Evidentiary Challenges in Establishing State Responsibility for Malicious Cyber Operations

Research Proposal – Doctoral Thesis

Doctoral Candidate: Mag. Isabella Brunner, BA
University: Universität Wien
Student ID: 01004941
Research Field: Public International Law
Seminar: 380034 „SE DissertantInnenseminar: Aktuelle Themen des internationalen Rechts“

Table of Contents

1. Introduction

The Internet has brought many advantages. It enabled the communication between individuals across the globe and consequently led to a largely inter-connected world. States have also realised this potential and integrated the Internet into their daily work.

However, the Internet also offers multiple ways to wreak havoc. And States have started to take advantage of that as well.[1] Past experience has shown that anything might be possible through cyber means – including the temporary deactivation of a large Iranian nuclear plant, allegedly executed by two powerful States (the so-called *Stuxnet* incident), or even a cyber operation against a power grid, plunging part of Ukraine into the dark for several hours.[2] Next to being significant incidents with precarious consequences, at least Iran did not officially blame anyone for these acts.[3] Cyberspace has, despite being a useful connectivity tool, thus developed into a powerful weapon, as it allows States and non-State actors to cause 'digital chaos' in the real (physical) world without revealing who is behind it: Although attributing an act to a certain person, entity or State is already difficult in the traditional realm, cyberspace offers even more sophisticated ways of hiding one's identity. This includes the possibility of IP address spoofing (to fake the origins of the cyber operation),[4] false-flag operations,[5] the use of botnets or multi-stage operations.[6] As a consequence, the actual attribution of an act in the cyber context to

[1] According to the Council Foreign Relations Cyber Operations Tracker, 25 States are suspected of having sponsored cyber operations, see <www.cfr.org/interactive/cyber-operations#Takeaways> (all online references are accurate as of 5 November 2019).

[2] On Stuxnet generally see i.a. Heather H Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 37 f; on the takeout of the Ukrainian power grid, see Michael McElfresh, 'Cyberattack on Ukraine Grid: Here's How It Worked and Perhaps Why It Was Done' (*The Conversation*, 18 January 2016) <http://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802>; see also David E Sanger, 'Utilities Cautioned About Potential for a Cyberattack' *The New York Times* (New York, 29 February 2016) <http://nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?auth=login-email&login=email>.

[3] Then-President Ahmadinejad merely stated that the malicious 'Stuxnet' worm was installed by 'western enemies', see Dinniss (n 2) 129.

[4] According to Cloudfare, IP spoofing 'is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both', see 'What is IP Spoofing?' (*Cloudfare*) <www.cloudflare.com/learning/ddos/glossary/ip-spoofing/>.

[5] See e.g. Kaspersky Team, 'Olympic Destroyer: Who Hacked the Olympics?' (*Kaspersky Daily,* 9 March 2018) <www.kaspersky.com/blog/olympic-destroyer/21494/>, on how Kaspersky first suspected a North Korean hacking group called 'Lazarus Group' due to the existence of several 'digital fingerprints' pointing at it, but then discovered material that pointed to a different actor, namely the Russian hacking group 'Sofacy', leading to the conclusion that there is never a one-hundred percent certainty about who is behind a cyber operation.

[6] So-called 'multi-stage attacks' are 'attacks, where the attacker infiltrates one computer to use as a platform to attack a second, and so on'; see David D Clark and Susan Landau, 'Untangling Attribution' (2011) 2 Harvard National Security Journal 323, 325.

establish State responsibility is significantly difficult.[7] This, in turn, facilitates the evasion of international responsibility.[8]

For example, in the face of a cyber operation reaching the severity of an armed attack as referred to in Article 51 UN Charter,[9] a lack of attribution inhibits the injured State to defend itself, as it does not know who is behind the attack and is thus not able to cease the wrongful conduct.[10] Moreover, the burden of proving that the injured State has the right to self-defence according to Article 51 UN Charter rests, in general, on the injured State.[11] Thus, if the process of attributing the attack takes longer than the attack lasts, self-defensive measures might be rendered obsolete, or regarded as unlawful reprisals instead if exercised anyway.[12]

The same is true for taking countermeasures: As countermeasures are only intended to induce the wrongful State to cease its wrongful conduct,[13] a belated reaction could very easily be seen as an unlawful retaliation.[14] Next to these examples, establishing attribution is also important to enable the imposition of other legal consequences on the State conducting the cyber operation, such as asking for reparation for the wrongful conduct.[15]

This raises the question, whether the conventional rules of international law, in particular evidentiary rules, are sufficient to deal with these new methods of conflict, or whether there is a need for additional regulation.

