its neutral obligations; and especially that it omitted, notwithstanding the warnings and official representations made by the diplomatic agents

[241] ILA Study Group, Second Report p. 3.
[242] Ibid p. 20.
[243] Schmitt, *In Defense of Due Diligence in Cyberspace* p. 75.
[244] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 42.
[245] Bannelier-Christakis p. 8.

of the United States […], to take in due time any effective *measures of prevention*, and that those orders which it did give at last, for the detention of the vessel, were issued so late that their execution was not practicable".[246] The ICJ, in the *Corfu Channel* case, further held that "nothing was attempted by the Albanian authorities to *prevent* the disaster. These grave omissions involve the international responsibility of Albania".[247] The ICJ stated that Albania neither notified the existence of the minefield, nor warned the British warships of the danger they were approaching, even though they had knowledge of it. In the latter case of *Armed Activities on the Territory of the Congo*, the ICJ stated that Uganda was responsible "for any lack of vigilance *preventing* violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account".[248] Simply notifying the target State may not always be enough. According to the Tallinn Manual 2.0, States are required to use all means at its disposal to *terminate* the activity.[249]

Some further comments can be made about what the due diligence obligation in cyberspace includes. The due diligence principle does not make a difference between a situation in peacetime and during conflict. However, the due diligence requirements expected of States during peacetime, may "become more difficult to meet during conflict".[250] There are also other rules that will come into play.[251] The standard of due diligence continues to apply, nonetheless.

Furthermore, the due diligence obligation is only concerned with ongoing operations.[252] The duty to apply due diligence expires when the cyber operation is complete. That is, unless the cyber operation is likely to be repeated.[253]

Environmental law can also be used as a comparison here. In Chapter 4.3, the due diligence principle in the more developed area of environmental law was shown to require certain specific measures in some circumstances. For example, in *Pulp Mills*, it was

[246] *Alabama claims of the United States of America against Great Britain*, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Volume XXIX, pp. 125-134, p. 130. [emphasis added].
[247] *Corfu Channel* p. 23. [emphasis added].
[248] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, ICJ Reports 2005, p. 168, para. 179. [emphasis added].
[249] See for example Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 34.
[250] ILA Study Group, First Report p. 11.
[251] For example Rule 153 in Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 560 about response by parties to the conflict to violations.
[252] Schmitt, *In Defense of Due Diligence in Cyberspace* p. 75.
[253] Ibid.

established that it might be necessary to do an EIA, the use of which was later further developed in *Certain Activities Carried out by Nicaragua*. In the *Seabed Mining Advisory Opinion*, the Seabed Disputes Chamber stated that due diligence is a variable concept and that it may change over time, for example due to new scientific or technological knowledge. Cyberspace is an entire new technological area, and from what has been described of the principle above, it is only logical that the principle needs to be adapted to fit into this area of international law. It may be possible to imagine that the due diligence principle in cyberspace would also include some sort of "EIA", that is, a method of assessing the risk of harm caused by a cyber operation, and that, if such a risk is confirmed, there will be a need to notify and consult the State that may be affected. Indeed, some authors argue that States should be required to conduct a cyber impact assessment.[254] However, such an assessment may be more difficult than an EIA, since the operations generally occur with more rapidity than in the environmental area. What is required of States, therefore, necessarily differs from what the due diligence principle requires of States when there is a risk of environmental transboundary harm. While environmental law serves as a good comparison, it cannot guide us completely in what the content of the due diligence principle will be.

It is important to point out as well, that due diligence is not a static principle – it may ultimately evolve into something more demanding of States.[255] As cyberspace develops, and regulation and State practice with it, it will become more clear what States are required to do.

4.5.8 Conclusion

It has been suggested that "the standard of due diligence [is] a useful yardstick by which to hold all States (to varying degrees) to a minimum standard of conduct" and that this is especially true for new global challenges and new areas of transnational regulation.[256] Cyberspace is undeniably included in this.

