The University Of Sheffield.

Inducing compliance with international law in cyberspace – State responsibility, countermeasures and the obligations of due diligence

By Andraz Kastelic

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

The University of Sheffield
School of Law

August 2019

Abstract

This thesis investigates the capacity of established international legal mechanisms to supress non-compliance with international law in cyberspace and thus to restore peace and security of individual nations as well as the international community.

Based on a rational choice theory of compliance with international law, this thesis argues that States choose to disregard their international legal obligations and resort to unlawful cyber operations when the benefits of non-compliance outweigh the associated costs. In the absence of a central enforcement authority, countermeasures are the only viable and potentially effective compliance inducing mechanism in the anarchical setting of international relations.

However, the technical complexity of cyber operations and legal standards of proof are likely to inhibit attribution, a legal precondition to invoking State responsibility and taking countermeasures. In response to the difficulties arising in relation to attribution, this thesis introduces the due diligence obligations of prevention and termination. Accordingly, States are not only required to abstain from conducting unlawful cyber operations but also to diligently prevent and terminate cyber operations emanating from their territory, which violate the international legal rights of other States and of which the State of emanation knew or should have known. Due diligence obligations require States not only to do their best to prevent and terminate internationally unlawful cyber operations but also to proactively develop the capacity to do so. Compared to attribution, invocation of State responsibility for non-diligent behaviour is indeed a more attainable task for the State injured by an unlawful cyber operation and wishing to take countermeasures.

The final section of the thesis elaborates on several legal and practical conditions required to be met to take countermeasures against a non-diligent State. Most importantly, it argues that only countermeasures proportional with the initial wrongdoing and with the material injury caused by that wrongdoing have the capacity to alter the rational choice of the non-diligent

State, *in fact* also responsible for conducting or sponsoring unlawful cyber operations. These countermeasures induce compliance with obligations of due diligence as well as with the international obligations breached by the unlawful cyber operation occasioned by the lack of diligence.

Acknowledgements

I would like to extend my sincere gratitude to the following people. To both of my supervisors, Dr Russell Buchan and Professor Nicholas Tsagourias, for their patient mentorship; to Dr Francesca Strumia, for her direction on questions of methodology; to Ms Sarah Beedham, for her instrumental administrative support; to Miss Ayda Dabiri for proofreading the thesis; to friends and family in Ljubljana, Oxford, Geneva, and Sheffield for putting up with me.

I am extremely grateful to the University of Sheffield, School of Law for the generous funding of my research and extracurricular activities.

Table of contents

Chapter 1

Introduction: aim, object and methodology

Faced with the proliferation of malicious cyber operations endangering international peace and security, the aim of this thesis is to examine the ability of international legal mechanisms to supress unlawful inter-State cyber operations and thus contribute to the maintenance of international peace and security.

To that end, this chapter begins by presenting the problem – unlawful, inter-State cyber operations below the threshold of the use of force, which not only constitute a threat to peace and security but also contribute to the erosion of international law. To avoid a purely theoretical discussion, three examples of non-forceful, yet unlawful, inter-State cyber operations are presented in this chapter. The circumstances of these real-world examples and their legal implications are analysed in detail in later chapters and throughout this thesis. The second part of the chapter outlines existing solutions to the aforementioned problem and explains why they are unlikely to have any meaningful impact on reducing threats to peace and security. For this reason, this chapter explores established international law and the encompassing mechanisms able to supress inter-State cyber operations thereby increasing peace and security. The chapter concludes by briefly explaining the methodology, originality and utility of this thesis.

1. Problem – internationally wrongful inter-State cyber operations below the use of force threshold

There is no denial that malicious cyber operations – the employment of software and the enabling hardware for the purpose of an unauthorised manipulation of a remote software and, consequently, various dependant computerised and networked physical systems – are a menace of the modern world. Gradually, the world is accepting cyber operations as a plausible and potentially dangerous threat preying not only on individuals and businesses but also

States. These 'unintended consequences of technological advances',[1] as UN Secretary General Guterres labelled them, are not science fiction and the list of serious occurrences seems to be of indefinite length.

This thesis considers internationally wrongful inter-State cyber operations below the threshold of the use of force. The paragraphs that follow elaborate on what are considered inter-State cyber operations and when they constitute internationally wrongful acts below the threshold of the use of force. This introductory chapter also rationalises the limited scope of the research by advancing the argument that inter-State cyber operations below the use of force are the biggest threat to peace and security and a very real problem of the present and not the dreaded future. To underline the practical implications of my research, this section also introduces three real-world examples of unlawful inter-State cyber operations below the use of force threshold which will then be subjected to further rigorous analysis throughout the thesis.

1.1. Inter-State cyber operations

Inter-State cyber operations are operations that target States *and* operations for which States are *in fact*, though not necessarily also *in law*,[2] responsible. These operations are hereinafter referred to as inter-State cyber operations.

In the context of this thesis, a State is the target of an unlawful cyber operation when the consequences of that cyber activity proximately result in the denial of a legally protected right of that State. As will be explained in the sixth chapter, a cyber operation can constitute a international legal rights of a State directly or indirectly.

---

[1] United Nations, 'The Secretary-General's remarks at opening of 72nd session of the General Assembly' (New York, 12 September 2017) <un.org/sg/en/content/sg/statement/2017-09-12/secretary-generals-remarks-opening-72nd-session-general-assembly> accessed 12 August 2019

[2] *See* ch 4

On the other hand, a State is considered to be *in fact* responsible for a cyber operation whenever the cyber operation is conducted or executed by a State organ or by any natural person exercising a State function. A State is also deemed to be *in fact* responsible for a cyber operation when it is conducted by a non-State actor and would not have materialised but for the enabling involvement of that State in any degree or capacity. This includes, *inter alia*, cyber operations conducted by a non-State actor receiving general or specific support by a State, be it in the form of financial, operational, intelligence or otherwise; such operations are hereinafter labelled as State-sponsored operations.

In addition to cyber operations conducted by private actors focused on illegal financial gains, States have embraced cyber operations as a new 'low-cost tool of statecraft'[3] to attain their self-interested strategic objectives in international relations.[4] Since 2007, the year Estonia was hit by a crippling cyber operation, there have been no less than 220 *known* malicious State-sponsored or -conducted cyber operations or on average 20 per year.[5] As such cyber activities often go undetected or unreported, it is highly likely that the incidence of such cyber operations is greater.[6]

Responsibility *in fact* is to be distinguished from responsibility *in law*. Socio-political methods of attribution of cyber operations can indicate responsibility *in fact* but, as the fourth chapter argues, do not provide evidence up to the international standard of proof required for the establishment of the responsibility *in law*. Responsibility in law is governed by the secondary rules of the law of State responsibility, in particular the legal framework of attribution. Asserting that a State is *in fact* responsible for a cyber operation does not automatically denote legal attribution of the act that deprived the injured State of its international legal rights, although

---

[3] Daniel R Coats, 'Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community' (Office of the Director of National Intelligence, US Senate Select Committee on Intelligence, 13 February 2018) 5 <dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf> accessed 12 August 2019

[4] *See* ch 2

[5] Council on Foreign Relations, 'Cyber Operations Tracker data' <https://www.cfr.org/interactive/cyber-operations/export-incidents?_format=csv> accessed 12 August 2019

[6] *See eg* ENISA, 'Threat Landscape Report 2017' (January 2018) 94 <enisa.europa.eu/publications/enisa-threat-landscape-report-2017> accessed 26 January 2019

the responsibility *in fact* and responsibility *in law* are intertwined concepts. The process of establishing the legal attribution of cyber operations to a specific State and the consequential invocation of the international legal responsibility of that State is elaborated upon in the fourth chapter of this thesis.

Even when technology fails to lead to *the* State and prevents the injured State from legally attributing a cyber operation to a particular State, the scope or sophistication of a cyber operation are sufficient indicators to exclude the private non-State actors acting out of their (usually) profit-pursuing rationale and to assert that it is a State that is *in fact* behind the cyber operation. This approach can be justified even when the non-State actor was the one who developed the tools and means for a cyber operation or even launched it. ProjectSauron, a cyber operation targeting the computer networks of (mostly) Russian government entities, has not been technically attributed to any State. Nonetheless, researchers concluded that an operation of such complexity 'can only be executed with support from a nation-State'[7] and thus qualifies as State-sponsored as well as an inter-State cyber operation. Rid and Buchanan draw similar conclusions in the context of a Stuxnet operation targeting Iranian uranium enriching facilities: 'No non-State actor, and indeed few governments, would likely have the capability to test Stuxnet, let alone build and deploy it.'[8] 'This is not some hacker sitting in the basement of his parents' house[;] it seems that the resources needed to stage [Stuxnet] point to a nation State'[9] another security analyst echoed.

Although inter-State cyber operations seldom cause physical damage or injury to persons, their negative consequences are considerable. States point their cyber arsenal towards another State to quickly and inexpensively maximise their relative power resources. Correspondingly, and what is of particular importance to this thesis, by diminishing the national

---

[7] Global Research & Analysis Team, 'ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms' (Kaspersky Lab, 8 August 2016) 21 <securelist.com/faq-the-projectsauron-apt/75533/> accessed 26 January 2019

[8] Thomas Rid & Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38(1–2) J of Strategic Studies 4, 20–21

[9] Jonathan Fildes, 'Stuxnet worm 'targeted high-value Iranian assets' *BBC* (23 September 2010) <bbc.com/news/technology-11388018> accessed 26 January 2019

power resources of the targeted State(s), malicious inter-State cyber operations lessen the security of the targeted State(s).[10]

Despite the fact that modern technology has theoretically democratised the ability to bring a State to its knees and to undermine its peace and security,[11] it holds true that State-sponsored or -conducted cyber operations still hold more significant potential to do so. According to the Swiss National Cybersecurity Strategy, for instance, '[n]ational actors or actors financed by States usually have greater financial, technical and personnel resources and are better organised, which explains their relatively great damage potential'.[12] Correspondingly, research indicates that the most feared threats among cybersecurity professionals are the ones exploiting previously undiscovered, so-called zero-day vulnerabilities and the ones conducted by actors with attack skills of highest sophistication or with the strong backing of States,[13] which are all typical attributes of a State-sponsored cyber operation.

Scale and complexity, the definitive characteristics of a State-conducted or -sponsored cyber operations are positively correlated with the magnitude of the resulting disruption. In other words, State(-sponsored) cyber culprits in possession of significant resources and knowledge are the ones that wreak the biggest havoc on the networked infrastructure and pose the greatest threat to peace and security of States. This is the reason this research focuses on cyber operations that are conducted or sponsored by States.

Being focused on inter-State cyber operations for their potential disruption and the scale of such disruption, the following chapters attempt no investigation of cybercrime, computer-related acts committed by private actors constituting a criminal offence in contravention of particular pieces of domestic legislation taking form of, for example, an offence against the

---

[10] *See* ch 2
[11] *See* ch 5
[12] Swiss Confederation, 'National strategy for the protection of Switzerland against cyber risks' (19 June 2012) 10. *See also* Eric Lundbohm, 'Understanding nation-state attacks' (2017) 2017/10 Network Security 1, 5–8: '[f]rom the limited number of verified State sponsored cyber activities, both the intent and the targets are large.'
[13] '2017 Black Hat Attendee Survey' (BlackHat USA, July 2017) 20 <blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf> accessed 12 August 2019

confidentiality, integrity and availability of cyber infrastructure and data, computer-related fraud and forgery, content-related offences, including ones related to infringements of copyright and related rights, etc.[14]

1.2. Internationally wrongful cyber operations below the use of force

The focus of this thesis are inter-State cyber operations which are internationally wrongful or, in other words, the ones constituting conduct not in conformity with the international legal obligations of States or conduct contrary to the international legal rights of another State, regardless of the origin or character of such obligations and rights.[15] Much like the understanding of the ILC in its deliberations on international law of State responsibility and of the Arbitral Tribunal in the Rainbow Warrior affair, 'any violation by a State of any obligation, of whatever origin'[16] is considered to be internationally wrongful for the purpose of this thesis.

As I explain in the following chapter, unlawful inter-State cyber operations present a serious threat not only to the targeted States but to the whole international community as well. On one hand, internationally wrongful inter-State cyber operations deprive the targeted States of their national power resources and award the State *in fact* responsible for the operation with illegitimate, inexpensive and quick power gains. On the other hand, non-compliance with international law further erodes the rule of law and endangers international peace that is sustained by legally prescribed constraints on the selfish maximisation of power. Both consequences have a detrimental effect on the security of the States.

The methodological approach adopted in this thesis is not without its limitations, however. This thesis excludes from its research scope cyber operations constituting an internationally prohibited use of force. In accordance with the prevailing use of terminology in the relevant literature, forcible cyber operations are referred to as *cyber attacks*. Instead, this research

---

[14] Examples inspired by the Convention on Cybercrime (Budapest, 23 November 2001) 185 CETS arts 2–10
[15] UNGA Res 56/83 'Responsibility of States for Internationally Wrongful Acts' (12 December 2001) UN Doc A/RES/56/83 art 12 (ARSIWA)
[16] *Rainbow Warrior (New Zealand v France)* [1990] XX UNRIAA 251 para 75

centres on cyber operations below the use of force, or the ones which fall short of resulting in injury to humans or physical damage to property. To understand when a cyber operation is indeed below the use of force, the content and limitations of the international prohibition of the use of force must be considered further.

Except for a pair of notable exceptions,[17] use of force in international relations is not only prohibited by the UN Charter Article 2(4) but it also constitutes a violation of 'the integral part'[18] of international customary law.[19] Acknowledging the historical context of the UN Charter, one can easily see that the ambitions of the Article 2(4), or of any other Charter articles, were never intended to govern inter-State cyber operations.

This, however, does not mean the law does not apply to cyber operations or that cyber operations cannot amount to an internationally prohibited use of force. Nevertheless, the prohibition of the use of force is limited to armed force and does not extend to the prohibition of political or economic pressures. Arguments in favour of the narrow understanding of Article 2(4) can be extrapolated from the object and purpose of the treaty expressed in the Charter's Preamble and upon a closer inspection of the *travaux préparatoires*. The purpose of the Charter to 'save succeeding generations from the scourge of *war*'[20] and to 'ensure […] that *armed* force shall not be used, save in the common interest'[21] is a clear indication that the prohibition of the use of force is limited to armed force. An even more compelling (and oft-cited) piece of evidence supporting this assertion are the rejections of the amendments during the Charter drafting process. Brazil's proposal to expand Article 2(4) to include the prohibition of the use of economic force[22] was rejected by a convincing majority[23] and so was the proposal

---

[17] Charter of the UN (San Francisco, 26 June 1945) arts 51 & 39
[18] Yoram Dinstein, *War, Aggression and Self-defence* (CUP 2001) 92
[19] 'Article 2, paragraph 4, together with other provisions of the Charter, authoritatively declares the modern customary law regarding the threat or use of force.' ILC, 'Draft articles on the law of treaties' (1966) II Ybk of the ILC 247
[20] Charter of the UN (n 17) Preamble [emphasis added]
[21] ibid
[22] UNCIO, 'Commission 1, general provisions' (San Francisco, 1945) VI London, United Nations Information Organisations 559
[23] ibid 335

of Iran to expand the Article 2(4) to include the prohibition of the use of political force.[24] Subsequent UN practice[25] confirms this narrow interpretation of the prohibition of the use of force.

What is more, conduct is to be characterised as an unlawful use of armed force when the effects of the conduct damage physical property or injure human beings, regardless of the instrument used.[26] This effect-conscious approach is particularly relevant for the definition of cyber attacks within the framework of Article 2(4) and has since gained considerable traction among legal scholars.[27] Roscini goes as far as to argue that '[i]t is virtually uncontested that a cyber attack that causes or is reasonably likely to cause physical damage to property, loss of life or injury to persons'[28] would nowadays be considered to have reached the threshold of a prohibited use of force.

Albeit limited, evidence of *opinio juris* supports this interpretation of the law of the use of force in cyberspace. Koh, then Legal Adviser to the US Department of State, argued that '[c]yber activities that *proximately* result in death, injury, or *significant* destruction would likely be viewed as a use of force'.[29] A similar argument has been put forward by Nakasone of the US

---

[24] Nico Schrivjer, 'The Ban on the Use of Force in the UN Charter' in Marc Weller (ed), *The Oxford Handbook on the Use of Force in International Law* (OUP 2015) 470

[25] UNGA 'Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-operation among States' (16 November 1964) 19th Sess UN Doc A/5746, 35 para 39

[26] *Dinstein* (n 18) 88. Similar argument put forward also by Karl Zemanek, 'Armed Attack' in *Max Planck Encyclopedia of Public International Law* (October 2013) para 21 <https://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e241?rskey=FxjPfU&result=1&prd=EPIL> accessed 26 January 2019

[27] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) J of Conflict and Security L 212, 221. *See also eg* Michael Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013)

[28] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 53

[29] Harold H Koh, 'International Law in Cyberspace' (US Department of State, 18 September 2012) <2009-2017.state.gov/s/l/releases/remarks/197924.htm> accessed 26 January 2019

Cyber Command,[30] British Attorney General Wright[31] and, most recently, Estonian President Kaljulaid.[32]

Although Koh's statement confirms how to apply the doctrine, as can be observed in the writings of prominent legal scholars, it also uncovers two particularities of the definition of the use of force in the cyber context. First, in assessing the legal qualifications of the cyber operation, its destructive and harmful effects need not be direct but can be proximate and must exhibit a legal causal nexus[33] with the cyber operation. For this reason, the Tallinn Manual argues that '*all reasonably foreseeable* consequences of the cyber operation'[34] qualify as proximate results. This argument is also advanced by Roscini, who claims the destructive or harmful secondary and tertiary effects of the cyber operation signal that the act itself is considered to have reached the threshold of the use of force.[35] The reasoning is in fact rooted in established international law; the unlawful character of (and State responsibility for) an indirect use of force has been recognised by the ICJ in its Nicaragua judgment.[36] Considering that the direct result of a cyber operation is in fact merely an alteration of a computer-code, which, indirectly, causes damage to physical objects, or injury or death to persons, this recognition of indirect consequences as a legal foundation for establishing the violation of the

---

[30] '[C]yber operations that cause death, injury, or significant damage to property would likely be considered a prohibited use of force triggering the U.S.'s inherent right of self-defense.' US Senate, 'Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service' (1 March 2018) 14 <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf> accessed 26 January 2019

[31] Wright argued 'the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self- defence, as recognised in Article 51 of the UN Charter.' Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) <gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 23 July 2019

[32] Michael N Schmitt, 'Estonia Speaks Out on Key Rules for Cyberspace' (Just Security, 10 June 2019) <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/> accessed 23 July 2019

[33] For more on causation in fact and in law, see ch 5.

[34] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 343 [emphasis added]

[35] *Roscini* (n 28) 53

[36] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep para 209

obligation to refrain from using force, is also imperative when establishing a breach of the prohibition of the use of force by a cyber operation.

Acknowledging the secondary and tertiary consequences of a cyber operation is especially important because the destruction of a computer code does not automatically constitute an unlawful use of force. Although traditional legal doctrine does not consider data as property, some scholars proposed that the destruction of, or damage to, computer data would constitute a use of force. One of the scholars in favour of this approach is Barkham who argues that '[g]iven that technological advances have increased the strategic importance of the information industry, there is a clear argument for equating data with property'.[37] I am not convinced computer data – zeroes and ones which, in comparison to brick and mortar, are replicated with relative ease – should be considered property, but its destruction or alteration can certainly amount to a use of force if the said cyber operation indirectly causes damage to physical property or injury to a human being. Such consequences are indeed likely, but certainly not guaranteed.

The second lesson from Koh's statement relates to the extent of physical damage required to classify a cyber operation as a use of force. It appears there is no *de minimis* threshold when it comes to the resulting injury or death, but there is one when assessing physical damage to property for the purpose of determining whether a cyber operation is indeed considered to be use of force or not. While every injury or death caused by a cyber operation means it is indeed a violation of the prohibition of the use of force, it seems that damage to property must be *significant* to qualify as such. This reasoning corresponds to arguments advanced by legal theorists who distinguish between so-called minor uses of force and uses of force that are not

[37] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2011) 34 (1) New York University J of Intl L and Pol 57, 88

minor; an act constituting a mere unlawful intervention and an act prohibited under the Article 2(4), respectively.[38]

Aside from Schmitt's attempt,[39] neither scholarship nor *opinio juris* related to cyber operations provide a clear legal framework for assessing the gravity of the damage caused by a cyber operation in order to classify it as an unlawful use of force. In fact, later expressions of *opinio juris* cast a shadow of a doubt on the hard delineation between forceful and non-forceful cyber operations previously advocated by Koh. In 2018, Commander Nakasone of the US Cyber Command noted that 'the malicious cyber operations that meet the definition of significant consequences *would likely also cross the threshold* of an unlawful use of force.'[40] Moreover, no explicit affirmation in the established doctrine of the use of force may be found to support the theory that the extent of damage determines whether the act is considered to have risen to the requisite level of the use of force or not. Discussing the prohibition enshrined in the UN Charter Article 2(4), ILC's Special Rapporteur Ago was adamant that 'no doubt should […] remain as to the prohibition by the Charter—in keeping with general international law—of any kind of conduct involving any assault whatsoever on the territorial sovereignty of another State, *irrespective of its magnitude*, duration or purposes'.[41] Also, the UN Declaration on the Granting of Independence to Colonial Countries and Peoples of 14 December 1960 reaffirmed the international obligation to respect the prohibition of the use of force, including '*[a]ll* armed action',[42] reaffirming the idea proposed by ICJ Judge Alvarez in his individual opinion in the Corfu Channel Case.[43] The fact that State practice recognises no *de minimis* threshold has

---

[38] *See eg* Marry E O'Connell, The Prohibition of the Use of Force' in Nigel White & Christian Henderson, *Research Handbook on International Conflict and Security Law* (Edward Elgar 2013) 89–120

[39] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Colum J of Transnat'l L 885, 914–915

[40] *US Senate* (n 30) 27–28 [emphasis added]

[41] ILC, 'Addendum - Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur the internationally wrongful act of the State, source of international responsibility (part 1)' (1980) II(I) Ybk of the ILC UN Doc A/CN.4/318/Add.5–7, para 58 [emphasis added]. *See also* Ian Brownlie, *International Law and the Use of Force by States* (OUP 1963) 214 & 432; *Dinstein* (n 18) 175; Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma (ed), *The Charter of the United Nations: A Commentary* (vol I, OUP 2002) 123

[42] UN GA Res 1514 (XV) (14 December 1960) UN Doc A/RES/1514 [emphasis added]

[43] *Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania)* (Individual Opinion of Judge Alvarez) [9 April 1949] ICJ Rep 4, 47

also been convincingly established by Yiallourides, Gehring and Gauci.[44] For these very reasons, and perhaps until State practice and *opinio juris* establish otherwise, this chapter remains focused on a rather basic definition of cyber attacks in violation of the use of force prohibition, defined by the reasonably foreseeable effect of any kind of physical damage to property or injury to a human being.