2. The Application of International Law to Cyber Operations

In general, the common understanding amongst academics and States is that international law applies to the new domain of cyberspace.[16] The argument is that it is still possible to apply the

[7] Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50 Texas International Law Journal 233, 234; William Banks, 'Who Did It? Attribution of Cyber Intrusions and the Jus in Bello', in Ronald T Alcala and Eric T Jensen, *The Impact of Emerging Technologies on the Law of Armed Conflict* (OUP 2019) 16; John P Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats' (2016) 7 Harvard National Security Journal 391, 409; Clark and Landau (n 6) 329, regarding DDoS attacks: 'If the actual attack involved falsified source addresses, [a] trace-back may be very difficult or even impossible'.

[8] Cf. Banks (n 7) 7: 'There can be no state responsibility for internationally wrongful acts until those acts have been attributed to a state'.

[9] Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Article 51.

[10] See, in particular, Dinniss (n 2) 101: 'The difficulty of attribution also affects the victim state's ability to engage in forcible countermeasures in self-defence'; Yoram Dinstein, 'Computer Network Attacks and Self-Defence' in Michael Schmitt et al (eds), *Computer Network Attack and International Law* (Naval War College 1999) 111.

[11] *Case Concerning Oil Platforms (Iran v United States)* (Merits) [2003] ICJ Rep 161, paras. 57 and 61; see also Dinstein (n 10) 111.

[12] See, *inter alia*, Dinniss (n 2) 102.

[13] See UN ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) GAOR 56th Session Supp. 10, 43 (Commentary to Article 49, para. 1) 130.

[14] See Article 49 para. 2 ILC Articles, which notes that '[c]ountermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State'. The phrase 'for the time being' indicates the temporary character of the countermeasure, which cannot be taken when the wrongful State has resumed its obligations; see ILC Articles Commentary (n 13) 129 ff (Article 49).

[15] See Part Two ILC Articles.

[16] See i.a. Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 29, which, without any doubt, finds the ILC Articles to be applicable in the cyber context; Michael Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 3; see, however, to the contrary Banks (n 7) 24: 'To date, state practice on intervention is based on kinetic examples; the analogy to cyber may not be persuasive'; see also, regarding the law of armed conflict, thus not

conventional rules to an inter-State cyber conflict, as the actors behind a cyber operation are always acting in physical space.[17] Also, there is no Internet without the necessary hardware behind it.[18] Lastly, it would be better to apply the legal framework that already exists, rather than have a *lacuna* in the law.[19]

However, some scholars as well as States have pointed out that the peculiarities of cyberspace – including the additional difficulties of tracing back the attacks – may require a new set of international rules.[20] However, most States have remained reluctant to publicly provide their opinion on how international law applies to the cyber context, let alone what evidentiary standards would be necessary when conducting an attribution. Either they do not publicly attribute at all, despite having become victim to a harmful cyber operation[21], or they do publicly attribute, but rarely specify their attribution based on international law and the evidence they rely on. This is, perhaps, because States fear that an expression of their opinion about the current status of international law could facilitate the creation of new customary international law.[22] These divergent views on the applicability or non-applicability of certain international law to cyberspace have consequently resulted in the failure of the UNGGE to submit a consensus

specifically focusing on the law of State responsibility, Dinniss (n 2) 28; Constantine Antonopoulos, 'State Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 56: 'As the Internet is an international domain, then States must conduct themselves over this domain in accordance with international law and therefore the use of cyberspace is subject to international law'; John R Crook (ed), 'Contemporary Practice of the United States Relating to International Law' (2013) 107/4 American Journal of International Law 243, 244; Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 13; see also Harold H Koh, 'State Department Legal Adviser Addresses International Law in Cyberspace' (2013) 107/4 American Journal of International Law 243, 244; see also The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, 2011) 9: 'The 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', taken from Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2014) 14 Baltic Yearbook of International Law 23, 23 f.