In conclusion, it need not be a concern that due diligence is an unreasonable burden for States. The obligation varies depending on the context and the level of development of the State. Due diligence must be seen in the light of the capabilities of the States

[254] Stockburger p. 248.
[255] ILA Study Group, Second Report p. 47.
[256] Ibid.

concerned and these capabilities will be taken into account when determining whether a State has breached the due diligence obligation or not. If a burden put on a State is deemed to be unreasonable, it will simply not be considered a breach of the due diligence obligation.

Furthermore, the principle of due diligence is not a new concept. It is well established customary law and the issue here is simply to understand the shape and form of the principle in relation to cyber operations. In my opinion, the Tallinn Manual 2.0 is a great addition to the doctrine of due diligence in cyberspace. The International Group of Experts' arguments are well-founded, and it greatly follows the case law and seems to be in line with the few existing statements about due diligence in cyberspace. Although Rule 6 is necessarily kept general, it is a start to shaping the due diligence principle in the field of cyberspace.

4.6 Expanding the scope of due diligence in cyberspace

While there is reason to keep the due diligence obligation to a minimum, at least for now, some authors consider the scope too narrow to make a difference. For example, Stockburger argues that a preventive feature should be included in the due diligence obligation.[257] By using the precautionary approach, it would help the due diligence principle to crystallize and it would encourage adherence to the principle.[258] He also argues for a cyber impact assessment to determine if the State's actions would potentially affect the rights and interests of another State.[259] At the same time, he states that this is not customary international law at this moment in time, but that it is his argument of *lex ferenda*.[260]

The fear is also that if the principle is too general, it will not be useful and therefore considered redundant. The principle needs to be given content in order to effectively be used to hold States responsible for cyber operations emanating from their territory.

Due diligence could be expanded in several ways, provided that the States agree to it. For example, the World Health Organization in Article 6(1) of its 2005 *International Health Regulations*[261] imposes the duty on Member States to notify the organization "of all events which may constitute a public health emergency of international concern within

[257] Stockburger p. 257.
[258] Ibid p. 260.
[259] Ibid p. 257. See also above in Chapter 4.5.7.
[260] Ibid p. 260.
[261] World Health Assembly, *International Health Regulations*. Geneva, World Health Organization (2005).

[their territories]". This sort of system could be used in the cyber context, which would be more of an obligation to prevent rather than repress. However, at this point in time, there is rather wide skepticism against pure preventive measures. Although the obligation itself would not pose a huge burden on States, the possibility of States agreeing on these types of obligations seems unlikely at the moment, considering for example that it was not too long ago that certain States for the first time acknowledged that international law applies to cyberspace. Expanding the scope of due diligence in cyberspace is rather a question for the future.

5 Countermeasures

5.1 Countermeasures in cyberspace

As explained in Chapter 3.5, countermeasures are a way for injured States to induce a State responsible for an internationally wrongful act to comply with its legal obligations. The use of countermeasures in response to a cyber operation has been regulated in the Tallinn Manual 2.0.

Rule 20 in the Tallinn Manual 2.0 lays out the general principle of countermeasures in cyberspace.[262] It holds that a State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State. Rule 21 states that the purpose of countermeasures is to induce a responsible State to comply with the legal obligations it owes an injured State and Rule 22 lays down the limitations on countermeasures.[263] According to Rule 23, countermeasures must be proportionate to the injury to which they respond.[264] The regulation in the Tallinn Manual 2.0 greatly follows the ILC Articles on State Responsibility and the case law of the ICJ.

Although some difficulties, which arise with attribution and countermeasures, are avoided when applying the due diligence principle instead, the use of countermeasures is not completely uncomplicated in relation to due diligence. The injured State still needs to prove, with clear and convincing evidence, that the attack originated from the territory of the territorial State, and that the State in question failed its due diligence obligation. Granted, it is easier to simply establish the territory from where the cyber operation emanated than to additionally have to establish the person or group behind the attack. However, it is still not a simple task. For example, it also needs to be ascertained whether the territorial State had knowledge of the harmful cyber operation or not. It is necessary to trace back the malicious data to establish the territorial link to the State "to a convincing degree".[265] The risk of incorrectly identifying the source of the cyber operations is relatively high.[266]

[262] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 111.
[263] Ibid p. 116 and 122.
[264] Ibid p. 127.
[265] Geiss & Lahmann p. 637.
[266] Ibid.