Two reasons guide the decision to limit the research scope of the present investigation to cyber operations which do not result in damage to physical objects or injury to human beings and thus fall below the threshold of the use of force. First, the legal treatment of cyber operations amounting to use of force attracted a wealth of contributions from prominent legal scholars who explored and applied the principles of jus ad bellum and jus in bello to cyber attacks. Indeed, the academic discussion on the application of public international law and the unlawful character of aforementioned cyber operations has been lively; scholars such as the above-quoted Buchan, Roscini, Schmitt, Tsagourias[45] and others have generated an impressive volume of scholarship explaining and applying existing international law to cyber operations amounting to the use of force and beyond. On the other hand, less has been written about cyber operations below the use of force. This is the first reason behind the decision to limit the research scope and focus on the legal inquiry of cyber operations which do not result in damage to physical objects or injury to human beings.

More importantly, the second reason for the limited scope of the research is dictated by the prevalence of cyber operations below the use of force. While I certainly lack the courage to claim that the future does not hold destructive or deadly cyber operations and I am of a firm conviction that clarification of the applicable international law framework before such a thing does occur is imperative, the research omits the investigation of forcible cyber operations, or

---

[44] Constantinos Yiallourides, Markus Gehring & Jean-Pierre Gauci, *The Use of Force in relation to Sovereignty Disputes over Land Territory* (British Institute of International and Comparative Law 2018) 34–44

[45] *See eg* Roscini (n 28); Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' 17 (2012) J of Conflict and Security L 231–232; Michael N Schmitt, The Law of Cyber Warfare: Quo Vadis? (2014) 25 Stanford L & Pol Rev 269

cyber attacks, because most computer network operations, a reality of a modern society, in fact fail to violate the prohibition of the use of force.

Despite the dire prognoses of an impending cyber Pearl Harbour,[46] cyber operations are yet to injure a human being. What is more, at the time of the drafting of this chapter, only two known cyber operations resulted in the destruction of property. In 2010, Stuxnet malware caused the destruction of about one thousand uranium enriching centrifuges in a Fuel Enrichment Plant in Natanz, Iran.[47] And in 2014, the German Federal Office for Information Security reported that a cyber attack had caused 'an accumulation of breakdowns of individual components of the control system or of entire facilities'[48] of a German steel mill facility. In accordance with the definition of the use of force in the context of cyber operations, both would qualify as an unlawful use of force.

Far more urgent than the discussion of destructive cyber attacks is the extensive scholarly debate on the capacity of international law to reduce the prevalence of cyber operations below the use of force. In the words of Michael Rogers, a Commander of the US Cyber Command, the major concerns nowadays are 'cyber threats to US interests and infrastructure, [many of which] now occur below the threshold of the use of force and outside of the context of armed conflict, but cumulatively accrue strategic gains to our adversaries.'[49]

---

[46] 'Leon Panetta warns of "cyber Pearl Harbour"' *BBC* (12 October 2012) <https://www.bbc.com/news/av/technology-19923046/leon-panetta-warns-of-cyber-pearl-harbour> accessed 19 May 2019

[47] David Albright, Paul Brannan & Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?' (Institute for Science and International Security Report, 22 December 2010) <http://goo.gl/yM4Wy> accessed 3 August 2018

[48] Bundesamt für Sicherheit in der Informationstechnik, 'Die Lage der IT-Sicherheit in Deutschland 2014' (November 2014) 31 <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf;jsessionid=686D15F6B6BFAD9B90DE29C65EE3937F.2_cid341?__blob=publicationFile&v=2> accessed 11 December 2018

[49] US House of Representatives, 'Statement of Admiral Michael S Rogers, Commander United States Cyber Command Before the House Committee on Armed Services Emerging Threats and Capabilities Subcommittee' (11 April 2018) 12 <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf> accessed 19 May 2019

1.3. Shamoon, 2007 DDoS, RedOctober

Three examples of unlawful inter-State cyber operations below the use of force serve as the framework for this enquiry and assist in eliminating the shackles of a purely theoretical perspective. Even though these examples are extensively analysed throughout the thesis, the following paragraphs offer a practical context and analyse how these operations fit in the limited framework of the present research.

Pragmatism guides the choice of these examples. While a great majority of inter-State cyber operations are shrouded in a veil of mystery, much has been uncovered and documented about each of the examples listed below and this wealth of publicly available information allows for a relatively detailed analysis. However, the three examples are by no means an absolute limitation on my analysis; the thesis frequently refers to a variety of other cyber operations to support the theoretical arguments presented in the following chapters.

The first example to be considered is the **Shamoon** cyber operation, which erased thousands of computer hard drives of Aramco, the national Saudi Arabian oil company in 2012. The operations of the biggest oil company in Saudi Arabia were crippled but no physical damage has been recorded;[50] indeed Aramco replaced the erased hard drives – which led the drafters of the Tallinn Manual 2.0 to argue that the operation resulted in physical damage.[51] In reality however, the cyber operation itself did not result in physical destruction; Aramco arguably replaced computer hard drives affected by the Shamoon malware but only because the company 'decided trying to recover data or figuring out what was usable would be too time-consuming'.[52] The operation had no negative effect on the oil production capacity of Aramco.[53]

---

[50] *See eg* Christopher Bronk & Eneken Tikk-Ringas, 'The Cyber Attack on Saudi Aramco' (2013) 55(2) Survival, Global Politics and Strategy

[51] *Schmitt* (n 34) rule 4 cmt 13

[52] Fahmida Y Rashid, 'Inside the Aftermath of the Saudi Aramco Breach' (Dark Reading, 8 August 2015) <https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676> accessed 11 August 2019

[53] Sahar Alshathry, 'Cyber Attack on Saudi Aramco' (2017) 11(5) Intl J of Management and Information Technology 3038

Despite the fact that no clear and convincing evidence identifying a specific orchestrator of the operation is freely available, the responsibility *in fact* for Shamoon is ascribed to a State. The use of previously-unknown system (so called zero-day) vulnerabilities as well as the quantity and quality of resources and skills employed by the perpetrators of this operation is what led the researchers to draw such a conclusion.[54]

Since Shamoon did not cause physical destruction or injury to human beings, it does not constitute an unlawful use of force. Much like any other cyber operation consisting of unauthorised access to cyber infrastructure located in the sovereign territory of another State, Shamoon does, however, constitute a violation of sovereignty; in this case, the sovereignty of Saudi Arabia. This means Shamoon can rightfully be classified as an unlawful inter-State cyber operation. To reinforce the assertion of its unlawful character, I must delve into the rather contentious status of the norm of sovereignty in cyberspace.

Sovereignty equals independence; 'whatever the person or thing is on [the territory of a sovereign State] is ipso facto subjected to the supreme authority of the State [and] no other State may exercise its power within the boundaries of the home territory.'[55] Being a principle of the international law, it denotes 'the collection of rights held by a state'[56] protecting the States from, for example, external intervention in its domestic affairs and the use of force against it.[57] Many of the principles of international law, however, 'find expression in customary law, and therefore exist as rules derived from that source.'[58] Accordingly, aside from being a

---

[54] Christiaan Beek & Raj Samani, 'The State of Shamoon: Same Actor, Different Lines' (*McAfee*, 25 April 2017) <https://securingtomorrow.mcafee.com/executive-perspectives/state-shamoon-actor-different-lines/> accessed 19 May 2019. *See also* Nicole Perlroth & Clifford Krauss, 'A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try' *New York Times* (15 March 2018) <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html> accessed 12 August 2019

[55] Robert Jennings & Arthur Watts (eds), *Oppenheim's International Law* (9th edn, vol I Peace, Longman 1992) 564. See also definition by Max Huber in *Island of Palmas Arbitration (Netherlands v US)* [1928] II UNRIAA 829, 838

[56] James Crawford, *Brownlie's Principles of Public International Law* (8th edn, OUP 2012) 448

[57] *See eg* Case Concerning Military and Paramilitary Activities in and Against Nicaragua (n 36) para 251

[58] Hugh Thurlway, 'The Sources of International Law' in Malcolm D Evans, *International Law* (4th edn, 2014 OUP) 128

general principle of international law, sovereignty has gained status as a customary norm, the violation of which bears legal consequences. In addition to the writings of prominent legal scholars arguing that 'States are under international *legal obligation* not to commit any violation of the independence, or territorial or personal authority, of any other State',[59] this narrative has been promoted also by international jurisprudence. In the Corfu case, the ICJ decided that the unauthorised intrusion of British naval forces into Albanian territorial waters 'constituted a violation of Albanian sovereignty'.[60] Similar claims were made by the ICJ in the Nicaragua case, pronouncing the unauthorised American overflight of Nicaragua's territory as having 'directly infringed'[61] the territorial sovereignty of Nicaragua.

The ideas of reconceptualisation of sovereignty for cyberspace proposed at the end of the last millennium[62] were laid to rest long ago; States[63] and scholars[64] have taken the position that the principle of sovereignty applies to cyberspace, not least because the integral parts of virtual cyberspace are the enabling physical objects, which are undeniably governed by the traditional doctrine of sovereignty. Thus, States have an absolute and supreme authority over the cyber infrastructure located on their territory, subject to restrictions laid down by international law. Accordingly, any unauthorised intrusion into a cyber infrastructure located on the territory of a sovereign State constitutes an internationally wrongful violation of the sovereignty of that State.

---

[59] *Jennings & Watts* (n 55) 382. *See also* Crawford (n 56) 448; Malcolm N Shaw, *International Law* (7th edn, CUP 2014) 353

[60] *Corfu Channel case* (n 43) (Merits) 35 & 36

[61] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (n 36) para 251

[62] David R Johnson & David Post, 'Law and Borders - The Rise of Law in Cyberspace' (1996) 48 Stanford L Rev 1367

[63] *See eg* UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 para 27

[64] *See e*g Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65(4) University of Chicago L Rev 1199; Schmitt (n 94) rule 1

While this interpretation of international law in cyberspace enjoys considerable support amongst scholars,[65] the position of the British government runs very much against it. Consider the expression of the *opinio juris* on the subject matter by the British Attorney General Wright:

> Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.[66]

I cannot agree with this interpretation of the law for a number of reasons. Not only does it go against the traditional understanding of sovereignty and the resulting norms involving the legal consequences outlined above but it has also, to my knowledge, not been supported by any other State or relevant legal scholarship.[67] In fact, Brazil has previously called the American intrusions into its sovereign cyber infrastructure internationally wrongful; they stated that '[a] country's sovereignty can never affirm itself to the detriment of another country's sovereignty'[68], a statement which was critical of American cyber espionage activities against Brazilian president Dilma Rousseff. What is more, in the face of these new circumstances,

---

[65] See eg *Schmitt* (n 34) 21–22, Russel Buchan & Navarrete Inaki, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 Cornell Intl L J 897, 915; Pål Wrange, 'Intervention in national and private cyberspace and international law' in Jonas Ebbesson et al (eds), *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, (Brill/Nijhoff 2014) 322 & 307–326; Sean Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (Just Security, 14 October 2016) <https://goo.gl/pLuad9> accessed 10 August 2019; Mary E O'Connell, 'Cyber Mania' in Mary E O'Connell, Louise Arimatsu, & Elizabeth Wilmshurst (eds), *International Law: Meeting Summary: Cyber Security and International Law* (Chatham House 2012) 3, 6; Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in C Czosseck, R Ottis, K Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (CCD COE 2012) 11–12; Michael N Schmitt & Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas L Rev 1639

[66] *Wright* (n 31)

[67] Two notable exceptions are the contribution by Pirker, noting the violation of sovereignty would only occur if cyber operation amounted to the use of force or intervention (Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCD COE 2013) 199–204); Gary P Corn & Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207)

[68] Julian Borger, 'Brazilian president: US surveillance a "breach of international law"' *Guardian* (24 September 2013) <https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> accessed 11 December 2018

normative value ascribed to the expressions of *opinio juris* in the formation of customary law encourages States to re-interpret old (or suggest new) norms and thus reshape the law in accordance with their interests and capacities. Considering that British offensive cyber capability is soaring[69] and their practice of such actions is widely-reported,[70] it would be reasonable to claim that the provided *opinio juris* is seeking to reshape the law and normalise the behaviour of the State, which is more than capable and willing to realise their geostrategic interests or procure peace and security by means of cyber operations in contravention of the sovereignty of the targeted States. As will be explained in the following chapter, the less restraint on the capable and powerful, the better for them. For less powerful States, on the other hand, international law presents an important framework of protection, providing peace and security. Freeland, Foreign Minister of Canada, argued '[a]s a middle power, Canada has a vital interest in a rules-based order in which might is not always right; in which the world's strongest countries are constrained by standards that are internationally recognised and enforced.'[71] This is perhaps why Canada has not spoken against the existence of the rule of sovereignty in the context of inter-State cyber operations.[72]

Another interpretation of the law of sovereignty in cyberspace argues that not every cyber operation consisting of unauthorised remote intrusion into sovereign cyber infrastructure is a violation of State sovereignty; according to the US State Department legal adviser, not every such act is unlawful, particularly so when '[cyber] activities in another State's territory have no effects'.[73] The theory is further developed and enumerated by the second Tallinn Manual,

---

[69] Intelligence and Security Committee of Parliament, 'Annual Report 2016–2017' (HC655, 20 December 2017) 43–44 <https://goo.gl/nvaqd4> accessed 9 August 2019

[70] 'Britain's GCHQ Hacked Belgian Telecoms Firm' *Der Spiegel* (20 September 2013) <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html> accessed 9 August 2019

[71] Chrystia Freeland, 'The Case for Progressive Internationalism' *The Economist – The World in 2018* (December 2017) 71

[72] Jeffrey Biller & Michael Schmitt, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences' *EJIL: Talk!* (24 October 2018) <ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences> accessed 9 August 2019

[73] Brian J Egan, 'Remarks on International Law and Stability in Cyberspace' (US Department of State, 10 November 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> accessed 9 August 2019

which argues that remote unauthorised intrusions into sovereign cyber infrastructure constitute an unlawful violation of sovereignty when its effects amount to physical damage, loss of functionality or other effects such as 'causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality.'[74] Accordingly, the proponents of this school of thought argue cyber operations, which have no effect on the foreign cyber infrastructure, are a legitimate, lawful State practice. Schmitt, for example, argues cyber operations qualifying as 'monitoring activities in another State may merely constitute espionage, which is not prohibited.'

Buchan and Iñaki have developed a strong argument against this interpretation of the law[75] and I am equally yet to be convinced that only intrusions into the sovereign cyber infrastructure bearing effects on the targeted State constitute internationally wrongful conduct. In addition to the aforementioned Brazilian expression of *opinio juris* contradicting the theory, the understanding of the law of sovereignty in analogous domains other than cyberspace indicates that tangible effects on objects by the sovereign territory are not prerequisites to establishing the violation of international law. Aerial reconnaissance is one such example. Not only has the ICJ argued that American intrusion into the national airspace of Nicaragua violated its sovereignty,[76] but so do recent instances of practice and expressions of *opinio juris* indicate that unauthorised aerial reconnaissance in a national airspace constitutes a violation of territorial sovereignty; 'Israel regards with utmost seriousness any violation of its sovereignty,'[77] protested Israeli Defence Minister in 2017 after a Syrian surveillance drone breached Israeli airspace.

---

[74] *Schmitt* (n 34) 21
[75] *Buchan & Inaki* (n 65)
[76] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (n 36) paras 212 & 292(5)
[77] 'Israel: Military Shot Down Syrian Spy Drone' *VOA News* (11 November 2017) <https://www.voanews.com/a/israel-says-its-military-shot-down-syrian-spy-drone/4110874.html> accessed 3 August 2019

Customary law is indeed in its embryonic state and any definitive conclusion is perhaps premature. Regardless of which school of thought prevails in the future, looking at the issue from a technical or practical vantage point makes me doubtful that remote operations constituting an unauthorised intrusion into sovereign cyber infrastructure can indeed be possible without any sort of effect on the said infrastructure. The alteration of the computer code allows the perpetrator to conduct a cyber operation and forces the targeted computer to perform actions not intended by the manufacturer or the user – send data to remote servers, log and share credentials, open a backdoor for additional malware package installation, turn on the microphone or camera for image and sound recording, etc. Having said this, and no matter the accepted threshold one choses to accept, Shamoon's unlawful character lies in its violation of the sovereignty of Saudi Arabia.

When an inter-State cyber operation interferes with what is essentially the sovereign prerogative of a State *and* does so by way of dictatorial means or by coercion, the cyber operation in question may be classified as an unlawful intervention. The 2007 DDoS operation against Estonia is an example of such.

The Estonian government's decision in 2007 to move the Bronze Soldier Soviet memorial from the centre of its capital to the military cemetery on the outskirts of Tallinn, not only sparked violent street riots but also attracted a negative response in the form of a **DDoS operation** shutting down the websites of all major political parties, government ministries, the parliamentary email server and even the computer network systems of two major banks.[78] The main targets of the operation 'were information distribution channels of both the government and the private sector, and business sector websites, specifically, banks.'[79]

[78] Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4 (2) J of Strategic Security 49 <http://goo.gl/xVf98> accessed 11 August 2018

[79] Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations* (CCD COE 2010) 21

The operation deserves to be labelled as inter-State because both the target and the source of the cyber operation were States. That Russia is *in fact* responsible for the DDoS operation has been widely argued.[80] At the same time, the operation unlawfully deprived Estonia of its international sovereign rights. By 'bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely',[81] which in this particular case means interference with the right of Estonia to decide freely where on its territory to display a war memorial, the 2007 DDoS operation is a clear example of interference with the sovereign prerogatives of Estonia. This argument is reinforced by the clearly expressed displeasure of Russian Foreign Minister Lavrov and Duma with the Estonian policy.[82]

Interference amounts to the prohibited intervention when it uses methods of coercion in regard to choices, which must remain free ones. The element of coercion, which defines and indeed forms the very essence of prohibited intervention,[83] is generally accepted to denote an act of compelling, intimidating, even forcing a sovereign State to pursue an involuntary course of action.[84] If expressions of *opinio juris* indicate no harmony in whether sovereignty is merely a guiding principle or in fact a norm with legal consequences, there is less contention when it comes to intervention; American and British positions have both argued that the traditional understanding of international prohibition of intervention is applicable to cyberspace.[85]

DDoS cyber operations, predominantly a form of politically motivated disruptive interference,[86] certainly fall within the ambit of prohibited coercion. Since the 2007 cyber operation was a

---

[80] *See eg* Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia' *The Guardian* (17 May 2007) <theguardian.com/world/2007/may/17/topstories3.russia> accessed 29 June 2019. *See also* ch 4

[81] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (n 36) para 205

[82] Steven L Myers, 'Russia Rebukes Estonia for Moving Soviet Statue' *New York Times* (27 April 2007) <nytimes.com/2007/04/27/world/europe/27cnd-estonia.html> accessed 11 December 2018

[83] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (n 36) para 205

[84] Joyner, for example, argues coercion 'involves the government of one State compelling the government of another State to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force'. Christopher C Joyner, 'Coercion' in *Max Planck Encyclopedia of Public International Law* (December 2006) para 1 <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749?prd=EPIL> accessed 19 May 2019

[85] *Wright* (n 31); *Egan* (n 73)

[86] Jose Nazario, 'Politically Motivated Denial of Service Attacks' in Christian Czosseck & Kenneth Geers (eds) *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 163

coercive response to the sovereign decision of the Estonian government to relocate the Bronze Soldier statue it may be reasonably argued that it is considered to have amounted to coercion against political independence of the State, and thus a violation of the established international prohibition of intervention.

Although the use of force is a form of prohibited intervention, the 2007 DDoS operation did not amount to a violation of the use of force; no source reports any physical damage to the infrastructure in Estonia. What is more, Goldstein, US Deputy Ambassador to Estonia at the time, reported that experts agreed that the operation was not a serious threat to the integrity of Estonia's cyber infrastructure, which 'was not in any serious danger of being shut down.'[87] In other words, the 2007 DDoS was a cyber operation below the use of force.

Much like the international law of sovereignty protects the cyber infrastructure in a given sovereign territory, international diplomatic law protects diplomatic and consular premises, documents, archives and communication. The violation of these provisions is exemplified by a third unlawful inter-State cyber operation below the use of force in a cyber operation titled **RedOctober**.

For at least five years, RedOctober malware harvested and misappropriated information belonging to the embassies of at least 47 nations in Algeria, Afghanistan, Belgium, Iran, Ireland, Switzerland, US etc.[88] Although technical research yielded no evidence of specific responsibility for the operation, the scope, customised malware, extensive command and control structure are clear indicators that RedOctober was the work of a State.[89]

---

[87] Jeff Goldstein, 'Estonia's Cyber Attacks: Lessons Learned' (Wikileaks, 30 August 2011) para 2 <http://goo.gl/1IOhn> accessed 11 August 2018

[88] Global Research & Analysis Team, '"Red October" Diplomatic Cyber Attacks Investigation' (Kaspersky Lab, 14 January 2013) <securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/> accessed 1 May 2019

[89] *See eg* Kelly J Higgins, '"Red October" Attacks: The New Face of Cyberespionage' (Dark Reading, 14 January 2013) <darkreading.com/attacks-breaches/red-october-attacks-the-new-face-of-cyberespionage/d/d-id/1138972> accessed 1 August 2019; Antonio Teti, 'Operation "Red October": and it is Cyber Espionage' (2013) 1 GNOSIS, L'Agenzia Informazioni e Sicurezza Interna <gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavigE/34-09.pdf/$File/34-09.pdf?openElement> accessed 18 May 2019; Maschenka Braganca, 'Hunt for Red October. The new face of cyber espionage' (2014) 4 SIAK-J (Intl Edition) 87, 90

No physical damage caused by the RedOctober has been reported, which means that it has not reached the threshold of the prohibited use of force. The operation did, however, violate the provisions of international diplomatic law on at last three accounts. '[E]ssential for the maintenance of relations between States'[90] and for the 'efficient performance of the functions of diplomatic missions as representing States',[91] international diplomatic law dictates, *inter alia*, the inviolability of diplomatic premises, documents and archives, as well as correspondence.[92]

First, much like how sovereign rights apply to cyber infrastructure located on a territory of a sovereign nation, inviolability of diplomatic premises applies to the computers and other networked infrastructure located therein.[93] Constituting an unauthorised intrusion into the computerised equipment of several diplomatic missions, the State responsible for RedOctober violated the Vienna Convention on Diplomatic Relations (VCDR), stipulating 'the premises of the mission shall be inviolable'.[94]

Second, the proscription of the inviolability of the diplomatic extends to archives and documents 'at any time and wherever they may be'.[95] The inclusion of the electronic form of documents and archives can be deduced from the wide definitions, provided by the commentary to the ILC Draft articles on Succession of States in respect of State Property, Archives and Debts, arguing that archives refer to 'all documents of *whatever kind*' and documents 'should be understood in its *widest sense*',[96] regardless of their form and material used for their storage. Thus, I see no real reason why archives and documents stored on

---

[90] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* [1980] ICJ Rep para 86

[91] Vienna Convention on Diplomatic Relations (18 April 1961) 500 UNTS 95, preamble

[92] ibid arts 21, 24, 27, respectively

[93] Jovan Kurbalija 'E-Diplomacy and Diplomatic Law in the Internet Era' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCD COE 2013) 415

[94] *Vienna Convention on Diplomatic Relations* (n 91) art 22(1)

[95] ibid art 24

[96] ILC, 'Draft articles on Succession of States in respect of State Property, Archives and Debts with commentaries' (1981) II(II) Ybk of the ILC 50 [emphasis added]

computer servers and removable storage drives, as was in the case of RedOctober,[97] pertaining to a diplomatic entity, would not fall within the scope of the protected archives and documents. Though it is unlikely that diplomatic archives and documents would be stored on a remote server (or on, what the popular discourse designates as, the cloud), '*wherever they may be'* is a clear indication that their inviolability is not awarded on the basis of their location but on the basis of their diplomatic status. Accordingly, since the archives and documents appropriated by the perpetrators of the RedOctober operation were located in embassy computer servers and removable USB storage,[98] the operation was indeed in violation of the provision of the VCDR establishing inviolability of diplomatic archives and documents.