[17] Dinniss (n 2) 28.

[18] *Ibid*.

[19] Cf. Antonopoulos (n 16) 56 f.

[20] see e.g. Banks (n 7) 15, calling for attribution principles for cyber operations during an armed conflict: '[I]t may be prudent and perhaps legally advisable for States to develop and agree upon principles for attribution of cyber operations during an armed conflict'; see also Bannelier-Christakis (n 16) 39; Tsagourias (n 16) 13; regarding States, see statements made by, *inter alia*, Egypt and Cuba at the first substantive meeting of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security in September 2019, <http://papersmart.unmeetings.org/ga/oewg-on-icts/first-substantive-session-2019/programme/>.

[21] See Sanger, 'Utilities Cautioned' (n 3): 'Even after it has reached a conclusion, the White House might decide not to name the attackers, just as it decided not to publicly blame China for the theft of 22 million security files from the Office of Personnel Management'.

[22] Cf. Kristen E Eichensehr, 'The Law & Politics of Cyberattack Attribution' (forthcoming 2020, draft of 15 September 2019) 67 UCLA Law Review, 30, quoting Martha Finnemore and Duncan B Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (Temple University Beasly School of Law Legal Studies Research Paper, 2019) 11 f: public attributions 'may serve as early evidence of a "usage" – that is, a habitual practice followed without any sense of legal obligation. If such accusations persist and spread over time, States may come to assume that these accusations are evidence of *opinio juris*, delineating which acts are either appropriate or wrongful as a matter of international law.'

report in 2017, as its governmental experts could not agree on, *inter alia*, the applicability of the rules of State responsibility and the law of armed conflict to the cyber context.[23]

In any event, it can certainly be argued that the current framework governing attribution of cyber operations to States lacks clear rules of evidentiary standards and the burden of proof. That is particular due to the fact that even in the traditional realm, this question remains unresolved.[24] Therefore, the question of the necessity of evidentiary standards or the burden of proving the responsibility of the wrongful State in the context of cyber operations – in a judicial and non-judicial setting – will be the main research focus of this thesis.

3. The ILC Articles and Attribution

Before addressing these particular concerns, however, it might be useful to take a look at the current international legal framework governing attribution. The ILC Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter: ILC Articles)[25] codify 'the basic rules of international law concerning the responsibility of States for their internationally wrongful acts'[26] and offer possible remedies to address these wrongful acts. While there is no reference in the ILC Articles to the specificities of cyberspace, the general consensus is that they are also applicable to the cyber context.[27] Moreover, they offer a useful starting point and the theoretical baseline to understand the concept of attribution.

The commentary to the ILC Articles refers to attribution as 'the operation of attaching a given action or omission to a State.'[28] In general, Article 1 of the ILC Articles clearly states that every internationally wrongful act of a State attributable to it 'entails the international responsibility of that State.'[29] Articles 4 to 11 of the ILC Articles contain the codified rules on which actors are attributable to the State in a given case. In general, the Articles distinguish between conduct of *State* organs (including *de facto* State organs)[30], and conduct of *non-State* actors, who are either under a sufficient control of the State or whose conduct is accepted by the State as its own.[31] Thus, if there is no sufficient link between the natural person or group of persons and the State, attribution based on the ILC Articles – which regulate the consequences of wrongful *State* behaviour – cannot be established. For establishing singular responsibility, the ILC Articles are, consequently, sufficiently clear and have proven to be robust during the course of time. However, what transpires to be the real issue is the difficulty of *proving* the sufficient link between the non-State actor or State actor and the commission of the wrongful act. Here, the ILC Articles remain silent (on that, see further below).

[23] See Arun M Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' (*Lawfare Blog*, 4 July 2017) <www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
[24] Cf. Roscini (n 7) 242.
[25] See *supra* n. 13.
[26] ILC Articles Commentary (n 13) 31.
[27] Schmitt and Vihul (n 16) 79, which explicitly cites the ILC Articles as a basis for their rules on international responsibility in the cyber context; Antonopoulos (n 16) 56 f.
[28] ILC Articles Commentary (n 13) 36 (Article 2, para. 12).
[29] Article 1 ILC Articles.
[30] Cf. Articles 4 ff ILC Articles.
[31] Cf. Articles 8 and 11 ILC Articles.