5.2 The scope of countermeasures in cyberspace

The *Gabcikovo-Nagymaros Project* case conditions still apply and are reflected in the Tallinn Manual 2.0. It is possible, however, in some situations, to aim the countermeasures at a private entity, and not only at States.[267] The Tallinn Manual 2.0 provides an example of a situation where countermeasures would be justified in a due diligence situation where the target is a private entity.[268] Suppose that a private firm in State A is engaging in harmful cyber operations against a competitor in State B. In this case, State B can use countermeasures against the firm *if* State A has wrongfully failed to control the activities of the firm, thereby breaching its due diligence obligation to control its territory once it became aware of the operations, according to Rule 6 and 7 in the Tallinn Manual 2.0.[269]

Not fulfilling its due diligence obligation constitutes an internationally wrongful omission by a State. It is important to remember that the injured State taking countermeasures based on that breach must be aware of the proportionality in its response. The countermeasure must be proportionate to the responsible State's omission, not to the severity and consequences of the cyber operations.[270]

This way of targeting private entities instead of States is somewhat rare in the international context. Generally in international law, States are not allowed to take measures against non-State actors. Self-defense and countermeasures only apply in relation to other States. However, the due diligence principle slightly "side-steps" that fact. Technically, the countermeasure will be against the State which failed its due diligence obligations, but in reality, the measure will be taken against the non-State actor, since that is how the targeted State will be able to defend itself.

As has been made clear by Rule 20 in the Tallinn Manual 2.0, the countermeasures can be either cyber countermeasures or non-cyber countermeasures, i.e. it need not be in kind.

It is also worth mentioning that, at the time of writing, there are no known uses of countermeasures, within the meaning of the term in the State responsibility framework, in the field of cyberspace. [271] State practice and *opinio juris* is therefore hard to come by. In its declaration in 2019, France stated that the consequences of a violation of the due diligence obligation may be political or diplomatic action, for example, the use of

[267] Schmitt, *In Defense of Due Diligence in Cyberspace* p. 77.
[268] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* p. 113.
[269] Ibid.
[270] Ibid p. 130.
[271] NATO CCD COE, *Trends in international law for cyberspace* (May 2019) at 2(b).

countermeasures.[272] At the same time, France made it clear that only non-forcible countermeasures are allowed and that the failure of a State to fulfill the due diligence obligation does not justify an exception from the prohibition of the use of force.[273] It is yet to be seen what other States believe to the be the law of countermeasures in cyberspace.

[272] Roguski.
[273] Roguski.

6 Conclusion

6.1 Some summarizing comments about due diligence in cyberspace

The purpose of this study was to examine whether the obligation of States to not allow knowingly its territory to be used for acts contrary to the rights of other States applies to activities conducted in cyberspace. The due diligence principle, as formulated in Rule 6 of the Tallinn Manual 2.0, was assessed in order to do this.

It has been stated in this examination that international law generally applies in the same way in relation to cyber operations as to traditional armed operations. Cyber operations, however, create difficulties for State responsibility, especially because of the anonymity of the attacks. It is therefore extremely difficult to attribute cyber operations to States.

Due diligence creates a special way of holding States responsible, without an act having to be attributed to the State. Instead, the due diligence principle affirms that States have a responsibility to ensure that their territory is not being used for harmful international activities which affect the rights of, and produce serious adverse consequences for, other States. This general responsibility creates a lower threshold than attribution and can be used also when the operator of a cyber operation is a non-State actor.

The main question of this study is whether the due diligence principle can be considered applicable in cyberspace. It has been concluded that the principle undoubtedly holds a status as an international customary rule. This has been confirmed both by case law, doctrine and a number of treaties. It is presumed in international law, that a principle, which has been established as a general principle of international law, is applicable to all areas of international law unless the contrary has been proved. Consequently, the general principle of due diligence must be considered applicable to cyberspace. That is the thesis of the Tallinn Manual 2.0, which I agree with. There is no State practice or *opinio juris*, or at least not sufficient State practice or *opinio juris*, to show that the principle does not apply. Unless State practice or *opinio juris* excludes it, the due diligence principle applies.