Third, much like archives and documents, international diplomatic law provides that 'all correspondence relating to the mission and its functions'[99] is inviolable. The fact that the perpetrators of the RedOctober operation appropriated locally and remotely stored email correspondence of several of the diplomatic missions[100] states that the operation's unlawful character rests on the violation of the aforementioned proscription enshrined in the VCDR, Article 27.

Since the operation ran contrary to the international rights of the 47 States, it may be classified as an inter-State cyber operation. No physical damage or injury to persons as a result of the cyber operation has been reported, making the RedOctober a cyber operation below the use of force.

---

[97] Teti (n 89) 66
[98] ibid
[99] *Vienna Convention on Diplomatic Relations* (n 91) art 27(2)
[100] Global Research & Analysis Team, '"Red October". Detailed Malware Description 2. Second Stage of Attack' (Kaspersky, 17 January 2013) <securelist.com/red-october-detailed-malware-description-2-second-stage-of-attack/36842> accessed 12 August 2019

2. Solution(s)

States appear to be well aware of the fact that inter-State cyber operations endanger not only their individual security[101] but also the security of the international community. In the words of a Dutch representative to the First Committee of the UN General Assembly, malicious cyber operations 'cause instability in international relations and could present risks for international peace and security.'[102] For this reason, many States have sought to supress the occurrence of internationally wrongful inter-State cyber operations and to maintain peace and security by building their defensive and offensive capacities, by investing in technology-based solutions and through promotion of voluntary norms discouraging the conduct of inter-State cyber operations.

By increasing their national institutional capacity[103] to defend from and respond to cyber threats, States attempt to maintain peace and enhance their national (cyber)security.[104] To achieve this, defensive capabilities are insufficient; accordingly, Panetta, former American Secretary of Defence, acknowledged that '[the US] won't succeed in preventing a cyberattack through improved defences alone.'[105] For this reason, many States have not only invested in the development of their defensive capacity,[106] but also established organisational units

---

[101] See, for example, statement by Kirstjen Nielsen, former US Homeland Security Secretary in Zolan Kanno-Youngs, 'Homeland Security Chief Cites Top Threat to U.S. (It's Not the Border)' *New York Times* (18 March 2019) <https://nyti.ms/2J2oHu0> accessed 29 June 2019> accessed 12 August 2019; Nigeria, 'National Cybersecurity Strategy' (2015) 1.1.3, 1.4.6, 1.5 & 1.6

[102] UN GAOR 1st Committee (71st Session) 'Thematic discussion on specific subjects and introduction and consideration of draft resolutions and decisions submitted under all disarmament and related international security agenda items' (24 October 2016) 15 UN Doc A/C.1/71/PV.19

[103] Examples include establishment of computer emergency response teams (CERTs) or specialised cyber defence bodies such as US Cyber Command and National Guard Cyber Defence Team or UK Joint Cyber Reserve.

[104] British Secretary of the State, for example, argued that '[the] Government is doubling investment in cyber and creating a National Cyber Centre *to help keep us safe*.' Office of the Secretary of State for Wales, 'UK cyber security a top priority for UK Government' (Press Release, 19 November 2015) [emphasis added] <gov.uk/government/news/uk-cyber-security-a-top-priority-for-uk-government> accessed 29 June 2019

[105] Elisabeth Bumiller & Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack' *New York Times* (11 October 2012) <nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html> accessed 3 August 2018

[106] For example, 'GCHQ's allocation of effort to developing offensive cyber capabilities has increased very substantially between 2014/15 and 2015/16.' *Intelligence and Security Committee of Parliament* (n 69) 44

responsible for cyber offence. The US, for one, established the US Cyber Command, a unit of self-proclaimed cyber warriors responsible for improving the security and stability of cyberspace, the success of which is measured 'by the reduction of adversary aggression'.[107] In fact, according to the 2018 Worldwide Threat Assessment of the US Intelligence Community more than thirty nation States have established a form of offensive cyber forces.[108] This statistic does not include nations that chose to outsource the development of their offensive cyber capabilities to non-State organisations.[109] Still, as elaborated by the second chapter of this thesis, reactionary offense has no positive effect on the proliferation of unlawful inter-State cyber operations and may aggravate the situation.

In addition to institutional capacity building, States have also invested in the development of **technology** aimed at prevention and defence against cyber operations targeting national infrastructure. Official statements assert that 'considerable time and attention […] invested in improving the intelligence and science behind attribution'[110] has resulted in a significant increase in the ability to point a finger at the culprits. However, whether such claims have merit or are merely deterrence tactics remains to be seen; US officials, for example, were quick to point out that the '[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their [cyber] actions that may try to harm America',[111] but have presented rather unsatisfactory evidence in support of the attribution of certain State-sponsored or -conducted cyber operations against their infrastructure.[112]

---

[107] US Cyber Command, 'Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command' (20 April 2018) 6
[108] *Coats* (n 3) 5
[109] *See* Tim Maurer, *Cyber Mercenaries – The State, Hackers, and Power* (CUP 2018)
[110] Martin C Libicki, 'It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture' (US House of Representatives, Committee on Armed Services, 1 March 2017) 2 <docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-LibickiM-20170301.pdf> accessed 29 June 2019
[111] Leon E Panetta, 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City' (US Department of Defence, 11 October 2012) <archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> accessed 29 June 2019
[112] *See* ch 4

National cybersecurity is multi-faceted, requiring solutions beyond those of a technical and operational nature. In addition to the aforementioned domestic efforts to shield themselves from malicious cyber operations, States have attempted to act externally and to reduce the number of malicious inter-State cyber operations by establishing and promoting various **voluntary, non-binding norms** which encourage responsible behaviour in cyberspace and therefore introduce some form of order in what is an otherwise chaotic state of inter-State cyber affairs and reduce the frequency of malicious inter-State cyber operations. Notably, China, Russia and several other States jointly introduced the International Code of Conduct for Information Security to the UN General Assembly in 2011[113] and 2015, which was to assure 'peaceful, secure, open [cyberspace] founded on cooperation'.[114] Another example of voluntary binding norms, which gained significantly wider international acceptance was the UN Group of Governmental Experts' (GGE) outline of the norms, rules and principles for the responsible behaviour of States in cyberspace,[115] unanimously adopted by the General Assembly at the very end of 2015,[116] aimed at '[reducing] risks to international peace, security and stability'.[117]

Some authors suggest voluntary cyber norms play a 'prominent role in contemporary international relations',[118] offering a temporary solution to the rise of malicious inter-State cyber operations in the absence of a codified international consensus on the legal matters of cyberspace. While one cannot deny their valuable contribution to the formation of customary international law, or their potential to contribute to peace and security in contemporary

---

[113] UNGA 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (14 September 2011) UN Doc A/66/359

[114] UNGA 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (13 January 2015) UN Doc A/69/723

[115] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General' (22 July 2015) UN Doc A/70/174

[116] UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237

[117] *UN Doc A/70/174* (n 115)

[118] Eneken Tikk-Ringas, 'International Cyber Norms Dialogue as an Exercise of Normative Power' (2016) 17 (3) Georgetown J of Intl Affairs 47, 49

international relations,[119] voluntary norms currently have no perceptible impact on the frequency or the magnitude of malicious inter-State cyber operations.[120] This should come as no surprise. The voluntary nature of norms, a form of 'shared beliefs held within a community',[121] means that their impact cannot stretch beyond that of a gentlemen's agreement. Adherence to the norms depends on 'individual conscience'[122] and on the power of an international community's disapproval to diminish the reputation of the nonconformist States. In particular, the aforementioned UN GGE report confirms that international cyber norms are 'the *expectations* of the international community […] and allow the international community to *assess* the activities and intentions of States'.[123] As elaborated upon in the following chapter of this thesis, a clear conscience and positive international reputation are not strong enough incentives to discourage the rational States from resorting to malicious cyber operations.[124]

In summary, reactions in the form of capacity building, investments in technological advancements and development of voluntary international norms of responsible behaviour in cyberspace have no tangible effect on the frequency of malicious inter-State cyber operations threatening peace and security. In fact, despite all of these efforts, such inter-State cyber operations are **on the rise**. 'We are witnessing an increase in cyberthreats originating from both State actors and non-State actors alike. Such activities have become increasingly

---

[119] Excellent overview of the impact of the voluntary norms on international relations can be found in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System* (OUP 2013)

[120] Charlie Mitchell, 'Panel: Still no sense of consequence for violating cyber 'norms' of behaviour' (Inside Cybersecurity, 9 August 2018) <insidecybersecurity.com/daily-news/panel-still-no-sense-consequence-violating-cyber-'norms'-behavior> accessed 12 August 2019; Francesca Casalini & Stefania Di Stefano, 'State behaviour in cyberspace: a new challenge for the international community' (Diplo Foundation, 12 March 2018) <diplomacy.edu/blog/state-behaviour-cyberspace-new-challenge-international-community> both accessed 29 June 2019

[121] Martha Finnemore, 'Cybersecurity and the Concept of Norms' (Carnegie Endowment for International Peace, 30 November 2017) <carnegieendowment.org/files/Finnemore_web_final.pdf> accessed 11 June 2018

[122] Onuma Yasuaki, 'International Law in and with International Politics: The Functions of International Law in International Society' (2003) 14(1) EJIL 105, 123

[123] *UN Doc A/70/174* (n 115) 7

[124] On why the reduction of international reputation is not enough to discourage the States to cease with the malicious cyber operations *see* ch 2.

targeted, complex and sophisticated'[125] warned the Swiss representative at the UN General Assembly 1st committee.

Empirical data confirms this. Out of the aforementioned 220 known malicious State-sponsored or -conducted cyber operations in the last 11 years, no less than 40 occurred in 2017, more than any year before.[126] What is more, it seems the trend will persist in the foreseeable future; according to the US authorities' official assessments of the 2018 threat landscape '[t]he risk is growing that some adversaries will conduct cyber attacks – such as data deletion or localised and temporary disruptions of critical infrastructure – against the United States in a crisis short of war'.[127]

Another solution to the proliferation of inter-State cyber operations, the one explored in detail in this thesis, is international law with its ability to restrict the selfish pursuit of power resources and to provide peace and security. In accordance with the theory of compliance elaborated upon in the following chapter, the basic nucleus of the anarchical international community is represented by a rational, self-interested State, primary interest of which is its security or survival. Accordingly, reducing the security of an adversary by way of cyber operations is merely a way of maximising the relative power of the State behind the malicious cyber operation and a self-centred act of survival. Historically, modern society has sought to limit the selfish maximisation of power and consequential decrease of security through the development and promotion of **international law**, the framework of rights and obligations of sovereign States uniting humanity in an effort to promote peace and cooperation, to establish, strengthen and re-establish international peace and security.[128] In the context of realism, international law traditionally restricts selfish maximisation of power and seeks to deliver

---

[125] *UN Doc A/C.1/71/PV.19* (n 102) 17. Note also similar statement by the Dutch representative: 'States and other actors are increasingly using cyber operations to pursue their strategic interests, not just for military purposes, but for coercive political purposes as well' ibid 15.
[126] *Council on Foreign Relations* (n 5)
[127] *Coats* (n 3) 5
[128] See eg *Charter of the UN* (n 17) preamble; UNGA Res 25/2625 (24 October 1970) UN Doc A/RES/25/2625. *See also* ch 2.

security by providing peace. As I explain in the following chapter, international law represents a normative framework of rights and responsibilities, enabling peaceful and orderly interaction between civilised nations united in a common goal – security. It provides a 'standard of conduct in the normal relations between nations',[129] by imposing limitations on rationality of members of the international community. As such, '[international] law stems from the human desire for society – not for society of any sort, but for peaceful and organised life according to the measure of his intelligence.'[130]

Unfortunately, there are currently no universally accepted special agreements outlining the international legal restrictions on the maximisation of power by way of cyber operations. There are no universally accepted agreements on the international law specifically governing inter-State cyber operations or the consequences of State responsibility flowing from the violation thereof. The prospects of a specialised, black-letter international legal regime, or a Treaty for Cyberspace[131] if you will, also appear bleak in 2019.

On paper, there is no lack of interest for such a new regime. The US representative at the UN GGE Markoff promoted the need of the international community to affirm that 'international law provides States with binding standards of behaviour that can help reduce the risk of conflict [in cyberspace]'.[132] Russia has also advocated for an international treaty regulating State behaviour in cyberspace.[133] The reason why no such attempts have come to fruition likely lies

[129] William W Bishop Jr, 'The Role of International Law in a Peaceful World' in Joseph J Norton (ed), *Public International Law and the future World Order* (F.B. Rothman 1987) 1–3
[130] Hersch Lauterpacht, 'The Grotian Tradition in International Law' (1946) 23 British Ybk of Intl L 1
[131] Rex Hughes, 'A Treaty for Cyberspace' (2010) 86(2) Intl Affairs 523–541
[132] Michele Markoff, 'Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (US Mission to the UN, 23 June 2017) <usun.state.gov/remarks/7880> accessed 11 February 2018
[133] John Markoff & Andrew E Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace', *New York Times* (27 June 2009) <nytimes.com/2009/06/28/world/28cyber.html> accessed 29 June 2019

in the highly politicised debate[134]fuelled by ideological differences[135] and the preference of powerful States to rely on their own cyber capacity rather than on international law to provide peace and security.[136]

This is also why the agreements among States are limited to non-binding norms of State behaviour in cyberspace. And even those attempts only enjoy limited support by the States; after issuing several consensual reports outlining the non-binding norms of responsible behaviour and applicable principles of international law to cyberspace, the latest functional UN GGE failed to reach an agreement and faced dissolution.[137]

For the above reasons, this thesis seeks a solution to the increase in malicious cyber operations threatening peace and security in the established international law. It disassociates itself from the proponents of an urgent need for a new cyber-specific international legal regime.[138] Instead, it establishes that there is no such thing as a legal vacuum in cyberspace and investigates how existing international law restricts the contemporary peace- and security-eroding behaviour of States in cyberspace.

The technological revolution, as disruptive as it is, has not altered the objective of the law nor has it diminished the legitimacy of established international legal obligations. The objective of international law remains focused on peace and security and is still 'essential to maintaining

---

[134] Michael Schmitt & Liis Vihul 'International Cyber Law Politicised: The UN GGE's Failure to Advance Cyber Norms' (Just Security, 30 June 2017) <justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> accessed 29 June 2019

[135] Oleg Khramov, Russian Security Council Deputy Secretary, stated: 'Russian attempts have been chastised by a number of leading Western states, and politicians have succumbed into years of fruitless discussions in which the objectivity has been replaced by ideological goals'. *Cited in* Ann Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly' (CCD COE, 1 September 2017) <ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html> accessed 7 November 2017

[136] *See* ch 2; Efrony and Shany, for example, argue States have 'limited interest in promoting legal certainty regarding the regulation of cyberspace.' Dan Efrony & Yuval Shany, 'A Rule Book in the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) AJIL 583, 585.

[137] Eneken Tikk & Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy' (Cyber Policy Institute 2017) <cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf> accessed 3 August 2019

[138] *See eg* Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harvard Intl L J 179

peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment,'[139] states the report submitted to the UN General Assembly by the Group of 25 Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2015. Similar assertions may be found in various individual national cybersecurity strategies. The Government of Japan, for example, pledged to 'take the initiative in implementing international rules and norms and subsequently make contributions to the establishment of the rule of law in cyberspace [in order to] bring *peace and stability to the international community*'.[140]

Also, international law generally remains a legitimate social order in the new era, undoubtedly considered to be 'obligatory or exemplary'[141] in relation to the activities of States in cyberspace. Writings of the most prominent scholars[142] and, more importantly, pronouncements of the States confirm this assertion; the American International Strategy for Cyberspace, for instance, explains that the introduction of cyberspace does not necessitate 'a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behaviour—in times of peace and conflict—also apply in cyberspace'.[143]

---

[139] *UN Doc a/70/174* (n 115) para 24 [emphasis added]

[140] Government of Japan, 'Cybersecurity Strategy' (4 September 2015) 38–39 [emphasis added]. Note also similar statements made by *Wright* (n 31): 'International law must remain relevant to the challenges of modern conflicts if it is to be respected, and as a result, play its critical role in ensuring *certainty, peace and stability* in the international order' [emphasis added]; *and* President of the United States, 'International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World' (May 2011) 8–11, where US vowed to promote stability, therefore peace or absence of commotion, in cyberspace through development of norms of responsible behaviour.

[141] Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (Guenther Roth & Claus Wittich (eds), University of California Press 2013) 19 & 31

[142] See eg *Roscini* (n 28) ch 1

[143] *President of the United States* (n 140) 9. Also, note the position of Japan, which is 'of the view that existing international law applies to cyberspace'; 'the rule of law should be thoroughly attained to cyberspace in the same way as it is applied in physical space.' (*Government of Japan* (n 140) 38 and 8 respectively); the position of China: 'The governance of cyberspace should follow the existing principles of international law and the basic norms of international relationships enshrined in the Charter of the United Nations, such as sovereign equality, non-interference in internal affairs, non-use of force, the peaceful settlement of disputes and the fulfilment of international obligations in good faith' (*UN Doc A/C.1/71/PV.19* (n 102) 22); conclusion of the 2013 UN GGE (UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98, para 19); and conclusion of the 2015 UN GGE (*UN Doc A/70/174* (n 115) para 24)

In order to be effective in supressing malicious cyber behaviour and therefore live up to its promise of peace and security, the law must be complied with. Only compliance of the subjects of law will provide the individual States and the international community with peace and security.[144] For this reason, the central question this thesis seeks to answer is **how can the established international legal mechanisms reduce non-compliance with international law in cyberspace and thus restore peace and security of individual nations as well as the international community?**

To answer this question, this thesis investigates the potential of countermeasures for the violation of the due diligence obligations of prevention and termination, to allow the injured State to restore the power relationship and thus induce compliance with international law of the State *in fact* responsible for the unlawful inter-State cyber operation.

3. Methodology, originality and utility of the thesis

3.1. Methodology

Tasked to find a solution and to uncover the ability of international law to supress unlawful inter-State cyber operations below the use of force, this thesis cannot neglect the technical aspect of the issue at hand. Accordingly, besides the international relations inspired theory of compliance that explains why States choose to disregard their international legal obligations, this thesis regularly points to lessons from computer science research. To an extent, this methodological approach is a distinct advantage of this research vis-à-vis other relevant legal scholarship. Careful consideration of the computer science underpinning the rising non-compliance with international law in the cyber era is imperative to understand the nature and extent of the problem and therefore necessary to be able to propose a viable solution.

[144] *See* ch 2

First and foremost, however, the primary methodological approach is the doctrinal investigation of international law. This thesis scrutinises different sources of international law, namely the primary obligations of the developing cyber-specific customary international law, the primary obligations stemming from the analogous and dynamically-interpreted traditional customary and treaty law applicable to inter-State cyber operations, as well as the secondary obligations of the customary international law of State responsibility, applicable in the event of violation of the primary rules. The analysis of these sources is augmented by an examination of the relevant general principles of law, jurisprudence and writings of the most prominent scholars.

Due to the aforementioned absence of a discrete treaty law, the main source of primary obligations in inter-State cyber relations and the first source of law scrutinised by this thesis is the developing cyber-specific international customary law. As is already apparent from the paragraphs above and without a doubt evident in the following chapters, the scope of State practice and *opinio juris* indicating the development of a specific customary international law in cyberspace is not extensive. While practice does exist, it cannot be claimed to be widespread and consistent, which is a recognised requirement of an established rule of international law.[145] Thus, at the time of drafting the present text, a customary body of law specific to conduct in cyberspace cannot yet be considered as fully formed. Although the passage of a certain amount of time is not a legal requirement for a customary norm to arise,[146] the formation of the law is more likely to occur over an extended period of time. In spite of its infancy, the cyber-specific customary law development trajectories are evident and presented throughout the thesis.

---

[145] Hugh Thurlway, 'The Sources of International Law' in Malcolm D Evans, *International Law* (2nd edn, OUP 2006) 124

[146] '[T]he passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law.' (*North Sea Continental Shelf* Cases (*Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands)* (Judgment of 20 February 1969) [1969] ICJ Rep para 74 para 74)

For now, the trends of the developing customary law are identified in expressions of *opinio juris* found in news sources, official reports, testimonies of officials, opinions of official legal advisers, national cyber security strategies and other relevant policy documents. Indeed, for now, 'legal evolution is likely to occur in significant part through defensive planning doctrine and declaratory policies'.[147] Documents and resolutions of international organisations, another recognised source of *opinio juris*,[148] will also be consulted to uncover the developing customary law. Additionally, in an attempt to identify the current and future State practice, the research will consult the abovementioned sources and other similar documents which are generally[149] accepted as a form of State practice, particularly so when the State conduct is shrouded in secrecy.[150]

Although this chapter has previously argued that the non-binding norms of responsible behaviour in cyberspace have no immediate tangible effect on the proliferation of inter-State cyber operations threatening peace and security, the role of so-called soft law in formation of customary law should not be neglected. As Finnemore and Hollis argued, 'the real power of norms (and much of their attraction as a regulatory tool) lies in the processes by which they form and evolve'.[151] Thus, the States which will decide to comply with non-binding norms in fear of the possible stigmatisation by the international community and the consequential loss of international reputation will inevitably aid in the formation of the customary law by way of their practice.