The ILC Articles also contain some references to the possibility of establishing *shared* State responsibility, although these references are not as detailed as compared to those pertaining to *singular* responsibility.[32] Shared responsibility arises when a wrongful conduct is attributable to more than one State.[33] Here as well, however, while the concept of shared responsibility offers additional ways to claim redress against additionally responsible States, the main issue, the issue of *proving* the responsibility, remains unresolved.

Thus, the ILC Articles lay down the general legal requirements for attributing a conduct of a certain person or entity to the State (or multiple States). Although they do not take account of the specificities of cyberspace, they nevertheless seem to be able to withstand the test of time.

4. Evidentiary Issues and Attribution

However, the ILC Articles deliberately do not address evidentiary questions[34] – they see it as a precondition that the facts of the case are sufficiently established. There is, in fact, no established legal framework governing the question of evidentiary standards for proving a violation of international law.[35] Previous attempts of codifying existing rules through, *inter alia*, the International Law Commission have so far failed.[36] It is needless to say, that, while there are some contributions regarding the cyber context, due to the novelty of the topic, literature in this field remains scarce.

While difficulties of proving the existence of facts is not a new phenomenon,[37] the possibility of IP address spoofing, false-flag operations and multi-stage operations make attribution an even more challenging task in cyberspace.[38] And even if there is evidence pointing at one pertinent direction, the question is *how much* evidence is needed in order to discharge the burden of proof. This is interesting both in a judicial and a non-judicial context. In a non-judicial context, it is interesting to know how much evidence a State must gather before taking a reactionary measure against the wrongful act and whether there is even an international obligation to publicly provide evidence for doing so. In a judicial context it is interesting to know how much evidence an international court or tribunal (in particular, the ICJ) needs in order to be convinced of a State's responsibility. The question is also whether there are different standards when it comes to proving a wrongful act in either of these contexts. This thesis,

[32] See, in particular, Article 16 ILC Articles ('Aid or assistance in the commission of an internationally wrongful act') and Article 47 ILC Articles ('Plurality of responsible States'); cf. Berenice Boutin, 'Shared Responsibility for Cyber Operations' (2019) 113 AJIL Unbound 197, 197.
[33] See Boutin (n 32) 198.
[34] See ILC Articles Commentary (n 13) 72 (Chapter V, para. 8): 'Just as the articles do not deal with questions of the jurisdiction of courts or tribunals, so they do not deal with issues of evidence or the burden of proof'; see also Eichensehr (n 22) 34.
[35] Roscini (n 7) 242; Eichensehr (n 22) 3; cf. also Banks (n 7) 26.
[36] See the proposal made by A. Rajput, 'Evidence before International Courts and Tribunals', UN Doc. A/72/10.
[37] See i.a. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)* (Merits) [1986] ICJ Rep 14, para. 57, concerning a conventional conflict, where the ICJ noted: 'One of the Court's chief difficulties in the present case has been the determination of the facts relevant to the dispute. […] Sometimes there is no question, in the sense that it does not appear to be disputed, that an act was done, but there are conflicting reports, or a lack of evidence, as to who did it. The problem is then not the legal process of imputing the act to a particular State for the purpose of establishing responsibility, but the prior process of tracing material proof of the identity of the perpetrator. The occurrence of the act itself may however have been shrouded in secrecy.'
[38] See already above, and Dinniss (n 2) 100 f; Roscini (n 7) 234.

therefore, aims to analyse whether there are any existing patterns concerning evidentiary standards and the burden of proof with regard to attributing a cyber operation to a State in 1) a non-judicial context, and 2) a judicial context, with particular notice of the practice of the International Court of Justice (ICJ).