States may not have rejected the applicability of due diligence in cyberspace, but neither have they affirmed it. There are only a few statements available about due diligence. The ones that do mention it tend to confirm its applicability. Nonetheless, the statements are so few that it is not possible at this time to draw any conclusions about

State practice or *opinio juris*. As stated, State practice must be widespread and consistent in order to establish a customary rule of international law. While the statements seem to be positive about the applicability of due diligence, the UN GGE have been a bit more reluctant to include it. This suggests that States were not able to agree on the due diligence obligation. While the conclusion at this time is that the principle is applicable to cyberspace, that may change if State practice and *opinio juris* develops in a different way.

Furthermore, it is not enough to conclude that the principle is applicable. Since the principle is of a general character, it must be specified how it works in relation to cyber operations. The Tallinn Manual 2.0 has made a great attempt at clarifying this, but as has been stated before in this study, the manual does not hold status of a binding legal source. Additionally, the principle in the manual is still very general and the commentary only slightly manages to clarify the scope of the principle. Nonetheless, it has been established by the Tallinn Manual 2.0 that the territorial State needs to have knowledge of the malicious cyber operation and that the operation must be an international wrongful act, must affect a right of the target State and produce serious adverse consequences for the State. At the same time, there are issues which the International Group of Expert could not agree on. The Tallinn Manual 2.0 lay the groundwork for the scope of the due diligence principle, but there are still problems to solve.

Further regulation is therefore necessary, and it must be established what the scope of the principle is, in order for it to be a valuable tool in the fight against malicious cyber operations. States need to come together to solve the issues in this emerging field of international law. Harmonization and regulation are important both for the efficiency of the due diligence principle, but also as a way to ensure that there is a fair balance between different interests. Harmful cyber operations will only increase in numbers unless the problem of unclear and unrealistic attribution requirements is solved. It is also necessary with a regulation of countermeasures which is compatible with cyber operations.

6.2 As we look to the future…

The UN General Assembly once again, in December 2018, requested the Secretary-General to establish a group of governmental experts to continue to study, *inter alia*, how international law applies to the use of information and communications technologies by

States, and to submit a report on the results of the study.[274] The new UN GGE already had a substantive session on 9-13 December 2019 and released a collated summaries of their regional consultations.[275] From the summary, it can be noted that some States suggested that due diligence should be brought up and looked into, particularly "where actions within one State's territory affect the rights of other States".[276] Furthermore, the UN GGE provided that the Tallinn Manual 2.0 offered an academic perspective on the applicability of international law, but that more work was needed in this field.[277] The UN GGE is due to submit its final report to the General Assembly in 2021.[278]

The UN General Assembly also decided to convene an open-ended working group with the applicability of international law on its agenda.[279] The working group convened for the first time in 2019 and operates on a consensus basis.[280] Due diligence in cyberspace is a current issue and the trend is indeed that it is being more and more included in the work of the UN and that States are starting to express their views on the obligation. Hopefully, by these initiatives, States will be able to further clarify their views on the due diligence principle in cyberspace.

[274] A/RES/73/266, *Advancing responsible State behaviour in cyberspace in the context of international security* (22 December 2018) p. 3 para. 3.
[275] United Nations, *Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (9-13 December 2019).
[276] Ibid p. 8.
[277] Ibid p. 7.
[278] A/RES/73/266 p. 3 para. 3.
[279] A/RES/73/27, *Developments in the field of information and telecommunications in the context of international security* (5 December 2018) para. 5.
[280] Ibid.

Sources

Bibliography

Arias, G.J., *Are the rules for the right to self-defense outdated to address current conflicts like attacks from non-state actors and cyber-attacks?*, Revista Tribuna Internacional, Volume 6, Issue 11 (2017).

Banks, W, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0.*, Texas Law Review, Volume 95, Issue 7 (June, 2017) pp. 1487-1514.

Bannelier-Christakis, K, *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, Baltic Yearbook of International Law, Vol. 14 (2014).

Barlow, J, *A Declaration of Independence for Cyberspace*, (Davos, 1996), accessed 24 November 2019. Available at: https://www.eff.org/sv/cyberspace-independence.