---

[147] Matthew C Waxman, 'Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions' (2013) 89 Intl L Studies, 109, 116

[148] See *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* paras 184,188 & 191; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep para 73; *Libyan American Oil Company (LIAMCO) v Government of the Libyan Arab Republic* [1982] 62 ILR 141, 189

[149] ILA Committee on Formation of Customary (General) International Law, 'Statement of Principles Applicable to the Formation of General Customary International Law' (Final Report of the Committee, London Conference, 2000) 14

[150] *Prosecutor v Duško Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995) para 99

[151] Martha Finnemore & Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 (3) AJIL 427

The fact that traditional international law applies to State conduct in cyberspace has already been established. The main issue, however, is to establish how it applies. Because the law is in the slow lane[152] and the traditional law precedes the cyber era, the research will resort to the customary interpretation rules,[153] namely: seeking the intent of the law, the ordinary meaning of terminology and subsequent practice of States[154] in order to establish how the traditional law applies to the modern reality.

An equally important part of this thesis are the secondary obligations of the law of State responsibility, arising in the event of violation of the primary rules of international law. Similar to the primary rules of the international law, States have recognised the applicability of the law of State responsibility in the event of unlawful cyber operations.[155] Much like the UN Charter does not discriminate between different weapons amounting to a violation of the use of force,[156] secondary rules of the law of State responsibility automatically arise upon the commission of any conduct in violation of the primary rules of international law, regardless of the methods employed by the wrongdoing State.[157]

While considering the law of State responsibility, I largely rely on the ILC's codification of the customary law laid down in the Articles on Responsibility of States for Internationally Wrongful Acts. Although the codification is, strictly speaking, not a binding international legal framework,

---

[152] Roger Brownsword, 'An Introduction to Legal Research' <http://www.scribd.com/doc/14260230/An-Introduction-to-Legal-Research#scribd> accessed 17 August 2018

[153] ILC, 'Report of the International Law Commission: Sixty-fifth session' (6 May–7 June and 8 July–9 August 2013) UN Doc A/68/10, 11

[154] Vienna Convention on the Law of Treaties (Vienna, 23 May 1969) 1155 UNTS 332 arts 31 & 32

[155] *See eg* Council of the European Union, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption' (Brussels, 7 June 2017) 9916/17, 5 <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> accessed 17 May 2019. *See also* ch 3.

[156] *Legality of the Threat or Use of Nuclear Weapons* (n 148) para 39

[157] *See, e.g.* James Crawford, 'State Responsibility' in *Max Planck Encyclopaedia of Public International Law* (September 2006) para 1 <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093?rskey=dfuWu4&result=1&prd=EPIL> accessed 17 January 2019

it has been endorsed by the UN General Assembly and is frequently relied upon by the international and national judiciary entities,[158] reaffirming its customary status.

In order to determine the options offered by international law to a State injured by a malicious cyber operation and therefore fully elaborate a solution to the rising occurrence of unlawful inter-State cyber operations, one must first understand why States resort to unlawful cyber operations. This is explained by the compliance theory based on the rational choice theory in the second chapter of this thesis.

3.2. Structure of the thesis

Following the elaboration of the rational choice theory of compliance with international law and the conclusion that the inflation of the costs of non-compliance is necessary to restore peace and security in cyberspace, the third chapter compares various compliance inducing measures provided by the international law of State responsibility and makes a case for countermeasures.

The fourth chapter considers the application of countermeasures in the context of inter-State cyber operations in violation of international law and presents a number of unsurpassable obstacles an injured State is likely to encounter when attempting to lawfully inflate the costs of the State behind an unlawful cyber conduct.

For this reason, the fifth chapter proposes a reconsideration of the unlawful character of inter-State cyber operations, which can be characterised not only as unlawful conduct but also as unlawful omission of diligent prevention and termination of acts injurious to another State. The chapter presents the due diligence obligations in cyberspace, their content, scope and the relevant international standards.

---

[158] 'Materials on the Responsibility of States for Internationally Wrongful Acts' (2012) 25 United Nations Legislative Series UN Doc ST/LEG/SER B/25, II–VIII

Under these circumstances, chapter six revisits the objective of the fourth chapter and investigates the inflation of the costs of non-compliance through the application of countermeasures, although this time on the basis of international responsibility for non-diligent behaviour occasioning a cyber operation injurious to the other State.

The concluding chapter provides a summary and a critical assessment of the arguments advanced in this thesis. It exposes the benefits and the limitations of the promoted theoretical solution to the rising non-compliance with international law in the cyber era.

3.3. Originality and utility

This thesis is original in number of ways. Aside from the advantage of using a methodological approach that embraces computer science, the thesis develops a unique rational choice theory of compliance with international law, accurately reflecting the state of international affairs in the 21st century and explaining why States decide to violate international law by way of cyber operations. In this context, it argues that countermeasures are the only viable and potentially effective compliance inducing mechanism under the given theoretical circumstances.

Secondly, the thesis proposes an innovative method of overcoming the issues preventing injured States from inducing compliance by way of countermeasures in reaction to internationally wrongful inter-State cyber operations. It explains how a State injured by a cyber operation can induce compliance of the non-diligent State, not only with the obligations to diligently prevent or terminate internationally wrongful cyber operations, but also with the obligations violated by the operation *in fact* sponsored or conducted by the non-diligent State.

Finally, the originality of the thesis is reflected in the extensive exploration of the principle of due diligence and the resulting obligations of prevention and termination, including the content and the legal standards of these obligations in cyberspace. The arguments are supported by a wealth of *opinio juris* and State practice examples.

All these aspects contribute to a unique solution to the problem presented at the beginning. It is hoped that the arguments presented in this thesis will be of interest and of use to a wide audience. I hope that legal scholars find it stimulating in their research of inter-State cyber operations below the use of force, of the international law of countermeasures, and of the due diligence obligations of prevention and termination in cyberspace. I hope this thesis will encourage also the international community to continue recognising the due diligence obligations in cyberspace and their potential to contribute to mutual international assurance in the modern interconnected world, where egoistic non-compliance with the international legal obligations is no longer a sustainable security maximisation tactic. Above all, this thesis is addressed to the operators of law, that is, the decision makers of the States injured by the unlawful and non-forcible State-sponsored or -conducted cyber operation. From its very beginning, the aim of this research project is to prove that the specific technological developments have not rendered existing international law obsolete and that it can indeed provide a useful self-help framework to the injured party in a cyber conflict. I hope the conclusions of this thesis will encourage the injured States to take lawful action against the rational power-maximising States and thus dissuade the latter (and others) from selfishly diminishing its relative power and eroding the rule of international law.

Chapter 2

International law, compliance and the rational choice theory

1. Introduction

Generally speaking, international law matters and is most of the time complied with.[1] Be that as it may, there is no denial that deviations do occur. As indicated by the previous chapter and by the oft-reported examples of unlawful inter-State cyber operations, violations of international law in cyberspace are not uncommon. Although the application of international law and its normative restrictions on operations in cyberspace have largely been explained by the scholarship, no comprehensive exploration has been attempted to understand the reasons behind the deviant behaviour of States in this context. This chapter attempts to rectify this and elaborate as to why States choose to disregard their international obligations in cyberspace.

To this end, the chapter is structured as follows. The first part argues that the anarchical nature of the international society encourages selfish, egoistic behaviour of States. Due to this competitive anarchy, the primary concern of States is security, their survival and self-preservation, which is provided by State power and/or peace. Peace, offered by international law, comes at the costs of constraints on the maximisation of power.

The second part explains how the anarchical environment, the desire for ultimate security and the enabling new technology provide States with temptation to violate international law.

---

[1] *See eg* Louis Henkin, *How Nations Behave: Law and Foreign Policy* (Council on Foreign Relations 1979); Anthony D'Amato, 'Is Law Really "Law"?' (1984) 79(5 & 6) Northwestern University L Rev 1293, 1304; Leo Gross, 'States as Organs of International Law and the Problems of Auto-interpretation' in George A Lipsky (ed), *Law and Politics in the World Community* (University of California Press 1953) 64: it is commonly accepted 'States by and large obey international law'.

The third section argues that rational and selfish States will choose to disregard their international obligations when a unilateral disregard of the normative constraints brings a positive cost benefit calculous.

In the last part, the chapter explains that benefits of unlawful cyber operations and the resulting ultimate security are nothing but a mirage. In order to restore the initial power relationship and the level of security it enjoyed prior to the unlawful act, an injured State will respond with a breach of its international obligations. Other States are likely to follow suit, which will eventually lead to the deterioration of the international norms in the specific context, inability of law to provide peace and the consequential decline of security for all members of the international society.

2. Interests of the rational egoists in an anarchical society

While there is no denial that this thesis is of a legal nature, one must seek the theoretical foundations beyond the law. Of course, law is 'generated by politics';[2] in the case of international law that would be international politics. In an effort to explain the role of public international law and State responsibility in the cyber era I resort to exploiting the wealth of theories in international relations; for it is international relations literature that provides answers to what motivates States' behaviour, including the decision to comply or not comply with the provisions of international law. Engagement with the international relations literature 'reminds us that international political forces affect State behaviour including in matters of international law'.[3]

Three assumptions underline the following theoretical framework; States, operating in an anarchical international society, are egoistic and rational. This **anarchical society**[4] is characterised by the superiority of the concept of sovereignty and, consequentially, the lack

[2] Nigel White, *The law of International Organisations* (2nd edn, Manchester University Press 2005) 3
[3] Andrew T Guzman, *How International Law Works: A Rational Choice Theory* (OUP 2010) 216
[4] Hedley Bull, *The anarchical society: A study of order in world politics* (3rd edn, Palgrave 2002) 25–30

of an overarching political or enforcement authority. Albeit plagued by a poorly chosen term,[5] anarchy is considered to be 'the fundamental fact of international relations'.[6] It is this very absence of a central authority which allows for the ultimate respect for the independence, sovereignty and unique cultural identities of different States. Those arguing that the UN or the Security Council may effectively assume the role of the world government[7] should look no further than article two of the UN Charter explicitly proclaiming that the 'Organisation is based on the principle of the sovereign equality of all its Members'.[8]

This anarchy dictates **egoism**. Every action of the State serves the attainment of its selfish agenda. This egoistic pursuit of national interest denotes that State policies guiding its international behaviour patterns are 'designed to promote demands that are ascribed to the nation rather than to individuals, subnational groups, or mankind as a whole. It emphasises that the policy subordinates other interests to those of the nation'.[9] It is this preference of self-interest over the interest of the international society as a whole that allows for survival. Addressing the UN General Assembly in 2017, US President Trump reminded us this is not an outdated Cold War mindset: 'As president of the United States, I will always put America first. Just like you, as the leaders of your countries, will always and should always put your countries first'.[10]

The lack of a central authority indeed makes this world a dangerous place. Thus, **security**, enabling self-preservation or survival is a core and consistent motive of States in the

---

[5] The definition of *anarchy* indicates the state of lawlessness. By labelling international society as anarchical one implies it is a primitive society. Which certainly is not true. See more on that below and, for example, Anthony D'Amato, 'Is International Law really "Law"?' (1985) Northwestern University L Rev 1293; Onuma Yasuaki, International Law in and with International Politics: The Functions of International Law in International Society' (2003) 14(1) EJIL 105

[6] Robert Art & Robert Jervis, *International Politics: Enduring Concepts and Contemporary Issues* (Pearson Education 2016) 7

[7] David L Bosco, *Five to Rule Them All: The UN Security Council and the Making of the Modern World* (OUP 2009) 47

[8] Charter of the UN (San Francisco, 26 June 1945) art 2(1)

[9] Arnold Wolfers, '"National Security" as an Ambiguous Symbol' (1952) 67(4) Political Science Quarterly 481, 481

[10] Andrew Buncombe, 'Donald Trump's explosive UN speech: Read it in full' *The Independent* (19 September 2017) <independent.co.uk/news/world/americas/us-politics/trump-un-speech-read-in-full-transcript-north-korea-general-assembly-a7956041.html> accessed 9 August 2019

competitive, international game of politics.[11] States in an anarchic 'constellation must be, and usually are, concerned about their security from being attacked, subjected, dominated, or annihilated by [others]'.[12] Though the notion of security may be contested, it generally denotes absence of (the fear of) internal and external threats to the State.[13] The concept is not limited to the threats of force. Statesmen, to whom security is entrusted by the social contract, will therefore seek security of all the components of the modern State – territory, people, governmental and legal institutions, as well as its sovereignty. The primary concern of this chapter is the security of various State elements from outside threats.

Some authors would have us believe that the primary concern of the State in an anarchical society is a struggle for power but even Morgenthau, one of the most prominent authors who sought to advance the power theory of international relations, was well aware of the fact that power is not the ultimate goal of States.[14] '[I]nternational politics is too serious business for that'[15] concurs Watlz. The fact that security is the primary concern of a State, is supported by the sciences other than international relations or law. Even though the language of this thesis often personifies the State, the State is a social construct, a community of people, acting through the medium of a national legal order. So, the description of the behaviour of the State is essentially the description of the deeds of people – statesmen, lawmakers and generally anyone in a position to steer the conduct of the State in the international setting. If they do so in the name and for the benefit of their people, an affirmation of the superiority of security can be found also in the science of psychology – Maslow's theory of human needs puts safety on the very top of human psychological needs.[16]

---

[11] Kenneth N Waltz, 'Realist Thought and Neorealist Theory' (1990) 44(1) J of Intl Affairs 21, 36. *See also* Avril McDonald & Hanna Brollowski, 'Security' in *Max Planck Encyclopedia of Public International Law* (May 2011) <https://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e399?rskey=321VIt&result=1&prd=EPIL> accessed 19 May 2019

[12] John Herz, 'Idealist Internationalism and the Security Dilemma' (1950) 2(2) World Politics, 157, 157

[13] *See eg* Arnold Wolfers, *Discord and Collaboration Essays on International Politics* (Johns Hopkins Press 1962), 150; *McDonald & Brollowski* (n 11)

[14] Hans J Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (McGraw-Hill 1993) 29

[15] Kenneth Waltz, *Theory of International Politics* (Waveland Press 2010) 127

[16] Abraham H Maslow, 'A Theory of Human Motivation' (1943) 50 Psychological Rev 370, 376

In this struggle to attain security, States behave **rationally**. It is assumed that security as a preference is universal and constant[17] and that States 'calculate costs and benefits of alternative courses of action in order to maximise their utility in view of those preferences'.[18] In other words, States pursue actions which pay off. This defines their attitude towards international law; the rational choice theory can explain why States comply and why they violate international law.

Security is attained by means of power and peace. The first part of this chapter focuses on the elaboration of the two preferences while the second part explains their interdependencies and the maximisation calculations of the rational States.

2.1. Security is attained by means of power

Although it may be true that the ultimate goal is security, power is the currency of international politics; competitive 'calculations about power lie at the heart of how States think about the world around them'.[19] States seek maximisation of their power resources as a means to security. While power resources may not guarantee security, they are essential for attaining security. And cyber operations have become an important tool for their maximisation.

Power is a resource of a State, representing 'specific assets or material resources that are available to a State'.[20] The assessment of State power therefore depends on quantitative indicators such as gross national product, the size and equipment of their armed forces, the size of the population and territory as well as other, harder to quantify indicators such as social stability, quality of government and diplomacy, international reputation etc. It is generally measurable[21] in absolute as well as relative terms. States maximise their power directly or

---

[17] For an insight in preferential consistency *see eg* Scott Burchill, *The National Interest in International Relations Theory* (Palgrave Macmillan UK 2005) 27

[18] Robert O Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton University Press 2005)

[19] John J Mearsheimer, *The Tragedy of Great Power Politics* (WW Norton 2001) 17

[20] ibid 57

[21] *See* Ashley J Tellis et al, *Measuring National Power in the Postindustrial Age* (Rand 2000) ch 3

indirectly – through actions which increase their power or actions which decrease the power of the adversaries, respectively. To cause damage to a State is to increase the relative power of the other States.

Striving to attain security, States 'are driven to acquire more and more power in order to escape the impact of the power of others.'[22] This is, to a certain degree, inevitable. Humankind is driven by progress and the advancement of knowledge, which naturally leads to the increases of the State power, be it military, economic or political. But how much power is enough to secure the nation from a foreign threat? Mearsheimer argued States aim for the top – 'the ultimate goal of the great powers […] is to gain hegemony, because that is the best guarantor of survival' – but was also quick to admit that '[i]n practice, it is almost impossible for any country to achieve global hegemony'.[23] If hegemony is not possible – and it certainly is out of reach for great majority of the States on this planet – the more power the better.

A wealth of power resources, however, does not guarantee security. Power as a resource is nothing without a successful conversion strategy or successful projection which would achieve the desired goal in particular circumstances or, in the context of this thesis, security. By all means, the United States is considered to be the most powerful country in the world. In terms of power resources, that is. It is (one of) the world hegemon(s), if you like. Yet, the events of 11th of September 2001 have demonstrated that power in terms of capacity is not enough for national security. Speculation would suggest the American strategy in employing this power was inadequate to prevent the devastating terrorist attack.

To delve into the wealth of conversion or power projection strategies would be an overly ambitious task for a chapter. Though operations in cyberspace may very well be a convenient and cheap instrument of power projection – think of the potential of spreading various forms of soft power through the Internet or a cyber-attack in the context of military operations – this

---

[22] John H Herz, 'Idealist Internationalism and the Security Dilemma' (1950) 2(2) World Politics 157, 157
[23] John J Mearsheimer, 'Structural Realism' in Tim Dunne, Milja Kurki, Steve Smith (eds) *International Relations Theories* (OUP 2010) 83

thesis focuses on the analysis of cyber operations as a function of maximisation of national power resources.

The contextual relativity of power resources and above-mentioned issues surrounding the conversion led certain scholars[24] to diminish the importance of power resources. Nevertheless, accumulation of power resources, either through cyber or any other means, is vital in the pursuit of security for two reasons.

Firstly, it is important to note that a good projection strategy is **nothing without a power resource**. To utilise the analogues language of Nye and Baldwin, winning cards at a game of poker may not guarantee the player to win but sure are a great advantage in the pursuit of the ultimate goal – domination. In the context of international relations, a sizable army (as a military power resource of a State) may not guarantee security, but certainly does hold a potential for a successful military power projection to attain security (defend the incoming armed attack by the neighbouring State, for example). The bigger the army, the greater the possibility of successful military power projection and, consequentially, security.

This argument extends beyond the considerations about military power. Countries with large GDPs, for example, have greater potential to successfully attain security through the projection of their economic power than States with a smaller GDP. A country of great wealth may use their financial resources for the projection of soft power and to secure its sovereignty, cultural values or even the primacy of its relative economic power. As Keohane puts it '[w]ealth is an absolutely essential means to power, whether for security or for aggression'.[25]

The US' Economic Cooperation Act of 1948[26] (known also as the Marshall Plan) is a fitting example supporting the assertion. After the Second World War devastated the continent, the

---

[24] *See eg* David Baldwin, 'Power and International Relations' *in* Walter Carlsnaes, Thomas Risse & Beth A Simmons (eds), *Handbook of International Relations* (SAGE 2002); Joseph Nye, *Bound to Lead: The Changing Nature of American Power* (Basic Books 1991) 26; Joseph Nye, *The Future of Power* (Hachette UK 2011) 240

[25] *Keohane* (n 18) 22

[26] S 2202 Economic Cooperation Act of 1948, 80th US Congress (2nd Sess, Ch 169, 3 April 1948) <legisworks.org/congress/80/publaw-472.pdf> accessed 24 February 2019

US offered unprecedented financial aid for the reconstruction of Europe. By way of this financial instrument, the US was thus able to convert its considerable economic power resources into security; a State with a significantly lesser economic power would not be able to do so. In the wake of the Cold War, the aim of the Marshall Plan was to secure the US from the growing threat of the communist Soviet Union and inhibit its influence in Western Europe.[27] Its aim was also to secure the American values and proliferate the free economy market; 'through economic, financial, and other measures necessary' the aid was intended to ensure 'the maintenance of conditions abroad in which free institutions may survive and consistent with the maintenance of the strength and stability of the United States'.[28] Considering that the US is the largest trading partner of the EU in 2016,[29] the projection can be labelled as successful.

Secondly, the possession of power resource provides security through **deterrent** function. Admittedly, the terrorist attack of September 11th (or any other terrorist attack for that matter) may not be the best example here. Impressive military power did not guarantee security for the US. But then again, one cannot argue terrorism activities are rational much as the States are. What one can maintain with a large degree of confidence is that no rational State will descend on the US with its current relative military power resources. State power resources therefore offer security in its role as a deterrent and may not need to be employed at all. 'We do not seek the progress of the defence industry for conquest and domination over other countries' former Iranian president Ahmadinejad said, as he rationalised the development and installation of new military hardware, 'rather, deterrence is our objective'.[30] Similarly, US

---

[27] US Department of State, 'The Truman Doctrine and the Marshall Plan' (*Office of the Historian*) <history.state.gov/departmenthistory/short-history/truman> accessed 24 February 2019

[28] *Economic Cooperation Act of 1948* (n 26) preamble

[29] European Commission, 'Client and Supplier Countries of the EU28 in Merchandise Trade' (Trade-G-2, 21 September 2018) <trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf> accessed 24 February 2019

[30] MNA, 'Iran unveils upgraded missile, five pieces of military hardware' *Mehr News* (21 August 2012) <en.mehrnews.com/news/52172/Iran-unveils-upgraded-missile-five-pieces-of-military-hardware> accessed 24 February 2019

Secretary of Defence Ash Carter spoke of the nuclear arsenal: 'America's nuclear deterrence is the bedrock of our security'.[31]

Economic power may very well act as a deterrent as well. For example, a small, poor State would be reluctant to impose a trade embargo on produce from a wealthy State with strong purchasing power. Economic power would, in this context, offer security to the stronger of the two. Indeed, States with lesser economic power resources rarely impose trade embargos against the stronger parties. And when they do, they are usually unsuccessful. A comprehensive historical analysis of trade embargos indicates that the country imposing them is usually economically much more powerful than the target. In most of the analysed cases, the GDP of the State imposing the trade embargo was ten times greater than that of the targeted State. What is most important is that in many instances when the difference in GDP between the States was less than tenfold, embargos proved to be futile.[32]

States maximise their power resources by, *inter alia*, expanding their military arsenal, by waging wars, by investing in education, research and development, through good governance, international trade and diplomacy. More importantly, States also complement their power-maximisation efforts by conducting (unlawful) inter-State cyber operations. China, for one, has been regularly accused of conducting cyber operations against foreign private and public entities for its economic gain,[33] which undoubtedly complements its top national priority – economic growth.[34] The following paragraphs offer a number of examples of unlawful inter-State cyber operations and identify their power maximisation effects.