4.1. Evidentiary Issues in a Non-Judicial Context

There is a considerable lack of literature and State practice (as well as *opinio juris*), when it comes to assessing how much evidence is necessary to undertake an '*ex ante* attribution' of a cyber operation – i.e. an attribution in a non-judicial context. The Tallinn Manual 2.0 just notes that 'the reasonableness of *ex ante* attribution must be assessed on a case-by-case basis, considering […] relevant […] factors.'[39]

Also, States seem to have diverging views regarding the disclosure of evidence when undertaking an attribution. The UNGGE Report of 2015 for example notes that '[a]ccusations of organising and implementing wrongful acts brought against States should be substantiated'.[40] Arguably, such substantiation means disclosing supporting evidence concerning the attribution. Such assumption is in contrast, however, with national statements made by France, the UK and the US that there is no international obligation to provide evidence, despite the fact that such evidence might be useful for credibility purposes.[41] The Tallinn Manual 2.0 also notes that there is 'insufficient State practice and *opinio juris* (in great part because cyber capabilities are in most cases highly classified)' supporting the existence of such a rule.[42]

However, the creation of international attribution mechanisms established by, *inter alia*, the EU could provide insights into necessary evidentiary standards for an '*ex ante* attribution': The task of such international attribution mechanisms should be to undertake the difficult attribution process in cooperation with other States and come to a conclusion of who is or was behind a cyber operation.[43] One example is the EU's 'Cyber Diplomacy Toolbox', which describes a set of measures with which the EU can respond to so-called 'malicious' cyber activities under the EU's Common and Foreign Security Policy.[44] The Draft Implementing Guidelines for the

[39] Schmitt and Vihul (n 16) 82.

[40] See 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) UN Doc No. A/70/174, 13, para. 28 lit f; see also UNGA Resolution 73/27 (11 December 2018) UN Doc A/RES/73/27, drafted in large part by the Russian Federation and voted in favour by 119 States, which takes reference of the UNGGE Report of 2015.

[41] See, *inter alia*, speech by US State Department Legal Adviser Brian Egan of 2016, Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35 Berkeley Journal of International Law 169, 177: '[D]espite the suggestion by some States to the contrary, there is *no* international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action'; see also speech by UK Attorney General Jeremy Wright in 2018, Jeremy Wright, 'Cyber and International Law in the 21st Century' (*Gov.uk*, 23 May 2018) <www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>: 'There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based'.

[42] Schmitt and Vihul (n 16) 83; see also Roscini (n 7) 241, fn. 58: 'Whether or not States have an obligation to make evidence public is a matter of debate'.

[43] see e.g. Microsoft's proposal for a 'Digital Geneva Convention' or its newest approach, the creation of a 'Cyber Peace Institute' 'dedicated to exposing the details of harmful cyberattacks', Shannon Vavra, 'Microsoft, Hewlett Foundation preparing to launch nonprofit that calls out cyberattacks' (*Cyberscoop*, 9 September 2019) <www.cyberscoop.com/microsoft-cyber-peace-institute-hewlitt-foundation-brad-smith/>.

[44] General Secretariat of the Council, 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")' (19 June 2017), Doc 10474/17 <data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>.

Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (hereinafter: Draft Implementing Guidelines) note that in order to resort to some, but not all, measures, prior attribution of a cyber activity is required.[45] An earlier draft version of an EU paper on attribution related to this Toolbox contained a so-called 'uncertainty yardstick', developed by the EU Intelligence and Situation Centre (INTCEN), the intelligence body of the European External Action Service (EEAS)[46], which divided the range of probabilities of an attribution into percentages from 0-5% (remote chance) to 95-100% (almost certain). This yardstick, however, was removed in a later draft version.[47] It is thus not clear which evidentiary standards the EU would like to find sufficient when undertaking a collective attribution. However, analysing the EU Member States' practice in this context while they refer to the Toolbox might provide some valuable insights.

Another indication of how much evidence States view as sufficient when undertaking an attribution in the cyber context, is analysing what evidence they provide when applying cyber sanctions. Sanctions are a popular tool to address 'malicious' cyber activities. With it, States aim to deter malicious behaviour in cyberspace and send a signal to the public that they do not tolerate malicious cyber behaviour. These sanctions mechanisms, although they at times explicitly note that they do not constitute an attribution[48], might have an influence on the creation of international evidentiary standards concerning attribution, particularly when they are aimed at State organs or non-State actors affiliated with a State. Of particular interest for this thesis will be the EU cyber sanctions regime, which entered into force on 17 May 2019 with Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796. So far, not a single individual has been listed in the regime. As mentioned above, it will, however, be particularly interesting to assess the reasons States put forward to list *State* organs or non-State actors and what reasons they find sufficient to prove their involvement in a wrongful cyber operation.