Buchan, R, *Non-State Actors and the Obligation to Prevent Transboundary Harm*, Journal of Conflict and Security Law, Volume 21, Issue 3 (Winter, 2016), pp. 429-453.

Chircop, L, *A Due Diligence Standard of Attribution in Cyberspace*, International and Comparative Law Quarterly, Volume 67, Issue 3 (2018) pp. 643-668.

Crawford, J, *State Responsibility: The General Part* (Cambridge Studies in international and comparative law), Cambridge University Press (2013).

Crawford, J & Olleson, S, *The character and forms of international responsibility*. In Evans, M, *International law*, Oxford University Press, 5th edition (2018).

Efrony, D & Shany, Y, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, The American Journal of International Law, Volume 112, Issue 4 (2018) pp. 583-657.

Geiss, R & Lahmann, H, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention* (January 2014) pp. 621-657. In Ziolkowski, K, Peacetime Regime for State Activities in in Cyberspace, International Law, International Relations and Diplomacy (Tallinn 2013).

Hankinson, O, *Due Diligence and the Gray Zones of International Cyberspace Laws*, Michigan Journal of International Law, Volume 39 (2017), accessed 23 March 2020. Available at: http://www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/#_ftn16.

Hessbruegge, J.A, *The historical development of the doctrines of attribution and due diligence in international law*, New York University Journal of International Law and Politics, Volume 36, Issue 2-3 (2004) pp. 265-306.

Hjertstedt, M, *Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt*. In Mannelqvist, R, Ingmanson, S, & Ulander-Wänman, C (eds.), Festskrift till Örjan Edström, Juridiska institutionen, Umeå universitet (2019) pp. 165-173.

Klimburg, A (ed.), *National Cyber Security Framework Manual*, NATO CCD COE (2012).

Koivurova, T, *Due Diligence*, Oxford Public International Law, Max Planck Encyclopedia of Public International Law (February 2010).

Lehrberg, B, *Praktisk juridik metod*, Iusté, 11th edition (2019).

Miller, R.A, *Trail Smelter Arbitration*, Oxford Public International Law, Max Planck Encyclopedias of Public International Law (May 2007).

Roscini, M, *Cyber operations and the use of force in international law*, Oxford University Press, 1st edition (2014).

Roguski, P, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*, Opinio Juris (24 September 2019), accessed on 6 March 2020.

Schmitt, M, *In Defense of Due Diligence in Cyberspace*, 125 Yale Law Journal Forum 68 (June 2015) pp. 68-81.

Schmitt, M (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge, Cambridge University Press (2017).

Shaw, M, *International law*, Cambridge University Press, 7th edition (2014).

Stockburger, P, *From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace*, in Minárik, T, Jakschis, R & Lindström, L (eds.), 10th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn (2018).

Tsagourias, N, *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Volume 17, Issue 2 (2012) pp. 229-244.

Tsagourias, N, *The legal status of cyberspace*, in Research Handbook on International Law and Cyberspace (2015), pp. 13-29.

Voitasec, D, *Applying international humanitarian law to cyber-attacks*, Lex ET Scientia International Journal, Volume 22, Issue 1 (2015), pp. 124-131.

Von Heinegg, W, *Legal implications of Territorial Sovereignty in Cyberspace*, In 2012 4th International Conference on Cyber Conflicts, Czosseck, C, Ottis, R, & Ziolkowski, KK (Eds.), NATO CCD COE Publications (Tallinn, 2012).

Väljataga, A, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*, INCYDER NEWS (Sept. 1, 2017), accessed 11 February 2020. Available at: https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

Väljataga, A, *Tracing* opinio juris *in National Cyber Security Strategy Documents*, NATO CCD COE (Tallinn, 2018).

Table of Treaties and Other Instruments

International Law Commission, *Draft articles on Prevention on Transboundary Harm from Hazardous Activities, with commentaries*, Yearbook of the International Law Commission, Volume II, Part Two (2001).

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, Yearbook of the International Law Commission, Volume II, Part Two (2001).

International Law Commission, *Draft Conclusions on Identification of Customary International Law*, Yearbook of the International Law Commission, Volume II, Part Two (2019).