---

[31] Ash Carter, 'Remarks on "Sustaining Nuclear Deterrence"' (*US Department of Defence*, 26 September 2016) <defense.gov/News/Speeches/Speech-View/Article/956630/remarks-on-sustaining-nuclear-deterrence/> accessed 24 February 2019

[32] Gary C Hufbauer, Jeffrey J Schott & Kimberly A Elliott, *Economic Sanctions Reconsidered: History and Current Policy* (Vol 1, Peterson Institute 1990) 63

[33] *See eg* Jon R Lindsay, 'The Impact of China on Cybersecurity' (2014/15) 39(3) Intl Security 7, 20

[34] Xinhua 'Stabilising economic growth "top priority"' *China Daily* (11 July 2012) <chinadaily.com.cn/business/2012-07/11/content_15568386.htm> accessed 24 February 2019

2.2. Security is attained by means of peace

The modern international society may be anarchic in that it lacks a central enforcement authority but it is most certainly not lawless. None of the States would appreciate a primitive society where only the self-inflicted constraints of morality and power capacity would limit their behaviour and safeguard them from annihilation. In such a lawless system 'war would be frequent, insecurity would be very high, and anarchy would approximate to chaos'.[35] In addition to this, the endless race of States to ever greater power is an exhausting and a dangerous game. Insecurity is an inherent element of a competitive setting, in which a threat of being outperformed is always present.

For these very reasons, in the pursuit of their security from the external threats, States also maximise peace. Even though, much like the concept of security, the conceptualisation of peace can be disputed, it generally denotes the state of international relations characterised by the absence of not only a violent conflict but any kind commotion or undesired disturbance. Under the conditions of peaceful coexistence of nations, States can enjoy the autonomy given by their sovereign prerogatives and freely pursue their economic, social, scientific, cultural etc. development as they see fit. To protect the nation, territory, sovereignty, culture and other components, States seek peace by, *inter alia*, the creation of so-called peace regimes, providing a multilateral normative framework of permitted rationality in their power maximisation efforts.

General public international law is an example of such a regime and peace is certainly one of its primary objectives. Firstly, as it is for example in the case of the UN Charter, modern international law outlaws a violent inter-State conflict and consequently provides peace; States are under obligation to 'refrain in their international relations from the threat or use of force

[35] Barry Buzan, 'Peace, Power, and Security: Contending Concepts in the Study of International Relations' (1984) 21(2) J of Peace Research 109, 121. See also *Henkin* (n 1) 15

against the territorial integrity or political independence of any State' reads the article 2(4).[36] Secondly, and what is more important in the context of this thesis, international law aims to provide peace or the absence of any commotion with the independence of the States through one of its key principles – principle of sovereignty. Accordingly, law protects the States from any external interference with their territorial integrity, political independence and, generally, its ultimate power and supreme authority within and over the specific territory.

In addition to establishing a normative framework of permitted rationality, international law also promotes cooperation and fosters peace among nations. Last but not least, international law provides means of conflict resolution or a framework and tools for restoration of peace, a function to which I will return in the third chapter of this thesis.

Ago's assertion that States 'are far more interested in attaining their objectives than in invoking strict and coherent principles'[37] is not entirely correct as the rule of law can very well be in the interest of the said subjects. More than for 'the well-being of the international society and possibly survival of mankind',[38] States establish, develop and participate because international law serves the egoistic purpose of their interests – peace and security of the nation.

Sceptics should look no further than at the pattern of historic periods of insecurity and the consequential rise of peace regimes during or soon after; peace of Westphalia, peace of Versailles and the birth of the League of Nations. Post-1945, States sought peace in the creation of the United Nations and the rapid development of modern international law. Many of these legal regimes are very specific in conveying their goals – the maintenance of peace and security.

Insecurity is sometimes consequential to the inevitable advancement of human knowledge and the leaps in computer science are certainly not the first example of such disruptive

---

[36] *Charter of the United Nations* (n 8) preamble
[37] Robert Ago, '4th report on State Responsibility' (1972) II Ybk of the ILC 71, 73
[38] John HE Fried, 'How Efficient is International Law?' *in* Karl Deutsch & Stanley Hoffmann (eds), *The Relevance of International Law* (Schenkman Publishing 1968) 96

progress of human knowledge. The Outer Space Treaty, for example, was adopted by the UN General Assembly only a few years after the Soviets landed an unmanned aircraft on the moon and it became clear that advancement of relevant sciences may soon allow the use of celestial objects for malicious projects. The Treaty aimed to neutralise the newly-arisen insecurity to the States by, *inter alia*, pronouncing that '[t]he moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes'.[39] Also, Eddington, theorising the unprecedented energy outputs of the nuclear fusion in 1926, and Rutherford proving the theory through experimentation less than a decade later, probably had no idea that their research would lead to the development of nuclear weapons and a consequential period of great international insecurity.[40] The unprecedented insecurity caused by the accumulation of nuclear military power during the Cold War gave rise to the Treaty on the Non-Proliferation of Nuclear Weapons, a particularly indicative example of States maximising peace and reducing insecurity through the instrumentality of law.

States also resort to international law when technology introduces a significant threat to shared spaces, resulting in an indirect and long-term insecurity to the individual nations. The objective realities of an interconnected world and the inability to individually address the insecurities drive the States to form new legal arrangements (or expand existing ones) purely out of their self-interest. The Outer Space Treaty, for example, aimed to not only prevent States from utilising celestial objects for malicious purposes but also to avoid harmful contamination of outer space, which could turn into insecurity for all mankind in the future.[41] Similar motivation may be observed in the texts of various environmental legal regimes. The Vienna Convention for the Protection of the Ozone Layer and its additional Montreal Protocol serve as an illustration. The depletion of the Earth's protective layer exacerbated by the scientific progress

---

[39] UNGA Res 2222 (XXI) (19 December 1966) art IV

[40] Robert Arnoux, 'Who invented fusion?' (ITER, 12 February 2014) <https://www.iter.org/newsline/-/1836> accessed 9 August 2019

[41] *UNGA Res 2222 (XXI)* (n 39) art IX states: 'States Parties to the Treaty shall pursue studies of outer space, including the moon and other celestial bodies, and conduct exploration of them so as to avoid their harmful contamination.'

is a concern for the States because it introduced a threat to the wellbeing of the population of every State on the planet. 'For any environmental threat to be a security threat, there must be some demonstrable connection to some vital national interest. In the case of ozone depletion, the connection is to public health and human lives'[42] argues Levy. No State can patch the ozone hole by itself and thus remove the insecurity introduced by the phenomenon. To this end, States vowed, *inter alia*, 'to protect human health and the environment against adverse effects resulting or likely to result from human activities which modify or are likely to modify the ozone layer'.[43]

Although the rapid advancement of computer science indeed introduced a great deal of insecurity, and cyberspace is a domain shared by all the nations, it is unlikely States will rush into creating a new, specific international legal regime anytime soon. The invention of the Internet did not introduce the same level of insecurity as did nuclear weapons. Also, unlike the natural environment, cyberspace is a manmade domain, which can be quickly rebuilt, repaired, even circumvented, and thus the insecurity stemming from the damaged domain eliminated. Coupled with the fact that it offers an unprecedented opportunity for a cheap (though illegitimate) power, a cyber-specific international legal regime is not in sight.[44]

Nevertheless, a newly accessible environment does not necessitate a new legal regime nor does it indicate the lawless state of international cyber affairs. As explained in the first chapter of this thesis, traditional international laws still apply in new domains and its primary functions remain unchanged. States have indeed indicated interest in pursuing peace through law in cyberspace. As pronounced by the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, '[i]nternational law, and in particular the Charter of the United Nations,

---

[42] Marc A Levy, 'Is the Environment a National Security Issue?' (1995) 20(2) Intl Security 35, 48
[43] Vienna Convention for the Protection of the Ozone Layer (Vienna, 22 March 1985) art 2 para 1
[44] *See* ch 1

is applicable and is essential to maintaining peace and stability'[45] in cyberspace. What is more, the aforementioned UN GGE has explicitly reaffirmed the State's right to the absence of any commotion with their sovereign rights in cyberspace; 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.[46]

3. Non-compliance with international law is a preference

As I argued above, States generally do comply with international law.[47] *Generally*, however, does not mean *always*. The anarchical system provides a temptation to deviate from compliance for a number of reasons. Indeed, '[a] regime of mutual cooperation is then better for all than no regime, but each actor is constantly tempted to cheat'.[48] The temptation arises because peace has its price and because the expected benefits of international law, the manifestation of security, are very much dependent on the self-restraint of others and not just themselves.

Through the facilitation of cooperation, international law can aid States in increasing national power resources.[49] Its crucial function in the context of this chapter, however, is that it promises peace and security, *inter alia*, by imposing limitations on maximisation of power. In other words, the discretion in matters which are normally in the exclusive domain of the sovereign State is restricted by its previous commitments in the form of international law.[50] International law creates a framework of permitted rationality in the pursuit of security. It is by the limitation

---

[45] UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98 para 19. See also ch 1

[46] ibid para 20

[47] Gross argues 'States by and large obey international law' (Leo Gross, 'States as Organs of International Law and the Problems of Auto-interpretation' in GA Lipsky (ed), *Law and Politics in the World Community* (University of California Press 1963) 64); Note also *Henkin* (n 1) 47: 'almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time'.

[48] Robert Jervis, 'Security Regimes' (1982) 36(2) Intl Organisation 357, 371

[49] WTO law would be an example.

[50] *Advisory Opinion No. 4* (advisory opinion) [1923] PCIJ Rep Series B 24 <http://www.icj-cij.org/pcij/serie_B/B_04/Decrets_de_nationalite_promulgues_en_Tunisie_et_au_Maroc_Avis_consultatif_1.pdf> accessed 1 May 2019

of one's sovereignty that it contributes to the peace and security of the other nations. Constraints are implicit or explicit, sometimes just the other side of the coin; one nation's right to sovereignty, for example, is another nation's duty to refrain 'from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any State'.[51] Similarly, normative prescription dictating the inviolability of diplomatic correspondence and archives represents the restriction on acquiring information on one hand, as well the right to the absence of commotion on the other.

Under the condition of a functioning international law, a compliant State will source security from peace and power. The existence of the aforementioned restrictions in the form of international law does not mean that law imposes status quo of the distribution of power and that States are not allowed to maximise their power. By establishing a framework of permitted rationality and in exchange for the security provided by peace, law renders the overall gains of power **incremental and expensive.**

For example, to maintain peace among nations, the prohibition of the 'threat or use of force against the territorial integrity or political independence of any State'[52] imposes a constraint on maximising the power resources; a State with an appetite to expand its territorial power may not attempt a forceful annexation of the territory belonging to another State. What it can do however is to use diplomacy or other non-forceful but significantly more time-consuming methods to expand the territory; in this case, lawful devolution or succession and subsequent reunification would be a permissible alternative to forceful annexation. Another example of constraint of international law is the VCDR articles on inviolability of diplomatic correspondence and archives,[53] codified to promote the development of friendly, ergo peaceful

---

[51] UNGA Res 2625 (XXV) 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations' (24 October 1970) UN Doc A/RES/2625(XXV) 2. *See also Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep para 205

[52] *Charter of the UN* (n 8) arts 1(1) and 2(4)

[53] Vienna Convention on Diplomatic Relations (18 April 1961) 500 UNTS 95 arts 24 & 27

inter-State relations.[54] States are therefore prohibited from unlawful appropriation of diplomatic documentation and the containing information, which may increase their security though the maximisation of, for example, economic or military national power. Law, however, does not, and quite frankly cannot, serve as an imposition of the status quo of a power distribution in a given space and time.[55] Law does not prevent States from increasing their power but it does make it rather expensive and incremental. Protecting the privacy of said documents, VCDR does not prohibit a member of the State's agents to get a hold of the diplomatic secrets with wine, compliments or any other usual method of diplomacy. While this method is likely to be rather inexpensive, it is also significantly slower than ignoring the said limits of the law, infiltrating the premises of the guest State and taking what one will.

International law also does not prohibit maximisation of power through innovation. The F-35 Joint Strike Fighter is an appropriate example of a slow and expensive yet lawful and innovative growth of national power. What is thought to be most advanced military aircraft to date, the F-35 was in development for over twenty years and its research and development expenses surpassed 55 billion USD.[56] This increase of US military power spells a decline in relative power and security for its international competitors. In an attempt to restore the power relationship, China seemed to have orchestrated a cyber operation infiltrating the US computer network infrastructure and snagged the blueprints and other documents pertaining to the above-mentioned military airplane.[57] To put it another way, by means of an unlawful cyber operation in violation of the US' territorial sovereignty,[58] China acquired the military technology

---

[54] ibid preamble

[55] Such argument is proposed, for example, by *Morgenthau* (n 14) 90: 'international law, is primarily a static social force. It defines a certain distribution of power and offers standards and processes to ascertain and maintain it in concrete situations.'

[56] US Department of Defence, 'F-35 Lightning II Program Fact Sheet – Selected Acquisition Report (SAR) 2015 Cost Data' (*Joint Strike Fighter*, 24 March 2016) <http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf> accessed 1 July 2019

[57] National Security Agency, SIGINT Development, 'Chinese Exfiltrate Sensitive Military technology' (S//REL) <http://www.spiegel.de/media/media-35687.pdf> accessed 1 July 2019

[58] In what may be a contested view on the international law of cyber operations, Buchan claims State-sponsored cyber espionage, by infiltrating a foreign cyber infrastructure, violates the territorial sovereignty. *See* Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' *in* Anna-Maria Osula & Henry

and hence reversed the loss of its security at a lower cost in a considerably shorter period; the unlawful cyber operation 'reduce[d] the costs and lead time of [the] adversaries to doing their own designs, so it gives away a substantial advantage'[59] heard the US Senate from Under Secretary of Defence Kendall in 2013.

In addition to the unwelcome costs in a form of a restricted power maximisation, peace and security provided by international law are based on trust. Since trust in a competitive, selfish and anarchical society represents a risk, States are tempted to seek security by disregarding these constraints. To make matters worse, with the introduction of a **new and complex technology**, distrust strengthens and (unlawful) maximisation of power resources becomes more accessible, reinforcing its preferential status vis-à-vis compliance.

In the wake of new circumstances, compliance with international law is based on a promise of peace and the enabling reciprocity. States thus comply with international law and adhere to the aforementioned constraints in exchange for a promise of a long-term peace and security. Compliance rests on faith and trust in the effects of the law; '[i]t rests on the premise that a veil of ignorance stands between us and the future, but that we should nevertheless assume that regime-supporting behaviour will be beneficial to us even though we have no convincing evidence to that effect'.[60] Compliance is also based on trust of reciprocity; a reciprocal respect of the law is 'a condition theoretically attached to every legal norm of international law'.[61] Therefore, by observing the legal restrictions, States put their faith in compliance by the rest of the community. Particularly so in the anarchical community defined by the absence of central supervision or enforcement authorities, security is awarded by compliance or self-restraint of not oneself but of the others. But to be able to reap the benefits, States need to

---

Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE 2016) 65, section 3

[59] David Alexander, 'Theft of F-35 design data is helping U.S. adversaries –Pentagon' *Reuters* (19 June 2013) <https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619> accessed 1 July 2019

[60] Robert Keohane, 'The demand for international regimes' (1928) 36(2) Intl Organisation 325 342

[61] Elizabeth Zoller, *Peacetime Unilateral Remedies* (Transnational Publishers 1984) 15

exhibit a reciprocal attitude, as a one-sided compromise is not really a compromise. Only mutual compliance will further the sustainability of international law and enable it to provide peace and security.

By complying with the limitations imposed by law, States increase their vulnerability. Compliance implies States prefer the promise of peace over unlimited power maximisation and that they are willing to place their faith in the hands of other rational and self-interested members of the international society. This is clearly a paradoxical conception of the state of affairs. Promise and trust are fragile concepts in the international society and misplaced trust can quickly result in inferiority. States have no reason to trust each other to respect the law. The problem derives from the anarchical conception of international relations and the absence of an overarching compliance monitoring entity.[62] Distrust is a powerful temptation to lure States into non-compliance and rely on security by maximisation of their own power. Besides, a newly established legal regime promises results and long-term benefits, which may not materialise overnight. Power gains, on the other hand, can.

Aside from these temptations, scientific developments provide several additional incentives for non-compliance. One cannot deny that the advances in computer science reduce the prospect of the compliance benefit, and the costs of restraint may just become too great to bear.

Cyberspace is a relatively new, technically complex and, apart from its enabling hardware, immaterial and invisible domain. Once praised as a great democratisation tool, it has also democratised the threat; to connect, to code, and to penetrate foreign State infrastructure is, in relative terms, easy and inexpensive. How is a State to detect an invisible threat and how is it to protect itself from teenagers and nation States alike? In his testimony before the US House of Representatives, Healey warned that ‘adversaries will continue to use cyber means

---

[62] Of course, exceptions pertaining to the specific legal regimes exist. *See eg* Statute of the International Atomic Energy Agency (New York, 23 October 1956) art 2

to challenge American power and our citizens, as it offers significant opportunities for our adversaries'.[63]

Invisible and hard to comprehend, cyberspace and cyber operations are frightening to decision makers; '[c]yber is just pounding me from every direction'[64] complained US Congressman John Carter, concerned about the omnipresence of cyber threats to the State. Technology empowered, ill-intended individuals and States violate law remotely and silently. States no longer need planes and bombs to delay one adversary's development of nuclear weapons or increase of nuclear military power;[65] a computer code can be just as successful.[66] Detecting zealous accumulation of power of a particular State is not as easy as it seems, warned Morgenthau in 1960;[67] it is even harder in the 21st century. Unlawful cyber campaigns can remain undetected for years. Red October malware, for instance, allowed for the gathering of data pertaining to several diplomatic establishments around the world for full five years before it was exposed to the public and its victims.[68] In other words, the State orchestrating the cyber operation was able to unlawfully maximise its informational power resources for five years before anyone noticed.

Lastly, unlawful cyber operations may enable States to go after a certain power resource, which was previously out of reach. Benefits of such nature are without a doubt a strong incentive to ignore the law. To demonstrate, as per a US Presidential Executive Order from

---

[63] Jason Healey, 'Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities' (Testimony to United States House of Representatives Committee on Armed Services, 1 March 2017) <http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Bio-HealeyJ-20170301-U1.pdf> accessed 1 July 2019

[64] Ross Miller, 'Congressman John Carter: "Cyber is just pounding me from every direction"' (*The Verge*, 27 March 2015) <https://www.theverge.com/tldr/2015/3/27/8299577/john-carter-the-Internet-is-a-series-of-cyber-poundings> accessed 1 July 2019

[65] Erich Follath & Holger Stark, 'How Israel Destroyed Syria's Al Kibar Nuclear Reactor' *Der Spiegel* (2 November 2009) <http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html> accessed 1 July 2019

[66] Consider Stuxnet cyber operation.

[67] *Morgenthau* (n 14) 77–83

[68] Global Research & Analysis Team, ,The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies' (*Kaspersky Lab*, 14 January 2013) <https://securelist.com/blog/incidents/57647/the-red-october-campaign/> accessed 1 July 2019

2011,[69] imports from North Korea are generally prohibited[70] and in the decade between 2005-2015 North Korea's net export to the US amounted to no more than 12,000 USD.[71] North Korea, therefore, has no legitimate means to maximise economic power on the account of US trade cooperation. And yet in 2016 North Korea, by employing its cyber capabilities, managed to steal 81 million USD from the US Federal Reserve Bank and increase its economic power.[72] Forty years ago, this would have not been possible without any use of force.

Even when the legal regime has proven to provide peace, States have good reason to gravitate towards violation. Nevertheless, they do need to keep the law alive for a simple reason – compliance of the adversary is necessary for the advantage of unlimited power maximisation.

States will attempt legal gymnastics in order to rationalise and legalise their conduct and by doing so reinforce the validity of the restraints imposed by law. For instance, there is a strong indication that Russia, by the annexation of Crimea in 2014, violated international law.[73] After they were unable to deny the presence of Russian armed forces in Crimea,[74] the authorities

---

[69] President Barack Obama, 'Executive Order 13570 -- Prohibiting Certain Transactions with Respect to North Korea' (18 April 2011) <https://obamawhitehouse.archives.gov/the-press-office/2011/04/18/executive-order-13570-prohibiting-certain-transactions-respect-north-kor> accessed 1 July 2019

[70] US Department of Treasury, 'North Korea Sanctions Program' (2 November 2016) 6 <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/nkorea.pdf> accessed 1 July 2019

[71] Alexander JG Simoes & César A Hidalgo, 'The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development' (Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence, 2011) <http://atlas.media.mit.edu/en/visualize/stacked/hs92/export/prk/usa/show/2005.2015/> accessed 19 July 2019

[72] Aruna Viswanatha & Nicole Hong, 'U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed' (*Wall Street Journal*, 22 March 2017) <https://www.wsj.com/articles/u-s-preparing-cases-linking-north-korea-to-theft-at-n-y-fed-1490215094> accessed 12 July 2019

[73] *See eg* statement by the EEAS, 'EU sanctions against Russia over Ukraine crisis' (European Union Newsroom, 10 March 2016) <https://europa.eu/newsroom/highlights/special-coverage/eu-sanctions-against-russia-over-ukraine-crisis_en> accessed 1 July 2019; Council of Europe, Opinion on "Whether Draft Federal constitutional Law No. 462741-6 on amending the Federal constitutional Law of the Russian Federation on the procedure of admission to the Russian Federation and creation of a new subject within the Russian Federation is compatible with international law" endorsed by the Venice Commission at its 98th Plenary Session' (CDL-AD(2014)004-e, Venice, 21-22 March 2014) <http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2014)004-e> accessed 1 July 2019; Christian Marxsen, 'The Crimea Crisis – An International Law Perspective' (2014) 74(2) Heidelberg J of Intl L 367, 389

[74] Bill Chappell & Mark Memmott, 'Putin Says Those Aren't Russian Forces in Crimea' *NPR* (4 March 2014) <http://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea> accessed 1 July 2019

did not attempt to dismiss the normative restrictions on maximisation of territorial power. Instead, Russian administration served an alternative legal explanation of the conduct and labelled it as lawful reunification[75] because international law on sovereignty and territorial integrity restraining their neighbours is in their security interest. Generally speaking, violators are not interested in the collapse of the international legal order. Although it gives them advantage in terms of maximisation of power violators, as explained at the beginning of the chapter, do not want chaos.

An egoistic State's preferred setting is one where they are not restricted by the law and can maximise their power by whatever mode they desire but can nonetheless count on the performance of the law to restrain the other States from doing so as well. In order to enjoy the peace offered by international law, States, from a standpoint of a purely rational egoist, do not need to comply. As long as their competition does, that is. Compliance or self-constraint from the maximisation of power is only for the benefit of the rest of the community and the survival of the peace regime, which will, as a matter of reciprocity, provide peace. This implies a desire for **unilateral violation** of the legal restraints on the maximisation of power.