4.2. Evidentiary Issues in a Judicial Context

When it comes to assessing what evidence is sufficient in a judicial context, there are, in general, different approaches within civil law and common law systems. While in civil law systems judges in general enjoy great liberties in the assessment of evidence, common law systems tend to follow a specific set of evidentiary standards.[49] Particularly the International Court of Justice, given that the 'constitutive documents of the ICJ are silent as to the question of the standard of

[45] *Ibid*, 4; General Secretariat of the Council, 'Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities' (9 October 2017), Doc 13007/17, 14 <data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf>.

[46] The EEAS serves as a diplomatic body of the EU High Representative for Foreign Affairs and Security Policy and exercises foreign ministry and defense ministry functions for the EU; the EU INTCEN is tasked with providing intelligence analyses to EU decision-making bodies, which are based on information voluntarily provided by the EU Member States.

[47] European External Action Service, 'Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities – discussion of a revised text' (18 March 2019), Doc 6852/1/19 REV 1, 10 <www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf>; note that this draft version is the only available version online.

[48] See, e.g. Recital 9 of Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber attacks threatening the Union or its Member States [2019] OJ L 129 I/13.

[49] Roscini (n 7) 248.

proof'[50], tends to follow a mixed approach, establishing standards on a case-by-case basis, without following set-in-stone rules.[51]

While some authors argue for a low evidentiary standard in the cyber context,[52] Roscini and Schmitt find a 'clear and convincing' evidentiary standard sufficient.[53] Whether that should be true for violations of any obligation, is to be questioned. Roscini concedes, for example, that the standard or proof might be lower for proving a lack of due diligence than for the commission of international crimes.[54] Similarly, Judge Higgins noted in her Separate Opinion to *Oil Platforms* that there is 'general agreement that the graver the charge, the more confidence must there be in the evidence relied on'.[55] This suggests that applying a universal standard for all cyber obligations seems unrealistic.

It is also important to note that, particularly in the cyber context, direct evidence will often be hard to obtain or even missing entirely. Most likely, circumstantial evidence will be the remaining option. The ICJ noted in *Corfu Channel* that, in case of reliance on mere circumstantial evidence, such evidence must leave '*no room* for reasonable doubt'.[56] The Court thus applied the, arguably, highest evidentiary standard for circumstantial evidence. Whether that will remain true in the cyber context, will be analysed in this thesis.

Regarding the burden of proof, the general rule is that the onus of proving a fact lies on the party claiming that fact.[57] Some scholars have advocated a reversal of the burden of proof in the cyber context, given the extreme difficulties some States face when proving the attribution of a cyber operation to a State.[58] One of these difficulties concerns the fact that the wrongful State exercises exclusive control over its territory, which is usually coupled with the fact that most of the evidence is classified.[59] These concerns have been rebutted by, e.g. Roscini, claiming that such an approach would, *inter alia*, be 'at odds with the *jurisprudence constante*

[50] Markus Benzing, 'Evidentiary Issues' in Andreas Zimmermann et al (eds), *The Statute of the International Court of Justice: A Commentary* (2nd ed, OUP 2012) 1263.
[51] *Ibid*, 1264; Cf. Roscini (n 7) 242; Mojtaba Kazazi, *Burden of Proof and Related Issues: A Study on Evidence Before International Tribunals* (Brill 1995) 323.
[52] E.g. David E Graham, 'Cyber Threats and the Law of War' (2010) 4 Journal of National Security Law and Policy 87, 93: 'Given the difficulties raised by the traditional requirement to attribute cyber attacks conclusively and directly to a state […] there is now a growing effort to formulate acceptable alternatives to the notion of 'conclusive attribution'.'
[53] Roscini (n 7) 252; Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited' (2011) 56 Villanova Law Review 569, 595: A clear and convincing standard 'obliges a state to act reasonably, that is, in a fashion consistent with the normal state practice in same or similar circumstances. Reasonable States neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence'.
[54] Roscini (n 7) 254.
[55] *Case Concerning Oil Platforms (Iran v United States)* (Merits) [2003] ICJ Rep 161 (Separate Opinion of Judge Higgins) 233, para. 33.
[56] *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 18.
[57] *Case Concerning Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Merits) [2010] ICJ Rep 14, 71, para. 162: 'To begin with, the Court considers that, in accordance with the well-established principle of *onus probandi incumbit actori*, it is the duty of the party which asserts certain facts to establish the existence of such facts'.
[58] Daniel J Ryan et al, 'International Cyberlaw: A Normative Approach' (2011) 42/4 Georgetown Journal of International Law 1161, 1185; Antonopoulos (n 16) 64.
[59] Ryan et al (n 58) 1185.