United Nations, *Charter of the United Nations*, 1945, 1 UNTS XVI.

United Nations, *Vienna Convention on the Law of Treaties*, Treaty Series, Volume 1155 (1969) p. 331.

United Nations, *Statute of the International Court of Justice* (18 April 1946).

United Nations General Assembly, *Convention on the Law of the Sea* (10 December 1982).

World Health Assembly, *International Health Regulations*. Geneva, World Health Organization (2005).

Table of Cases

International Court of Justice

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, ICJ Reports 2007, p. 43.

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

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

Continental Shelf (Libyan Arab Jamahiriya/Malta), Judgment, ICJ Reports 1985, p. 13.

Corfu Channel case, Judgment of April 9th, 1949: ICJ Reports 1949, p. 4.

Gabcikovo-Nagymaros Project (Hungary/Slovakia), Judgment, ICJ Reports 1997, p. 7.

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

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

North Sea Continental Shelf cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. The Netherlands, Judgment, ICJ Reports 1969, p. 3 (20 February 1969).

Pulp Mills on the River Uruguay (Argentina v. Uruguay), ICJ Reports 2010, p. 14.

United States Diplomatic and Consular Staff in Tehran, Judgment, ICJ Reports 1980, p. 3.

Permanent Court of International Justice

SS Lotus (France v. Turkey), 1927 PCIJ (Ser. A), No 10.

International Tribunal on the Law of the Sea

Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports 2011, p. 10.

Other cases

Alabama claims of the United States of America against Great Britain, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Volume XXIX, pp. 125-134.

Final Award – Ethiopia's Damages Claims between the Federal Democratic Republic of Ethiopia and the State of Eritrea, Eritrea-Ethiopia Claims Commission (17 August 2009).

Island of Palmas Case (or Miangas), United States v. Netherlands, Award, II RIAA 829, ICGJ 392 (PCA 1928), Permanent Court of Arbitration (4 April 1928).

Rainbow Warrior Case, (New Zealand v. France) 82 I.L.R. 500 (1990).

Trail Smelter Arbitration, United States v. Canada, 3 UNRIAA 1905 (1938 and 1941).

Other sources

International Law Association

International Law Association, *Study Group on Due Diligence in International Law*, First Report (7 March 2014).

International Law Association, *Study Group on Due Diligence in International Law*, Second Report (July 2016).

UN Security Council Resolutions

S/RES/1267 (15 October 1999).

S/RES/1333 (19 December 2000).

UN General Assembly Resolutions

A/RES/55/63, *Combating the criminal misuse of information technologies* (4 December 2000).

A/RES/56/83, *Responsibility of States for internationally wrongful acts* (12 December 2001).

A/RES/58/32, *Developments in the field of information and telecommunications in the context of international security* (8 December 2003).

A/RES/70/237, *Developments in the field of information and telecommunications in the context of international security* (23 December 2015).

A/RES/73/27, *Developments in the field of information and telecommunications in the context of international security* (5 December 2018).

A/RES/73/266, *Advancing responsible State behaviour in cyberspace in the context of international security* (22 December 2018).

UN GGE

A/68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 June 2013).

A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (22 July 2015).

United Nations, *Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (9-13 December 2019).

NATO CCD COE

NATO CCD COE, *Trends in international law for cyberspace* (May 2019).

European Law

Commission (EC) and High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (joint communication) JOIN(2013) 1 final (7 February 2013).

Council of Europe Convention on preventing and combating violence against women and domestic violence, CETS No. 210 (11 May 2011).

National statements and other national sources

Australia, *Cyber Security Strategy* (2009). Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

Austria, *Austrian Cyber Security Strategy* (2013). Available at: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

Minister of Foreign Affairs of the Netherlands, *Letter to parliament on the international legal order in cyberspace + Appendix: International law in cyberspace* (26 September 2019).

The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, 2011).

United States of America, *National Initiative for Cybersecurity Careers and Studies Explore Terms: A Glossary of Common Cybersecurity Terminology* (28 November 2018), accessed 24 March 2020. Available at: https://niccs.us-cert.gov/about-niccs/glossary#I.