True, violations may invite other internationally wrongful acts or repercussions. To be able to violate and keep the others from doing so as well, States violate in secrecy or denial. What is more, to reinforce the constraints on the others, a non-complying State tends to reiterate the legitimacy of international law; '[t]he law-breaker will constantly invoke the sacredness of treaties if his opponents' obedience to them will be to his advantage'.[76] Two brief examples support this assertion. The US, believed to be behind the unlawful cyber-attack that resulted

---

[75] Putin was on the record stating that 'Russia has not annexed anything. Everything that has happened in Crimea is the result of illegitimate actions by certain political forces in Ukraine who provoked a coup d'état.' UNIAN, 'Putin on Crimea: Russia has not annexed anything' (*Ukrainian Independent Information Agency*, 17 September 2016) <https://www.unian.info/politics/1526324-putin-on-crimea-russia-has-not-annexed-anything.html> accessed 1 July 2019

[76] *Fried* (n 38) 99

in the physical destruction of the Iranian uranium enriching centrifuges,[77] explicitly argued that 'long-standing international norms guiding State behaviour—in times of peace and conflict—also apply in cyberspace'.[78] In a similar vein, the Russian Federation decreed its Information Security Doctrine is based on, *inter alia*, the observance 'of the generally recognised principles and norms of international law in carrying out activities to ensure national information security'.[79] This is the doctrine of the very same Russian Federation that is frequently accused of internationally wrongful cyber conduct.[80]

4. (Non-)compliance with international law is a rational choice

Rational States, ones with a consistent preference for security achieved through the maximisation of power or peace, choose their preferred behaviour by weighing costs and benefits. The underlying assumption of rationality is that States engage in 'purposive, means-ends calculation in order to attain their goals – that is, they select actions so as to maximise their utility'[81] in their struggle for security. Once we are equipped with the understanding of the costs and benefits of a given situation, rational choice theory can explain past and predict future behaviour of the States, including their decisions on whether to comply or not to comply with international law.

In the context of rational choice theory, States comply with the law when the benefits of compliance outweigh the associated costs, that is to say, when peace is expected to generate more security than unrestricted power maximisation would. Under the circumstances

---

[77] William J Broad, John Markoff & David E Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay' *New York Times* (15 January 2011) <nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all> accessed 1 July 2019

[78] President of the United States, 'International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World' (May 2011) 9

[79] Russian Federation, 'Information Security Doctrine of the Russian Federation' (9 September 2000) 26 <itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf> accessed 1 July 2019

[80] *See eg* Agence France-Presse, 'Russia accused of series of international cyber-attacks' *Guardian* (13 May 2016) <https://www.theguardian.com/technology/2016/may/13/russia-accused-international-cyber-attacks-apt-28-sofacy-sandworm> accessed 1 July 2019

[81] Alexander Thompson, 'Applying Rational Choice Theory to International Law: The Promise and Pitfalls' (2002) 31(1) J of L Studies S287. See also *Guzman* (n 3) 26–70

elaborated in the preceding sections, compliance is not distinctively rational. On the one hand, costs of compliance with the international obligations come in the form of restrictions, severely limiting the ability of a State to attain security by maximisation of power. States conform to the restrictions because the unfulfilled potential for security is theoretically compensated for by international law and its function of maximising peace. However, due to the competitive constellation of international relations, defined by egoism and anarchy, as well as the impact of modern technology, benefits of compliance are uncertain, to say the least.

Non-compliance with international law by means of inter-State cyber operations is a more rational strategy in attaining one's security. The benefits of violating international law are in diametrical opposition to the costs of compliance elaborated above; by dismissing the restrictions of the law, power and security surges are faster to materialise, require investment of fewer resources and are not dependent on the promise of reciprocity by other rational egoistic States. To substantiate the assertion of rationality of non-compliance the final thing I must demonstrate is that costs of unlawful inter-State cyber operation are no match to these benefits.

Every power maximisation effort necessitates the investment of the existing and limited (power) resources. For the purpose of the argument, I will label these as *direct* costs. Specifically, cyber operations may result in financial costs associated with, for example, recruitment, training and education of one's cyber operators, the establishment of computer network infrastructure, intelligence gathering and analysis activities, as well as other operational steps leading to deployment. Indeed, other costs of nonfinancial nature such as human capital should also be considered though they are easily expressed in monetary value.

In addition to the direct costs, internationally wrongful conduct can also attract *reactive* costs in the form of an undesired consequence, counterbalancing the benefits of the unlawful act or omission. If the benefits increase the power and security of the perpetrating State, the reactive costs have an opposite effect. In the absence of an international enforcement entity, reactive costs are imposed by other members of the international community. A State affected by a

malicious inter-State cyber operation may respond with a comparable act and thus counterbalance (or even surpass) the benefits the perpetrating party expected after the initial act. Stolen diplomatic documentation may be met by a mirroring act, depriving the initial perpetrator of its secrets and thus decreasing its diplomatic power, for example.

In essence, whether the State will engage in the internationally wrongful conduct depends on the probability and extent of the costs associated with the unlawful act.

Direct costs of inter-State cyber operations are unavoidable. The imposition of reactive costs for the non-compliance, on the other hand, is conditioned by the detection of the unlawful act. When assessing the potential costs, the violators will therefore take into consideration the **probability** of detection; the less likely the detection and the consequential occurrence of reactive costs, the more likely the non-compliance.

As already indicated before, unlawful cyber operations can be hard to detect. The RedOctober operation is an excellent example of this. The State behind the violation of the international diplomatic law reaped significant gains in power resource, while, due to the issues with detection, it encountered no significant reactive costs. Whichever State got a hold of the archives and the correspondence of several diplomatic establishments, gained informational power resource. Depending on the content, these power resources may be translated into a greater diplomatic, economic and even military power.

Nevertheless, issues with detection have been lessened and the probability of detection is not as insignificant as it used to be. In recent years American private-public partnership ventures 'made tremendous gains in determining – relatively quickly and with high confidence – what nations are responsible for cyber attacks' the US House of Representatives heard from Professor Healey in 2017.[82] True, States are nowadays much more comfortable voicing the

[82] *Healey* (n 63) 4. See also testimony by Martin C Libicki, 'It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture' (US House of Representatives, Committee on Armed Services, 1 March 2017) <docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-LibickiM-20170301.pdf> accessed 1 August 2019

political attribution of unlawful cyber operations. The US, for example, has repeatedly accused China, Russia, North Korea and Iran of deviant cyber behaviour. China has also openly blamed the US for continuous intrusions of their computer networks[83] and South Korea pointed a finger at its northern neighbour for meddling with the computer networks of their power infrastructure.[84]

However, the vague nature of the evidence provided in support of the political attributions of the cyber operation aimed at, for example, Sony[85] and Democratic National Committee,[86] implies the political attributions do not raise to the level of 'high confidence'. For now, States are hesitant to publicly substantiate statements of political attribution with any sort of technical proof other than an IP address attesting to the origin or transit of the cyber operation.

The fact that direct costs of these cyber operations are low and that non-compliance is rarely met with any reactive costs is the second reason behind non-compliance; ill-intended States will choose non-compliance when the benefits of deviation outweigh the costs.

Unlawful cyber operations are usually not free but the direct costs are nonetheless low. In fact, they are too low to change the rational State calculations. Direct costs associated with the cyber operations in this chapter are not available but valuations of a pair of comparable operations may provide a point of reference. Mirai DDoS botnet, for instance, is a publicly available open source toolkit,[87] allowing anyone with a connected computer and intermediate knowledge of the subject matter to trigger a large-scale DDoS attack and point it at a national

---

[83] Xinhua, 'China publishes latest data of US cyber attack' *China Daily* (20 May 2014) <http://www.chinadaily.com.cn/china/2014-05/20/content_17519283.htm> accessed 1 July 2019

[84] Ju-min Park & Meeyoung Cho, 'South Korea blames North Korea for December hack on nuclear operator' *Reuters* (17 March 2015) <reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317> accessed 1 July 2019

[85] FBI, 'Update on Sony Investigation'5 (17 December 2014) <http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> accessed 11 June 2019

[86] US DHS & FBI, 'GRIZZLY STEPPE – Russian Malicious Cyber Activity' (29 December 2016) <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> accessed 1 July 2019

[87] Jerry Gamblin, 'Mirai-Source-Code' GitHub (15 July 2017) <github.com/jgamblin/Mirai-Source-Code> accessed 21 May 2019

Internet infrastructure.[88] Moreover, US intelligence budget indicates that the costs related to a more sophisticated cyber operation, one intended to electronically compromise remote computer systems, access their functions, harvest the data and perform 'other operational goals',[89] average at 7,350 USD.[90] Direct costs can be even lower considering that cyber infrastructure is a distinctively dual-use technology which can be later used for other legitimate activities of the State. Also, malware can be modified and reused in other internationally wrongful activities, as was the case with WannaCry functionality which relied on an exploit previously developed by (and stolen from) the US National Security Agency (NSA).[91] These points in conjunction with the examples of cyber operations and the resulting benefits below validate the claim that direct costs of non-compliance in cyberspace do not surpass the benefits.

Similar claims may be made about the reactive costs. In spite of the fact that States seem to possess some information related to the attribution of cyber operations and are quite happy to blame their adversaries for the wrongdoing, reactions are usually non-existent or, in the best case, lukewarm. If not related to the issue with detection and attribution, the reason may lie in the uncertainty related to the application of international law to the new domain. While States may have confirmed the application of international norms to inter-State relations in cyberspace, States are yet to agree on how exactly the law applies in the new environment. Also, general international law established by multilateral agreements predates cyber operations and it is too early to speak about the conclusive customary law. In the environment

---

[88] Nicky Woolf, 'Massive cyber-attack grinds Liberia's Internet to a halt' *Guardian* (3 November 2016) <theguardian.com/technology/2016/nov/03/cyberattack-Internet-liberia-ddos-hack-botnet> accessed 23 July 2019

[89] US National Security Agency, 'Computer Network Operations – Genie' *Spiegel* (3 February 2015) 105 <http://www.spiegel.de/media/media-35660.pdf> accessed 1 July 2019

[90] In 2013 US allocated 652 million USD for the GENIE project, which enabled a remote control of 85.000 network machines around the world; an average cost of a cyber operation is therefore valued at 7.350 USD. Barton Gellman & Ellen Nakashima, 'U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show' *Washington Post* (30 August 2013) <https://wapo.st/2LTGsyD> accessed 1 July 2019. *See also* US National Intelligence Community, 'FY 2013 Congressional Budget Justification' (Volume I, National Intelligence Summary, February 2012) <https://fas.org/irp/budget/nip-fy2013.pdf> accessed 1 July 2019

[91] Andy Greenberg, 'Hold North Korea Accountable for WannaCry—And the NSA, too' (*Wired*, 19 December 2017) <https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/> accessed 1 July 2019

of normative ambiguity caused by any significant technological leap, States sometimes cannot react and impose significant costs. And when they do, the reaction of the injured States is (self)limited to public outrage causing a decrease of the adversary's reputation. Rejecting the hypothesis of Guzman, claiming that the concern over the costs to reputation is the prevailing motive of compliance, examples of non-compliance in the cyber domain point at the fact that loss of reputation is not proportional to the benefits of non-compliance and thus not an efficient deterrent.[92]

The Shamoon virus, for example, erased more than three quarters of all the hard drives of the Saudi petrochemical company Aramco in 2012. It handicapped the State-owned company for more than a week. While the oil production did not slow down because of the virus, business operations had been brought to a standstill; some claims suggest it took no less than five months for the company to completely restore its computer network.[93] Such a disruption had a negative effect on Saudi national economic power and, as such, a positive effect on the power or the State behind the operation. Considering that the Kingdom of Saudi Arabia is heavily dependent on its export of oil and that in 2012 Aramco, the world's largest producer of crude oil by far, generated a revenue of more than one billion USD per day, accounting for more than 80 percent of the total of the Kingdom's revenues and almost half of its GDP,[94] a week of such a disruption of its business operations had significant economic consequences for the company as well as the State. Benefits of the wrongdoing State, interested in the decrease of Saudi economic power, were therefore significant, which cannot be claimed for the costs. A year after the incident, the US NSA privately pointed the finger at Iran.[95] While, and probably because, no one provided any proof as to who the perpetrator behind the

---

[92] *Guzman* (n 3) 34–42

[93] Sico van der Meer, 'Foreign Policy Responses to International Cyber-attacks' (Clingendael Institute, September 2015) <https://bit.ly/2JQU4In>; Jose Pagliery, 'The inside story of the biggest hack in history' *CNN* (5 August 2015) <http://money.cnn.com/2015/08/05/technology/aramco-hack/> both accessed 9 June 2019

[94] Jim Finkle, 'Exclusive: Insiders suspected in Saudi cyber attack' *Reuters* (2 September 2012) <http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907> 18 July 2018

[95] US National Security Agency, 'Iran – Current Topics, Interaction with GCHQ' (12 April 2013) <https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/> accessed 1 July 2019

devastation at Aramco was, the reactive costs inflicted by the international community on Iran were low, to say the least. Besides bad press[96] inflicting a negligible decrease in the reputation of the State, Iran suffered no reactive costs for the cyber operation violating Saudi sovereign rights.

Reputational costs were not enough to stop perpetrators from crippling Estonia with a DDoS operation in 2007. One of the victims was Estonia's banking sector.[97] The President protested[98] and numerous news outlets[99] reported the political attribution made by the Estonian government officials,[100] tying the malicious cyber deeds to the Russian government. It undeniably made a dent into Russian international credibility but clearly not enough for Russia to cease maximising its power by (unlawful) cyber operations.[101] This is understandable. The benefits in 2007 were numerous and clearly outweighed the costs. The economic power of Estonia, a country where 97% of all banking transactions are conducted electronically, was reduced.[102] Not only was Russia maximising its power, but by attempting to coerce Estonia from moving a World War II monument to where Russia publicly opposed,[103] the primary aim of the cyber operation was a demonstration of its power over the former Soviet republic.

---

[96] Thom Shanker & David E Sanger, 'U.S. Suspects Iran Was Behind a Wave of Cyberattacks' *New York Times* (13 October 2012) <http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html> accessed 21 July 2019

[97] Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4(2) J of Strategic Security 49, 51–52

[98] Toomas Hendrik Ilves, 'Address by H.E. Mr. Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly' (25 September 2013) <http://goo.gl/kyKNbD> accessed 8 February 2015

[99] *See eg* 'Estonia hit by 'Moscow cyber war' *BBC* (17 May 2017) <http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

[100] Dave Phillips, 'Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State' (4 June 2017) <https://wikileaks.org/plusd/cables/07TALLINN366_a.html> accessed 1 July 2018

[101] *US DHS & FBI* (n 86)

[102] *Herzog* (n 97) 49

[103] An attempt to move the monument is a 'disgusting' act, said Russian Foreign Minister Lavrov and Russian Duma demanded sanctions. Steven Lye Myers, 'Russia Rebukes Estonia for Moving Soviet Statue' *New York Times* (27 April 2007) <http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html> accessed 1 July 2019

Infrequently reactive costs surpass the loss of reputation. The US has attempted to increase the costs of the perpetrating States by means of indictments under the domestic criminal law and issued arrest warrants for five People's Liberation Army and People's Republic of China officials in 2014 for, *inter alia*, 'damaging computers through the transmission of code',[104] which could very well constitute an unlawful cyber attack. Yet, whatever the negative effect of this cost was on the power of China, it was not enough to deter the State from non-compliance; US military officials claim China has not ceased to rely on cyber operations 'targeting and exploiting US government'[105] in a search for the maximisation of its power resources.

The US administration has promised a proportional response to the unlawful cyber operations against its infrastructure, promised to impose 'swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities'.[106] It delivered on this promise in 2016, when it froze the assets of Russian governmental entities and several individuals for influencing the US presidential elections, which constituted a 'violation of established international norms of behaviour'.[107] Time will tell whether this was enough of a cost to deter future similar cyber operations by Russian authorities. Similar reactions against Iran were proposed to the US House of Representatives but have not materialised.[108]

---

[104] US Department of Justice, 'Cyber's Most Wanted' (*Federal Bureau of Investigation,* 1 May 2014) <https://www.fbi.gov/wanted/cyber/sun-kailiang/@@download.pdf> accessed 31 May 2017. Note also the arrest warrants related to the North Korean heist of FED assets. See *Viswanatha & Hong* (n 72)

[105] Michael S Rogers, 'Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities' (*US House of Representatives*, 16 March 2016) 4 <http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf> accessed 11 December 2018

[106] President of the US, 'National Security Strategy of the United States of America' (December 2017) 13 <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> accessed 1 July 2019

[107] President of the US, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (*White House*, 29 December 2016) <https://bit.ly/2kuHFtU> accessed 1 July 2019

[108] HR 5222 Iran Cyber Sanctions Act of 2016, 114th US Congress (2nd Sess 2016) 5 <https://www.congress.gov/114/bills/hr5222/BILLS-114hr5222ih.pdf> accessed 1 July 2019

5. The illusion of power gains and unlawful maximisation of security

In spite of the fact that costs of wrongdoing may be low or non-existent, the maximisation of security by simultaneously reaping benefits of international law and then breaching it is an illusion. Loss of security by the injured State calls for unlawful reaction, likely to be imitated by other States and to eventually lead to the deterioration of law and thus increased insecurity of everyone.

In relative terms, an increase of one's security by the modality of power maximisation decreases the power and therefore security of its adversary. In spite of the apparent absence of a meaningful reaction from the injured States and the significant gains of the perpetrating State power, the former is unlikely to remain as passive as suggested above and power gains of the latter will sooner than later be diminished. Injured States will react by focusing on the lost power. In other words, they will pursue the restoration of the power relationship enjoyed prior to the unlawful act – either by eventually inflicting damage to the foreign power or by increasing their own.

In 2012, a lesser known cyber operation forced Iran to disconnect the Kharg Island facility, its largest oil terminal. The destructive malware was named Flamer. In a country heavily dependent on its petrochemical industry, the disruption of an operation responsible for 80% of its daily production of crude oil[109] undeniably translates into loss of economic power. Iranian authorities attributed the cyber operation to the US.[110] A year later, however, the communication between NSA and British Government Communications Headquarters (GCHQ) pointed at the fact that Iran had not remained static. Despite official denials from Iran that the cyber-attack dealt any significant damage to its oil industry and even refusing to

[109] Saeed Kamali Dehghan, 'Iranian oil ministry hit by cyber-attack' *Guardian* (23 April 2012) <https://www.theguardian.com/world/2012/apr/23/iranian-oil-ministry-cyber-attack> accessed 1 July 2019

[110] 'Iran oil fires raise cyber sabotage fears' *Press TV Iran* (14 August 2016) <http://www.presstv.ir/DetailFr/2016/08/14/479952/Iran-oil-industry-fires-cyberattack-US-Israel> accessed 1 July 2019

impose reputational costs against the alleged orchestrators at the time of their occurrence, Iran has nevertheless 'demonstrated a clear ability to learn from the capabilities and actions of [its adversaries]'[111] and sought to decrease US economic national power through disruptive cyber campaigns against approximately 46 of its major financial institutions.[112] '[A] counter attack by Iran against American financial institutions',[113] as classified by the US Senator Lieberman, intended to restore the initial economic power relationship vis-à-vis the US and replace the unlawful loss of power by unlawfully decreasing the power of the adversary.

With this, the initial power equilibrium may be re-established, but consequences may be more significant than they appear. When the initially injured State seeks to restore the original power relationship, it will inevitably be lured into non-compliance. As previously noted, it is only by violation that an injured State can match the speed, quantity or type of unlawful power resource maximisation.

And they are likely to repeat it as well. The broken windows theory, developed by criminologists Wilson and Kelling, argues that unaddressed violation attracts repetition; if 'a window building is broken and is left unrepaired, all the rest of the windows will soon be broken'.[114] In the context of international law, Fisher specifically warns of the dangers of internationally wrongful precedents[115] as being crucial to the survival of the international legal rule. Not talking about cyber incidents may be prevalent but it certainly is not '[the] best international practice',[116] as stated by the representative of the International Olympic Committee in the aftermath of the cyber operation disrupting the computer systems during the 2018 Pyeongchang Winter Olympics. Violations should not be swept under the rug and left

---

[111] *US National Security Agency* (n 95)
[112] US v Ahmad Fathi et al, No 1:16-cr-00048 (South D New York 21 January 2016) <https://www.justice.gov/opa/file/834996/download> accessed 1 July 2019
[113] 'Newsmakers with Senator Joe Lieberman' (*C-SPAN*, 21 September 2012) <https://www.c-span.org/video/?308327-1/newsmakers-senator-joe-lieberman> accessed 1 July 2019
[114] James Q Wilson & George L Kelling, 'Broken Windows' (1982) 249(3) Atlantic Monthly 29, 30
[115] Roger Fisher, *Improving compliance with international* law (University Press of Virginia 1981) 21–22
[116] Karolos Grohmann, 'Games organisers confirm cyber attack, won't reveal source' (*Reuters*, 11 February 2018) <https://uk.reuters.com/article/us-olympics-2018-cyber/games-organizers-confirm-cyber-attack-wont-reveal-source-idUKKBN1FV036> accessed 1 July 2019

unaddressed or inadequately addressed; if so, more will inevitably follow. In fact, it would appear Iran did indeed continue breaking the windows after the initial response to the disrupting cyber operation aimed at its oil industry. According to US intelligence, Iran not only sought to restore the initial power equilibrium with the cyber operations against the US but also used the Shamoon malware to unlawfully decrease the economic power of Saudi Arabia in 2012. What is more, it would appear the net profits of the 2012 cyber operation encouraged Iran to chip the power of Saudi Arabia even further in 2016 by pointing the very same malware at the Saudi's General Authority of Civil Aviation, 'erasing critical data and bringing operations there to a halt for several days'.[117]

If the violations are not addressed and the offenders not coerced into compliance, others will take note and likely follow.[118] Rational States, other than parties involved in the conflict, will observe, calculate, learn and imitate for various reasons; they will either give in to the temptation of opportunism, find compliance too expensive or be forced to look for alternatives to the security normally provided by the functional legal regime. Firstly, the so called free-rider problem is certainly a frustrating reality and, if the situation persists, even the States on the right side of the law may soon turn to opportunism and 'eventually give in to the intensity of the competition between the nations',[119] where unrestricted power maximisation comes at such a low price. Secondly, once the aforementioned distrust in self-restraint of the international society has materialised, compliance becomes simply too expensive. In the absence of promised peace, rational States are unlikely to willingly restrain their methods of power maximisation.