of the ICJ'.[60] Why that should be a grave issue, is, however, debatable. Given the fact that especially the ICJ does not restrict itself to set-in-stone rules, it could be plausible that the Court might decide differently in the cyber context. Therefore, the question still seems to be open to debate.

Also, what methods of proof are most effective in the cyber context is a point of interest for this thesis. There are voices in the literature noting that the Court should have to and most likely *will* make more use of its powers to appoint technical experts.[61] This is especially important as, already, private security firms provide valuable analyses on significant cybersecurity incidents, often revealing much more information than sovereign actors as to who could be behind a cyber operation.[62]

All of the above leads us to the unsatisfactory conclusion that the evidentiary framework in a judicial and non-judicial context is far from settled, let alone in the cyber context. The paragraphs above have hopefully demonstrated that there are lots of interesting and unresolved questions that arise in the context of proving the attribution of a cyber operation to a State. While there is a significant amount of literature, State practice and jurisprudence on questions of evidence, the literature landscape concerning the cyber context remains scarce. The aim of this thesis will be, therefore, to bring more clarity to the issue.

5. Research Question and Methodology

This research project will therefore aim to answer the following research questions:

1. What are the specific evidentiary issues when attributing cyber operations to States?
2. Is there a unique evidentiary standard required to discharge a State's burden of proof when undertaking an attribution in a non-judicial and a judicial context?
3. Regarding the judicial context: Which methods of evidence will be most effective to adhere to by courts, in particular the ICJ, in the cyber context?

To begin with, the research for this thesis will, on the one hand, consist of analysing existing literature in this field – literature on questions of evidence in a traditional setting, on the one hand, and literature on applying these conventional rules to the cyber context, on the other hand – and analyse advantages and shortcomings of the assumptions made.

Regarding evidentiary issues in a non-judicial context, especially official statements made by States with regard to the application of international law to the 'cyberspace' and State behaviour in the context of the EU Cyber Diplomacy Toolbox and the EU cyber sanctions regime will be closely analysed. In general, when assessing the evolution of new customary rules in this context, existing State practice and *opinio juris* will be assessed. Thus, research will focus on publicly available information from States (such as public governmental websites, EU press releases or other releases from intergovernmental organisations), and on the other hand, aim at

[60] Roscini (n 7) 245; Benzing also notes that 'commentators agree that the *jurisprudence constante* of the Court, especially in procedural and evidentiary questions, is normatively relevant', see Benzing (n 50) 1237.
[61] See Roscini (n 7) 263; Isabella Brunner et al, 'Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ' (2019) 25 Finnish Yearbook of International Law 75, 102 ff.
[62] Eichensehr (n 22) 9.

creating an overview over the different views States have with regard to proving attribution under international law.

Regarding the analysis of evidentiary standards, the burden of proof and methods of evidence in a judicial context, particularly the ICJ's jurisprudence, but also jurisprudence of other courts and tribunals, relating to evidentiary issues will be analysed and examined.

6. Preliminary Bibliography

6.1. Books and Book Chapters

Constantine Antonopoulos, 'State Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015).

William Banks, 'Who Did It? Attribution of Cyber Intrusions and the Jus in Bello', in Ronald T Alcala and Eric T Jensen, *The Impact of Emerging Technologies on the Law of Armed Conflict* (OUP 2019).

Markus Benzing, 'Evidentiary Issues' in Andreas Zimmermann et al (eds), *The Statute of the International Court of Justice: A Commentary* (2nd ed, OUP 2012).