---

[117] Sewell Chan, 'Cyberattacks Strike Saudi Arabia, Harming Aviation Agency' *New York Times* (1 December 2016) <https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html> accessed 1 July 2019

[118] UK National Cybersecurity Strategy warns: 'States may use [offensive cyber] capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit.' HM Government, National Cyber Security Strategy 2016-2021 (1 November 2016) 18 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> accessed 1 July 2019

[119] Stanley Hoffmann, 'International Law and the Control of Force' *in* Karl Deutsch & Stanley Hoffmann (eds), *The Relevance of International Law* (Schenkman Publishing 1968) 51

And sometimes, they cannot afford to do so. When the law struggles to deliver on the promise of security through established frameworks of peace, States will turn to alternatives. Specifically, they may seek peace through a new and issue-specific legal regime. For instance, in 2011 and 2015 Russia, China et al tabled the International code of conduct for information security at the UN General Assembly.[120] If the establishment of universal legal frameworks proves to be an overly ambitious project, States will seek peace by establishing new bilateral legislation. Again, China and Russia, after failing in the international setting, sought out peace by a bilateral treaty pledging to withhold from cyber operations in violations of each other's respective sovereign rights.[121]

Considering a comprehensive worldwide agreement on the interpretation of international law in cyberspace is unlikely to be adopted anytime soon[122] and the fact that illegitimate but significant power maximisation comes at a minimal cost, it is more likely that States will substitute peace with power as a means of attaining security. Once again, to keep up with their non-complying counterparts, States will be forced to disobey the law.

This leads to escalation or a spiral of conflict.[123] And an ever greater frequency of delinquent behaviour, consequentially, leads to the deterioration of norms and decline of security. States, confident in the superiority of their cyber offensive capabilities,[124] may be certain in their

---

[120] UNGA 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' UN Doc A/69/723 (13 January 2015)

[121] Olga Razumovskaya, 'Russia and China Pledge Not to Hack Each Other' *Wall Street Journal* (8 May 2015) <https://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/> accessed 1 July 2019

[122] Recently collapsed negotiations under the auspices of the UN, for example, confirm the fact that an international cyber treaty is unlikely. Michele Markoff, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (*US Mission to the UN*, 23 June 2017) <https://usun.state.gov/remarks/7880> accessed 1 July 2019

[123] *See* Kathleen A Kennedy & Emily Pronin, *Bias Perception and the Spiral of Conflict in Jon Hanson, Ideology, Psychology, and Law* (OUP 2012) ch 12

[124] For example, General Keith Alexander, Commander of the US Cyber Command bragged in 2013: 'We believe our offense is the best in the world. Cyber offense requires a deep, persistent and pervasive presence on adversary networks in order to precisely deliver effects. *Information Technology And Cyber Operations: Modernisation And Policy Issues To Support The Future Force, Hearing Before the Subcommittee on Intelligence, Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives,* 113 Cong (1 Sess 2013) (Statement of Gen Keith B. Alexander, USA, Commander, United States Cyber Command) 87 <https://fas.org/irp/congress/2013_hr/cyber.pdf> accessed 1 July 2019

immunity from the deterioration of the international normative framework but 'though disorder may profit [them] today in one case it may hurt them in another tomorrow, and in the long run is bound to work them harm'.[125] Once the number of the of non-complying power maximisers reaches a certain point, compliance is not rational anymore,[126] and the community will approximate to the state of chaos.

6. Conclusion

In the anarchical conception of international relations, the primary concern of every State is its security, attained either by maximisation of power or peace. The latter, awarded by, *inter alia*, the rule of international law constrains the maximisation of power. The lack of trust among competitive, selfish States, as well as the development of computer science, represents temptations for them to deviate from legally prescribed behaviour and seek ultimate security – unrestricted, fast, and cheap power and peace – by compliance with the other members of the community.

Whether States will violate international law depends on the cost benefit-analysis of non-compliance. The calculations of the numerous examples listed in this chapter suggest States violate because cyber operations bring significant benefits at very low costs, normally only damaging their international reputation. The gains, therefore, outweigh the costs.

Or so it seems. The injured States respond with the illegitimate maximisation of their power to make up for the newly introduced deficiency in power which causes insecurity. And by doing so, they encourage the spiral of conflict between the two States. Due to the aforementioned temptations, opportunism will attract other wrongdoers and the community will soon consider compliance with the underperforming law simply too expensive.

---

[125] Dag Hammarskjold, 'Liberty and Law in International Life' *in* Clarence W Jenks, Roberto Ago & Oscar Schachter (eds), *International Law in a Changing World* (LLC 2012) 24–25

[126] Jens D Ohlin, 'Nash Equilibrium and International Law' (2012) 23(4) EJIL 915

Injured States should, therefore, focus on the peace provided by international law and not on power at all costs. In order to do so, their reactions and the costs they impose on the violators should be within the framework of international law. The following chapter explores the role of the international law of State responsibility, which provides the injured State, not only the accountability framework for restoration of the power relationship and the cessation of the unlawful cyber operation but also, a mechanism of self-help which secures the present and future performance of the power-hungry States by altering the cost benefit calculus in the cyber era.

Chapter 3

State responsibility, countermeasures and compliance

1. Introduction

While the preceding two chapters explained the issue of unlawful inter-State cyber operations and the motives behind non-compliance in the cyber era, the following paragraphs explore the legal consequences following a breach of international obligations. To this end, the chapter investigates the law of State responsibility and elaborates its capacity to induce compliance with international law, therefore to restore peace by supressing the occurrence of unlawful inter-State cyber operations below the use of force.

In the context of a distinctively positive cost benefit analysis of non-compliance, the present chapter analyses the capacity of the law to induce compliance by imposing a trinity of secondary international obligations arising upon the breach of primary ones.

The chapter also compares and examines the enforcing mechanisms of international law – adjudication, multilateral sanctions, reprisals, retorsion and countermeasures.

The final part of the chapter delves into the theory of countermeasures and their role in enforcing compliance of the rational States. In particular, it elaborates the instrumentality and proportionality of countermeasures in the light of their lawfulness and effectiveness in relation to present and future compliance.

2. Consequences of the breach of international law

A breach of the international legal obligation, and the consequential denial of the corresponding right to its bearer, involves a legal responsibility of the party in the wrong. The same holds true in international law; the fact that every violation of international law by a State

involves responsibility,[1] is 'most strongly upheld by State practice and judicial decisions and most deeply rooted in the doctrine of international law'.[2]

Responsibility for the violation of one's duties or another one's rights is essential to the legal character of the normative order. Legal responsibility in the international setting is based on the 'actual existence of an international legal order and in the legal nature of the obligations it imposes on [the States]',[3] argued the ILC in their preparatory work related to the international law of State responsibility codification efforts. Thus, State responsibility is understood to be 'the necessary corollary of a right [and all] rights of an international character involve international responsibility.'[4]

The law of State responsibility aims to restore and maintain peace in the international society after it has been momentarily disturbed by non-compliance. The purpose of this 'system of multilateral public order'[5] has been explicitly voiced by the UN General Assembly, declaring that 'it is desirable for the maintenance and development of peaceful relations between States that the principles of international law governing State responsibility be codified'.[6] The law of State responsibility does so by seeking the restoration of compliance, which is vital to the performance of law and thus the manifestation of peace and security.[7]

The contemporary system of international responsibility seeks to impose compliance and restoration of power relationship by the operation of law. Specifically, responsibility for the

---

[1] *Rainbow Warrior (New Zealand v France)* [1990] XX UNRIAA 251 para 75: 'any violation by a State of any obligation, of whatever origin, gives rise to State responsibility.'
[2] ILC, 'Document A/9010/Rev.1: Report of the International Law Commission on the work of its twenty-fifth session (7 May- 13 July 1973)' (1973) II Ybk of the ILC UN Doc A/CN.4/SER.A/1973/Add.l, 174
[3] ILC, 'Third report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility' (1971) II(1) Ybk of the ILC UN Doc A/CN.4/SER.A/1971/Ad(U (Part 1), 205. A view is inspired by prior writing of Anzilotti: [T]he existence of international legal order postulates that the subjects on which duties are imposed should equally responsible in the case of a failure to preform those duties.' Dionisio Anzilotti, *Cours de droid international* (trans Gidel, Pantheon-Assas/LGDJ 1999) 467
[4] *Spanish Zone of Morocco (Great Britain v Spain)* [1924] II UNRIAA 615, 641. See similar claims made by the PCIJ in *Chorzów Factory Case (Germany v Poland)* (Merits) [1928] PCIJ Rep Ser A, No 17 para 66
[5] ILC, 'Report of the International Law Commission on the work of its fifty-second session (1 May–9 June and 10 July–18 August 2000)' (2000) II(2) Ybk of the ILC UN Doc A/CN.4/SER.A/2000/Add.1 (Part 2)/Rev.1 para 365
[6] UNGA Res 799 (7 December 1953) UN Doc A/RES/799(VIII)
[7] Peace, which is provided by the mutual, reciprocal compliance with the international law. *See* ch 2

internationally wrongful conduct gives rise to the secondary obligations of cessation and non-repetition, explicitly commanding present and future compliance with the primary obligations of international law. It also gives rise to the secondary obligation of reparation, which, in the context of the rational choice theory, imposes a restoration of the power relationship that existed prior to the violation of the international obligations, hence altering the cost benefit analysis of the wrongdoers and rendering current and future non-compliance irrational.

In the event that the secondary obligations fail to persuade the responsible State to respect the primary obligation, the law of State responsibility authorises injured States to take matters into their own hands and utilise one of many legal enforcement mechanisms. Much like reparation, legal enforcement mechanisms represent an infliction of a reactive deprivation of power of the wrongdoing State. Instead of relying on the power of legal obligations, enforcement mechanisms allow States to impose costs on the non-complying party, to collect the debt due by the responsible State. Akin to reparation, these enforcement mechanisms erase the benefits of the violation, alter the cost benefit analysis of the wrongdoer and render the non-compliance irrational.

The following paragraphs discuss these law-enforcing consequences of State responsibility in detail.

3. Inducing compliance by operation of the law of State responsibility

The system of international responsibility seeks to impose compliance and restoration of the previous power relationship by the operation of law. Specifically, it materialises in the secondary obligations of cessation, non-repetition and reparation, dictating compliance and restoration of the power relationship that existed prior to the violation of the law by cyber means.

The secondary duty of **cessation** aims to restore compliance with the primary obligation. Aimed at the re-establishment of the rule of law, the duty seeks to revert the loss of peace and neutralise the insecurity introduced by the unlawful cyber operation. It requires the wrongdoing

State to put a stop to the continuing unlawful conduct at will and comply with the primary obligation.[8] This may involve a discontinuation of an unlawful act or a positive action to remedy the unlawful omission. The introduction of this secondary obligation does not render the pre-existing, primary obligation moot. This is clearly expressed in article 29 of the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), emphasising the 'continued duty of the responsible State to perform the obligation breached.'[9]

On the contrary, the obligation of cessation emphasises the duty of performance. Indeed, the primary obligation and the secondary obligation of cessation are in close relationship[10] and the latter is hardly an entirely new obligation. By imposing an obligation to restore compliance, the duty of cessation is a reiteration of the 'non-optional or obligatory'[11] nature of the primary obligation. While this may seem to be contradictory to the position of the ILC, which decided to separate said obligations in the ARSIWA, it was the very same ILC that, in the context of the international responsibility of international organisations and building on the previous codification of State responsibility, opined:

> When the breach of an obligation occurs and the wrongful act continues, the main object pursued by the injured State or international organisation will often be cessation of the wrongful conduct. Although a claim would refer to the breach, what would actually be sought is compliance with the obligation under the primary rule. This is not a new obligation that arises as a consequence of the wrongful act.[12]

From the vantage point of the rational choice theory, the obligation of cessation imposes the duty to restore, through law, the levels of peace that States enjoyed prior to the breach in question. Peace, a product of a functioning legal regime marked by mutual compliance, will provide the States with the security they enjoyed before the occurrence of the wrongdoing.[13]

---

[8] UNGA Res 56/83 'Responsibility of States for Internationally Wrongful Acts' (12 December 2001) UN Doc A/RES/56/83 (ARSIWA) art 30
[9] ibid art 29
[10] Antonios Tzanakopoulos, *Disobeying the Security Council: Countermeasures against Wrongful Sanctions* (OUP 2011) 142–143
[11] HLA Hart, *The Concept of Law* (2nd edn, Clarendon 1994) 82
[12] ILC, 'Draft articles on the responsibility of international organisations, with commentaries 2011' (2011) II(2) Ybk of the ILC UN Doc A/CN.4/SER.A/2011/Add.1 (Part 2), art 30 cmt 2
[13] *See* ch 2

In spite of the fact that the obligation of cessation is only relevant in relation to a continuous violation, the significance of the obligation of cessation stretches beyond the present. Since a breach poses a danger to the effectiveness, the validity and, potentially, the very existence of the primary rule, a swift restoration of compliance is an important warning signal to States wishing to imitate these illegitimate power maximisation methods in the future. Instead of contributing to the deterioration of the legal regime and exacerbating insecurity by encouraging similar deviant behaviour of the other States, the injured State should therefore take note of the law and invite the wrongdoing State to comply with its international obligations and restore peace. Even though the obligation of cessation is established by operation of law and as such does not require the injured State to call upon the wrongdoing party to cease the operation, practical considerations may indeed require this step to be taken to achieve the restoration of the situation prior to the breach.[14]

Under these conditions and after being called upon to fulfil the duty of cessation, the wrongdoing State is thus required to put an end the continuing unlawful act at will. To comply, the wrongdoing State can, for example, terminate the ongoing operation of a malicious program by activating the so-called kill switch,[15] which was how the Stuxnet cyber attack came to an end. Two years after inflicting physical damage to the Iranian nuclear uranium enriching centrifuges, Stuxnet ceased to propagate its malicious code because the orchestrating State stopped updating the malware's protocols and, through this deliberate refrain, triggered the kill switch and disabled its further functionality.[16]

---

[14] *ARSIWA* (n 8) art 34 cmt 2

[15] An example of a kill switch definition: 'A kill switch is a mechanism for turning off a device or a piece of software remotely – and abruptly – in an emergency, such as when it has been stolen or accessed without authorisation. In malware, a kill switch is a way for the operator to terminate their connection to the software to prevent authorities from discovering their identity.' Adrian Winckles, 'Kill switches, sinkholes and how to stop a cyber attack' (*Anglia Ruskin University*, 19 May 2017) <http://www.anglia.ac.uk/news/kill-switches-sinkholes-and-how-to-stop-a-cyber-attack> accessed 28 July 2019

[16] William Jackson, 'Stuxnet shut down by its own kill switch' (*GCN*, 26 June 2016) <https://gcn.com/Articles/2012/06/26/Stuxnet-demise-expiration-date.aspx> accessed 28 July 2019

Another continuous and State orchestrated cyber operation that ceased operation after its kill switch was triggered is known as Flamer.[17] The malware infiltrated Iranian computer networks and, among other things, caused a significant loss of data on several computer systems,[18] forcing the authorities to disconnect some of its biggest oil terminals, thus inflicting damage to Iran's economic power.[19] Operational between May and June 2012 and in violation of the international legal principle of sovereignty, this cyber operation qualifies as a continuous wrongful act. Flamer ceased to function when the orchestrator issued a remote command, instructing the malware installed on the hosting and affected machines to simply delete itself as well as all traces of its operation.[20] Considering that the obligation of cessation is only relevant when the breach is continuous, the State responsible for the Flamer cyber operation was under the obligation to cease the unlawful conduct between May and June 2012.

Sometimes the temporal characteristics of the unlawful act are not as easily established. Although the primary unlawful character of Stuxnet lies in its contravention of the international legal prohibition of the use of force, I use it below to illustrate the argument. Considering that the obligation of cessation is relevant and arises only in the context of a continuing violation of international law and that Stuxnet, by amounting to an instantaneous[21] violation of the prohibition of the use of force, did not extend in time, one may argue that the responsible State was not under the secondary obligation of cessation. However, one point that is often overlooked is that the State legally responsible for the Stuxnet operation was not only responsible for the internationally wrongful cyber attack; by retaining its active presence in the

---

[17] 'sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks Laboratory of Cryptography and System Security' (CrySyS, Budapest University of Technology and Economics, v1.05 (31 May 2012) 3 <http://www.crysys.hu/skywiper/skywiper.pdf> accessed 28 July 2019

[18] MAHER, 'Identification of a New Targeted Cyber-Attack' (28 May 2012) <https://web.archive.org/web/20131105160213/http://www.certcc.ir/index.php?name=news&file=article&sid=1894> accessed 28 July 2019

[19] *See* ch 2

[20] Symantec Security Response, 'Flamer: Urgent Suicide' (*Symantec*, 6 Jun 2012) <https://www.symantec.com/connect/blogs/flamer-urgent-suicide> accessed 28 July 2019

[21] Stuxnet damaged the Iranian nuclear infrastructure in 2009 or 2010. David Albright, Paul Brannan & Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?' *Institute for Science and International Security Report* (22 December 2010) <http://goo.gl/yM4Wy> accessed 3 August 2018

various computer systems years after the incident at Natanz nuclear facility, Stuxnet also violated the sovereign rights of Iran. From this perspective, the violation did have a continuous character and involved the obligation of cessation for as long as the functional malware was present in the sovereign Iranian computer network.

While the investigation of the possible technical measures leading to cessation is beyond the scope of this chapter, it should be noted stopping a continuing wrongful cyber operation is not always as simple as triggering the kill switch. This is particularly true in the case of DDoS operations, which, once launched, flood the network systems with data from a great number of various sources and the orchestrator does not always control the participants once the operation is underway. To make things even worse, these sources are not always personal computers; in October 2016, a previously mentioned DDoS operation coming from more than 10 million Internet connected cameras seriously disrupted several major commercial web services.[22] A target could very well be the governmental systems of Estonia, for example. While there is no indication that this was indeed a State-orchestrated operation, it illustrates the potential issues with the performance with the legal obligation of cessation.

Cessation is only the first step towards compliance and peace. In addition to the termination of an ongoing violation, the obligations consequential to the State responsibility seek to secure compliance also in the future. Depending on the circumstances, the wrongdoing State may accordingly be required to provide assurances or guarantees of **non-repetition**.[23] Assuring future compliance contributes to the rebuilding of trust and strengthens the rule of law, which in turn provides peace and security.

---

[22] Symantec Security Response, 'Mirai: what you need to know about the botnet behind recent major DDoS attacks' (*Symantec*, 27 October 2016) <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks> accessed 28 July 2019

[23] *ARSIWA* (n 8) art 30

Shelton[24] and the ARSIWA commentary[25] list examples of State practice where non-repetition guarantees or assurances were demanded and both sources offer a similar conclusion; the situations requiring assurances or guarantees of non-repetition are defined by a significant risk of repetition. Considering that technological advancement democratised and simplified the act of breaching international obligations and considering that the risk of repetition is indeed high, the State responsible for the wrongdoing should promise or guarantee non-repetition. Particularly when the responsible State has either a track record of similar violations[26] or is in possession of offensive cyber capabilities. In addition to the significant risk of repetition, logic would dictate that the duty to assure or guarantee non-repetition also in the case of instantaneous wrongdoing that has already concluded or ceased. Since in the case of the concluded unlawful act the duty of cessation is irrelevant, the least the wrongdoing State could do is offer an apology in the form of a guarantee to comply with the law in the future.

Assurances of non-repetition that an injured State may demand can take the form of verbal declarations while the guarantees should amount to something more tangible. As pronounced by the ICJ in the LaGrand case,[27] the form of the guarantee is left to the discretion of the responsible State although an injured State may be able to demand specific measures.

An effective dissolution of the governmental cyber group responsible for the wrongful operation is one example of a guarantee of non-repetition. Handing over the details of the vulnerabilities exploited in the unlawful inter-State cyber operation would also be an appropriate guarantee of non-repetition since it would give the injured State an opportunity to patch the exploitable software features and thus prevent future operations using the same

---

[24] Dinah Shelton, 'Righting Wrongs: Reparations in the Articles on State Responsibility' (2002) 96(4) AJIL 833, 845

[25] ILC, 'Materials on the Responsibility of States for Internationally Wrongful Acts' (UN Legislative Series, 2012) UN Doc ST/LEG/SER B/25, art 30 cmt 9

[26] Considering that China, Russia and Iran are suspected to be responsible for almost three quarters of all the publicly known State-sponsored cyber operations, non-repetition assurances and guarantees can be rightfully be demanded from one of those frequent wrongdoers. *See* Council on Foreign Relations, 'Cyber Operations Tracker data' <https://www.cfr.org/interactive/cyber-operations/export-incidents?_format=csv> accessed 28 July 2019

[27] *LaGrand (Germany v United States of America)* (Merits) [2001] ICJ rep paras 124–125

vectors of system breach. Moreover, handing over a web domain hosting malware could constitute a partial guarantee of non-repetition in the context of cyber operations. To illustrate, three web domains were crucial for the performance of Shamoon. In particular, http://mol.com-ho.me was used in the initial phishing operation, which lured the Aramco employees into the installation and execution of said malware. As of January 2017, it was still targeting Saudi public entities. According to IBM, 'an anonymised registrant' registered the domain[28] but if the American attribution of the operation to the Iranian authorities is credible, the Iranian authorities may give the guarantee in the form of handing over the domain to Saudi Arabia. This would halt the propagation of the malware using the current malware injection methodology but not also completely disable Iran from distributing the Shamoon malware in the future.

The issue, however, is that promises are easily broken, especially in cyberspace where operations go frequently undetected. What is more, guarantees of non-repetition can easily be circumvented[29] and a State determined to seek illegitimate power through cyber operations against another nation can hardly be stopped. Considering the State's decision to pursue illegitimate power maximisation in the first place and the fact that denial of attribution or responsibility by the wrongdoing State is common, it is unlikely the obligation of cessation and non-repetition will have any effect on its behaviour.

In addition to the obligations of cessation and non-repetition explicitly dictating present and future compliance or restoration and maintenance of peace, the law of State responsibility also relies on the operation of law to restore the prior power relationship and alter the non-compliance cost benefit calculation of the wrongdoers. This is the function of the third secondary obligation – the one of **reparation**.

---

[28] Kevin Albano & Limor Kessem, 'The Full Shamoon: How the Devastating Malware Was Inserted into Networks' (*IBM*, 15 February 2017) <https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks> accessed 28 July 2019

[29] By registering a new, similar domain and continue with the phishing and infection stages of a cyber operation, for example.