Heather H Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012).

Yoram Dinstein, 'Computer Network Attacks and Self-Defence' in Michael Schmitt et al (eds), *Computer Network Attack and International Law* (Naval War College 1999).

Mojtaba Kazazi, *Burden of Proof and Related Issues: A Study on Evidence Before International Tribunals* (Brill 1995).

Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).

Michael Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015).

6.2. Articles

Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2014) 14 Baltic Yearbook of International Law 23.

Berenice Boutin, 'Shared Responsibility for Cyber Operations' (2019) 113 AJIL Unbound 197.

Isabella Brunner et al, 'Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ' (2019) 25 Finnish Yearbook of International Law 75.

John P Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats' (2016) 7 Harvard National Security Journal 391.

David D Clark and Susan Landau, 'Untangling Attribution' (2011) 2 Harvard National Security Journal 323.

John R Crook (ed), 'Contemporary Practice of the United States Relating to International Law' (2013) 107/4 American Journal of International Law 243.

Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35 Berkeley Journal of International Law 169.

Kristen E Eichensehr, 'The Law & Politics of Cyberattack Attribution' (forthcoming 2020, draft of 15 September 2019) 67 UCLA Law Review.

Martha Finnemore and Duncan B Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (Temple University Beasly School of Law Legal Studies Research Paper, 2019).

David E Graham, 'Cyber Threats and the Law of War' (2010) 4 Journal of National Security Law and Policy 87.

Harold H Koh, 'State Department Legal Adviser Addresses International Law in Cyberspace' (2013) 107/4 American Journal of International Law 243.

Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50 Texas International Law Journal 233.

Daniel J Ryan et al, 'International Cyberlaw: A Normative Approach' (2011) 42/4 Georgetown Journal of International Law 1161.

Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited' (2011) 56 Villanova Law Review 569.

6.3. UN and EU Documents

Charter of the United Nations, 24 October 1945, 1 UNTS XVI.

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber attacks threatening the Union of its Member States [2019] OJ L 129 I/13.

European External Action Service, 'Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities – discussion of a revised text' (18 March 2019), Doc 6852/1/19 REV 1, 10 <www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf>.

General Secretariat of the Council, 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")' (19 June 2017), Doc 10474/17 <data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>.

General Secretariat of the Council, 'Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities' (9 October 2017), Doc 13007/17, 14 <data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf>.

'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) UN Doc No. A/70/174, 13.

UNGA Resolution 73/27 (11 December 2018) UN Doc A/RES/73/27.

UN ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) GAOR 56th Session Supp. 10, 43.

6.4. Governmental Documents

Jeremy Wright, 'Cyber and International Law in the 21st Century' (*Gov.uk*, 23 May 2018) <www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

6.5. Newspaper and Blog Articles

Michael McElfresh, 'Cyberattack on Ukraine Grid: Here's How It Worked and Perhaps Why It Was Done' (*The Conversation*, 18 January 2016) <http://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802>

Kaspersky Team, 'Olympic Destroyer: Who Hacked the Olympics?' (*Kaspersky Daily*, 9 March 2018) <www.kaspersky.com/blog/olympic-destroyer/21494/>.

David E Sanger, 'Utilities Cautioned About Potential for a Cyberattack' *The New York Times* (New York, 29 February 2016) <http://nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?auth=login-email&login=email>.

Arun M Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' (*Lawfare Blog*, 4 July 2017) <www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

Shannon Vavra, 'Microsoft, Hewlett Foundation preparing to launch nonprofit that calls out cyberattacks' (*Cyberscoop*, 9 September 2019) <www.cyberscoop.com/microsoft-cyber-peace-institute-hewlitt-foundation-brad-smith/>.

6.6. Case Law

Case Concerning Oil Platforms (Iran v United States) (Merits) [2003] ICJ Rep 161.

Case Concerning Oil Platforms (Iran v United States) (Merits) [2003] ICJ Rep 161 (Separate Opinion of Judge Higgins).

Case Concerning Pulp Mills on the River Uruguay (Argentina v Uruguay) (Merits) [2010] ICJ Rep 14.

Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States) (Merits) [1986] ICJ Rep 14.