The fact that a breach of international duties warrants reparation is, as per the PCIJ Factory at Chorzów judgment, 'a principle of international law, and even a general conception of law'.[30] What is more, during the preparatory deliberations leading to the codification of the law of State responsibility, the ILC considered reparation to be a central obligation of the international responsibility of the wrongdoing State.[31] The position was heavily influenced by Anzilotti, whose oft-cited theorising of the international law of State responsibility focused on the obligation of reparation and eluded the questions of inducing compliance. After the commission of the unlawful act a new legal relationship emerges 'between the State to which the act is imputable (that State being under a duty to make reparation) and the State with respect to which there exists an unperformed obligation (this State having a claim to reparation)'[32] argued Anzilotti. The prominence of reparations as a main consequence of the State responsibility for the violation of its international duties is also apparent in the aforementioned Chorzów case, adjudicated in the time of Anzilotti's presidency to the Court in 1928. For him, reparation was not about compliance since 'the ultimate reason why States comply with the rules set by their common will is not a legal reason, but an ethical idea.'[33]

While it is said that Anzilotti 'liberated the international law of State responsibility from the question of enforcement',[34] reparation is in fact an important mechanism of inducing compliance. It should, as much as possible, 'wipe out all the consequences of the illegal act'.[35] In the context of the theoretical underpinnings set in the previous chapter, the reversal of the benefits derived from the violation and the re-establishment of the material situation as it existed prior to the occurrence of the violation renders the cost benefit calculation of the non-

---

[30] *Chorzów Factory Case* (n 4) 29
[31] ILC, 'Report on International Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur' (1956) II Ybk of the ILC UN Doc A/CN.4/96, 180–181
[32] Dionisio Anzilotti, *Corso di Diritto Internationale* (vol 1, 3rd edn, Athenaeum 1928) 416 *cited in* F.V. Garcia-Amador, *Recent Codification of the Law of State Responsibility for Injuries to Aliens* (Brill 1974) 9
[33] Dionisio Anzilotti, *Scritti di Diritto Internazionale Pubblico* (CEDAM 1956–7) 243 *cited in* Giorgio Gaja, 'Positivism and Dualism in Dionisio Anzilotti' (1992) 3 EJIL 127
[34] Georg Nolte, 'From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Inter-state Relations' (2002) 13(5) EJIL 1083, 1087
[35] *Chorzów Factory Case* (n 4) 48

compliance irrational. Indeed, there is no point in unlawful maximisation of power resources if it should be promptly reversed or compensated for. The consequences of the reparation in full should, in theory, have the same effect as the reactive violation States pursue to regain the lost power but without the side-effect of normative deterioration.

Because an unlawful inter-State cyber operation is not a self-serving act of rebellion but a means of increasing the State power,[36] wiping out the newly introduced imbalance of power is an important aspect of accountability and the only truly effective method of inducing compliance. For example, the termination of RedOctober and the consequential cessation of unlawful appropriation of diplomatic archival documentation would not be a sufficient consequence of legal responsibility to induce future compliance if the wrongdoing State would get to retain the illegitimate relative gains of power in a form of the harvested diplomatic secrets. Violation would still be a profitable outcome for the perpetrating State and a rational choice in the future. Restoration of power balance, on the other hand, would change the rational choice of the perpetrating State and therefore provide peace and security by rendering present and future non-compliance irrational.

Three forms of reparation are recognised by the law of State responsibility – restitution, compensation and satisfaction. All of them constitute undesired costs attached to the illegitimate power maximisation, counterbalancing the benefits of non-compliance and thus theoretically eliminating the benefits of the unlawful cyber conduct. Although the law of State responsibility emphasises the priority of restitution, reparation must be done in full,[37] regardless of the (combination of) method(s). Only reparation in full will erase the benefits of the unlawful conduct and be effective in changing the rational choice of the wrongdoing party and induce future compliance.

---

[36] *See* ch 2
[37] *ARSIWA* (n 8) art 34

Restitution, 'being the re-establishment of the situation which existed before occurrence of the wrongful act'[38] is the preferred[39] reparation method. It dictates the reversal of the illegitimate power gains, thus rendering violation a waste of time and resources. Restitution is not always possible nor is it practical simply because the status quo ante cannot always be restored. If a foreign national is killed due to the unlawful conduct of the State, restitution cannot be achieved, for example.[40] While it may very well be an appropriate reparation method in the context of this thesis, attributes of cyber operations may inhibit the restitution from fulfilling its role as a fitting reparation method. Specifically, when the cyber operation erases computer data, as it did in the case of the Shamoon malware, restitution in kind is not a viable form of reparation. Also, one of the examples of restitution offered by the ARSIWA commentary is the return of unlawfully acquired documents.[41] While, in the context of cyberspace, this may be as easy as the click of a mouse, it cannot always be considered an appropriate and sufficient reparation. Archives taken during the RedOctober operation, for example, were never really removed from the storage drives of the targeted diplomatic establishments; the wrongdoing State copied the content and transferred it to a remote location, therefore increasing its power by gaining knowledge of the other State's secrets, duplicating documents etc. Even if the documents were returned, the damage is irreparable, and restitution cannot re-establish the power relationship between the parties to the conflict.

When restitution is not possible, reparation can take the form of compensation, satisfaction or both.[42] Intended to erase the 'financially assessable'[43] loss of power sustained by the injured State, compensation aims to make amends for the damages by a proportional[44] repayment

---

[38] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ rep para 273
[39] *Chorzów Factory Case* (n 4) 48; *ILC* (n 25) art 35 cmt 3
[40] In its memorial to the ICJ, Paraguay argued that in case it's national is executed pursuant to the local judgement in the US. *Vienna Convention on Consular Relations (Paraguay v United States of America)* (Request for the Indication of Provisional Measures, Order of 9 April 1998) [1998] ICJ Rep para 8
[41] *ILC* (n 25) art 35 cmt 5
[42] *Pulp Mills on the River Uruguay* (n 39) para 273. See also *Chorzów Factory Case* (n 4) 48
[43] *ARSIWA* (n 8) art 36(2)
[44] *Mixed Claims Commission (United States and Germany)* (Opinion in the Lusitania Cases) [1923] VII UNRIAA (No. 1956.V.5) 32, 39

with interest.[45] Considering the context of this thesis is cyber operations below the use of force, damage consequential to the unlawful cyber operation is likely to result in decreased economic power, rendering compensation a suitable reparation method. As already explained, Iran as well as Saudi Arabia sustained significant economic damages due to the disruption of their oil industries by their respective cyber operations. A similar conclusion can be made in the case of the 2007 DDoS operation and the economic consequences it had on the Estonian banking sector. In addition to the neutralisation of damage, compensation should also reimburse the expenses incurred during the mitigation and reconstruction phases of the cyber incident. Once again, if the intention of the wrongdoing State is to minimise the economic power of the adversary, adequate compensation would revert the effects of the unlawful act.

Not all unlawful cyber operations however result in a financially assessable injury and can be compensated for. When restitution and compensation fail to provide acceptable reparation, injured States can request satisfaction. As per Special Rapporteur Ruiz, 'apologies, with the implicit admission of responsibility and the disapproval of and regret for what has occurred; punishment of the responsible individuals; a statement of the unlawfulness of the act by an international body'[46] or similar appropriate modalities of satisfaction may successfully make amends for the nonmaterial injury caused by the wrongdoing. Indeed, the ICJ has repeatedly argued that its judgment in favour of the applicant serves as a form of satisfaction.[47] Satisfaction is therefore a symbolic reparation, imposing reputational costs, thus decreasing the soft power of the responsible State. A regretful apology, diminishing the State's international reputation, would be an effective and proportional satisfaction for a cyber operation that caused nothing but reputational damages of the injured State. As such, it would

---

[45] *ARSIWA* (n 8) art 38

[46] ILC, 'Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur' (1989) II(1) Ybk of the ILC UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1, para 139

[47] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43; *Application of the Interim Accord of 13 September 1995 (The Former Yugoslav Republic of Macedonia v Greece)* [2011] ICJ Rep 644. Mind that, a judgment of an international tribunal usually also institutes the restoration of relative power through its imposition of reparation or of an award of damages.

neutralise the illegitimate soft power gains obtained by the wrongdoing State. For a breach causing anything beyond the loss of 'honour, dignity and prestige',[48] on the other hand, satisfaction can only be considered an adequate reparation when complemented by compensation or restitution.

4. Enforcing mechanisms and international law

In the absence of a central enforcement authority and in the light of a positive cost benefit calculus of the wrongdoing, a State in breach of its primary obligation is unlikely to be compelled into compliance and restoration of the power relationship as demanded by State responsibility. The secondary obligations of cessation, non-repetition and reparation assume a certain degree of agreement between the injured State and the wrongdoing State in regard to the acts in breach of international responsibilities. They assume the acceptance of responsibility by the allegedly perpetrating State.

As of 2018, instances of accepting the international responsibility, in the context of unlawful cyber operations, have not been publicly recorded; we are yet to see a situation where a State admits to a internationally wrongful cyber operation let alone complies with the secondary duties of cessation and reparation. Investigation of the cyber operations aimed at the disruption of US electoral systems in 2016 indicates that the American administration indeed reached out to the Russian Federation and demanded cessation. The latter not only denied the allegation but the operation has not ceased.[49] In the anarchical community of distrust, assurances of non-repetition are of questionable value as well. This is particularly true in the case of cyber operations. Rational States must be well aware of this inefficiency of the secondary obligations to provide restoration of power relationships and to advance the rule of

---

[48] Nina HB Jorgensen, 'A Reappraisal of Punitive Damages in International Law' (1997) 68(1) British Ybk of Intl L 247, 264

[49] Michael Riley & Jordan Robertson, 'Russian Hacks on U.S. Voting System Wider Than Previously Known' (*Bloomberg*, 13 June 2017) <https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections> accessed 28 July 2019

law. This is why, as explained previously, ill-intended States see the imposition of costs as improbable. And this is why the injured parties seek to regain power and security by reactive, unlawful cyber operations.[50]

Restoration of the previous power relationship and compliance with international law should therefore be lawfully enforced. If Anzilotti considered reparations to be the primary consequence of State responsibility, Kelsen was a firm believer in the concept of law as a coercive order. He promoted the idea of enforcement,[51] a reactive and lawful interference in the sphere of the wrongdoing State's interests, as the most important consequence of an established State responsibility. Taking the form of reprisals and war, the aim of an enforcement mechanism is to coerce the responsible State to adhere to the prescribed, socially desired conduct. Kelsen was very adamant about the fact that such mechanisms can assume the role of an enforcement mechanism only when they may be accompanied by the 'admissibility of employing physical force'.[52]

Under the contemporary international law, a State, whose rights were violated by a conduct below the use of force, is not permitted to induce compliance of the State responsible for the unlawful (cyber operation) by way of force. Nevertheless, international law does offer a number of non-forceful enforcement mechanisms, all of which rely on the imposition of undesired costs and therefore the alteration of the cost benefit calculation of the wrongdoing States to induce compliance.

First and foremost, compliance can theoretically be enforced by way of **international adjudication**. Indeed, States have generally responded to the ICJ decisions with compliance, which indicates its relative efficiency in resolving issues of non-compliance with international

---

[50] *See* ch 2
[51] Which he called *sanctions*. Hans Kelsen, *Principles of International Law* (Lawbook Exchange 2003) 5–33
[52] *Kelsen* (n 51)

law.[53] The reason behind this lies in the inflation of the non-compliance costs and the consequential alteration of the rational choice of the wrongdoer, imposed on it by the tribunal's decision. Although I have previously shown that reduction of reputation is not enough for a rational State to reconsider its unlawful cyber behaviour,[54] a cost to reputation[55] administered not by an injured State lacking any tangible attribution evidence but by an authoritative and impartial tribunal with a strict adherence to the established principles and standards of international law, would appear to be an exception to this rule. In addition to cost to reputation, international adjudication imposes the reduction of economic power or complete reversal of the power gains though an order of reparations and award of damages, which render the non-compliance irrational.

However, due to the aforementioned lack of common ground between the parties to a cyber conflict and the requirement of consensual jurisdiction, the success of the international judiciary to secure compliance of the States responsible for the unlawful cyber operations is unlikely. Specifically, the supreme status of sovereignty in international law prevents the ICJ from judging on the case without the consent of the involved parties.[56] In the Case of the Monetary Gold Removed from Rome in 1943, the ICJ stated that 'to adjudicate upon the international responsibility of Albania without her consent would run counter to a well-established principle of international law embodied in the Court's Statute, namely, that the Court can only exercise jurisdiction over a State with its consent'.[57]

---

[53] *See eg* Constanze Schulte, *Compliance with Decisions of the International Court of Justice* (OUP 2004) 436 & 437; Sara Mitchell & Paul Hensel, 'International Institutions and Compliance with Agreements' (2007) 51(4) American J of Political Science 721, appendix (published at <http://www.paulhensel.org/comply.html> accessed 28 July 2019)

[54] *See* ch 2

[55] As argued by the court, ICJ judgment itself provides satisfaction, a form of reparation, to the injured State. See *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 47) 239; *Application of the Interim Accord of 13 September 1995* (n 47). Satisfaction, as I have argued previously is an imposition of reputational costs.

[56] Statute of the International Court of Justice (San Francisco, 24 October 1945) art 36

[57] *Monetary Gold Removed from Rome in 1943 (Italy v France, United Kingdom of Great Britain and Northern Ireland and United States of America)* (Judgment) [1954] ICJ Rep 19, 32

Compliance may also be achieved by way of **sanctions**. While "sanctions" seems to be a popular choice of terminology by either political theorists,[58] journalists[59] or sometimes even governmental entities[60] in labelling the positive and negative reactions of a single State or a collective of them against the wrongdoing State(s), contemporary legal terminology classifies sanctions as (institutionalised) collective enforcement measures employed by a specialised international machinery[61] or 'an organ legally empowered to act in the name of the society or community'.[62] As Pellet and Miron put it, '[f]or the sake of clarity it seems therefore more appropriate and operational to define sanctions as socially organised acts of constraint'.[63] Aimed at the non-performing State, these include peaceful as well as forceful reactions with punitive or compliance-inducing function.[64] The UN Security Council and its broad mandate to impose measures 'to give effect to its decisions[65] comes to mind, for instance. Much like other compliance-inducing measures, sanctions constitute a deprivation of power in order to alter the cost benefit calculation of a rational wrongdoer. The previously mentioned reaction of the EU freezing the assets of Russia in response to the unlawful 'annexation of Crimea and deliberate destabilisation of a neighbouring sovereign country'[66] is an example of a sanction. It aimed to reduce the economic power of Russia and alter the cost benefit calculation of the unlawful territorial expansion in order to force Russia's hand into compliance.

---

[58] See *Kelsen* (n 51); David Baldwin, 'Inter-Nation Influence Revisited' (1971) 15(4) J of Conflict Resolution 471, 477; Karl W Deutsch, *The Analysis of International Relations* (Prentice–Hall 1968) 18

[59] Jeff Mason, 'Obama sanctions Russia for intervening in 2016 election' (*Reuters*, 29 December 2016) <http://www.reuters.com/article/us-usa-russia-cyber-obama-idUSKBN14I1W2> accessed 29 July 2019

[60] US Department of the Treasury, 'Cyber-related Sanctions: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Executive Order 13694), as amended' (29 December 2016) <https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber> accessed 29 July 2019

[61] Nigel D White & Ademola Abass 'Countermeasures and Sanctions' *in* Malcolm D Evans, *International Law* (4th edn, OUP 2014) 554

[62] Georges M Abi-Saab 'De la sanction en droit international' in Jerzy Makarczyk (ed), *Theory of International Law at the Threshold of the 21 Century* (Kluwer 1996) 71

[63] Alain Pellet & Alina Miron, 'Sanctions' in *Max Planck Encyclopedia of Public International Law* (August 2013)

[64] ILC, 'Eighth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur. The internationally wrongful act of the State, source of international responsibility (continued)' (1979) II(1) Ybk of the ILC UN Doc A/CN.4/SERA/1979/Add.I (Part 1) 39–47

[65] Charter of the UN (San Francisco, 26 June 1945) arts 41, 42

[66] 'EU sanctions against Russia over Ukraine crisis' (*European Union Newsroom*) <europa.eu/newsroom/highlights/special-coverage/eu-sanctions-against-russia-over-ukraine-crisis_en> accessed 29 July 2019

The fact that UN Security Council sanctions can form a lawful enforcement mechanism, also in the context of the cyber operations constituting 'threat to the peace, breach of the peace, or act of aggression',[67] has already been convincingly demonstrated by Roscini.[68] Also, from the standpoint of rational choice theory, the methodology of inducing compliance by way of multilateral sanctions is also effective; sanctions can inflict, for instance, undesired financial costs and reduce the economic power the wrongdoing State, rendering the unlawful cyber operation irrational.

Nevertheless, the present chapter argues against the multilateral or institutional enforcement measures for a very particular reason. Considering that sanctions imply an agreement between various States, depend 'on the existing political consensus within that body and on various configurations of power and State interests'[69] and frequently serve 'as a symbol of international unity and resolve in the face of lawless conduct,' [70] the prospect of these criteria being met in the cyber era is questionable. Specifically, there is no international unity in the matters of inter-State cyber operations and the scope of the application of international law to the new domain. Granted, agreement on collective sanctions may be more likely in the context of homogenous international communities, for example, the EU, though we are yet to see them. Moreover, the selfish behaviour of States in the cyber era and the consequential lack of unity of the interests between States renders the institutional enforcement mechanisms improbable. Intergovernmental organisations do not operate with a mind of their own but act upon the decisions of the collective membership. As former US Secretary of State Albright puts it, 'effective enforcement depends less on what institutions do than on what the members of those institutions have the will to do. And what States have the will to do will depend on

---

[67] *Charter of the UN* (n 65) art 39

[68] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 110–116. See also Nicholas Tsagourias, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' (2012) 15 Ybk of Intl Humanitarian L 37 & 38

[69] Vera Gowlland-Debbas, 'Security Council Enforcement Action and Issues of State Responsibility' (1994) 43(1) Intl and Comparative L Quarterly 55, 63

[70] Madeleine Albright, 'Enforcing International Law' (1995) 89 Proceedings of the Annual Meeting (ASIL) 574, 576

what it is in their interests to do'.[71] Considering the arguments above and the fact that sanctions take time to negotiate, the feasibility of timely reactions in the context of blazingly fast cyber operations is highly questionable.

Under these circumstances, I turn to compliance inducing measures of self-help. Firstly, **reprisals** were once thought to be the main instrument of enforcing compliance in the event of a breach of international obligations. The classic understanding of the concept of reprisals is found in the Naulilaa Incident Arbitration of 1928, which was tasked to resolve a dispute between Germany and Portugal. The court defined reprisals as 'a measure of self-help taken by the injured State in reply to an act contrary to the law of nations on the part of the offending State' with the objective 'to compel the offending State to make reparation for the injury or to return to legality, by avoiding further offences.'[72] In spite of the fact that the court limited the application of reprisals as being 'by the experiences of humanity and by the rules of good faith'[73] it has not ruled out the use of force as part of the reprisals. The notion of potentially forceful reprisals aimed at enforcing compliance with the primary legal obligations as well as the obligation of reparation for the consequences of the wrongs has been further promoted by the scholarship, namely Kelsen[74] and Oppenheim.[75] However, later developments of the international law have outlawed reprisals involving the use of armed force in the absence of Security Council authorisation. Reprisals are nowadays understood as belligerent reprisals and the term is reserved to designate the 'action taken in time of international armed conflict'.[76] The fact that the investigation of this thesis is limited to the non-forceful inter-State cyber operations should be a sufficient reason why this text does not consider reprisals to be an appropriate compliance enforcement methodology.

---

[71] ibid
[72] *Naulilaa Arbitration (Portugal v Germany)* [1928] II UNRIAA (Sales No. 1949.V.1) 1011, 1025 & 1026
[73] ibid
[74] *Kelsen* (n 51)
[75] Lassa Oppenheim, *International Law: A Treatise* (vol II, Longmans 1952) 136
[76] *ILC* (n 25) 304

Inflation of costs consequential to the unlawful conduct and thus enforcement of compliance with international law can be achieved also by way of **retorsion**, which constitutes a reaction of unfriendly[77] nature and as such does 'not interfere with the target State's rights under international law'.[78] Measures qualifying as retorsion may include, *inter alia*, severance of diplomatic relations,[79] official protests or withholding foreign aid.

Because the gravity of the reaction in the form of retorsion is far from the gravity of the initial injury, effects of the action and the reaction on power of the parties to the conflict exhibit similar symptoms of disparity. Being the mildest form of the self-help measures, retorsion will often inflict damage to the reputation of the responsible State. Particularly so when the official protests are public. Yet, as indicated in the preceding chapter, reputational costs inflicted by the injured State do not exhibit a proportional relationship with the injury cyber operations normally cause and thus have no tangible effect on compliance with international law.

For this very reason, official protests, a common form of retorsion, have previously proven to be futile. For example, in 2013 the US Congress acknowledged that 'numerous computer systems around the world, including those owned by the US government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military'[80] and President Obama publicly boasted about the official protests with Chinese government over the unlawful inter-State cyber operations.[81] In spite of that, two years later the Chinese Ministry of State Security, so claims the US Congressional report,

---

[77] ibid

[78] Thomas Giegerich, 'Retorsion' in *Max Planck Encyclopedia of Public International Law* (March 2011) <opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983?prd=EPIL> accessed 29 July 2019

[79] For example, in 2014 EU cancelled EU–Russia summit and withheld the support of the Russian membership in the OECD in the wake of the Ukraine crisis. 'EU restrictive measures in response to the crisis in Ukraine' (*Council of the EU*, 20 March 2014) <http://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis> accessed 29 July 2019

[80] US-China Economic and Security Review Commission, '2013 Annual Report to Congress' 13th US Congress (1st Sess, 20 November 2013) 245 <https://www.uscc.gov/Annual_Reports/2013-annual-report-congress> accessed 29 July 2019

[81] 'We've made it very clear to China and some other state actors that, you know, we expect them to follow international norms and abide by international rules.' 'President Obama upbraids China over cyber attacks' *BBC* (13 March 2013) <www.bbc.co.uk/news/world-us-canada-21772596> accessed 29 July 2019

infiltrated the US Office of Personnel Management and got a hold of 'fingerprints of 5.6 million people, some of which could be used to identify undercover US government agents or to create duplicates of biometric data to obtain access to classified areas'.[82] In other words, the disparity between the action and reaction resulted in a disparity between their consequences; the US traded US government computer data for a dent in Chinese international reputation in 2013; China, satisfied with this exchange rate, thus proceeded with the unlawful enterprise.

This should come as no surprise; the fact that only **reciprocal** self-help measures hold the potential to effectively induce compliance has already been proven by the experimentation of game theorists. In the context of a bilateral Prisoner's Dilemma, a form of game theory employed to predict the behaviour of rational actors, reciprocity of countermeasures is the key factor in determining the effectiveness of their instrumentality in enforcing compliance. With the help of 63 game theorists and computer simulations, Axelrod set to determine what kind of behavioural strategy brings the biggest rewards to the rational participant in the bilateral game of the Prisoner's Dilemma. Briefly, this derivative of the rational choice theory aims to determine the optimal behaviour[83] of the actor(s) in bilateral strategic relationships where two actors (for example, States) are presented with two choices – to cooperate (to comply with the law) or to defect (to violate the law). In the matrix of four possible outcomes (defect – defect; cooperate – defect; defect – cooperate; cooperate – cooperate) each of the actors is awarded a scenario-specific utility.[84] The investigation of compliance with the help of game theory is particularly useful when the actors 'pursue their own self-interest without the aid of [a] central

[82] US-China Economic and Security Review Commission, '2016 Annual Report to Congress' 14th US Congress (2nd Sess, 16 November 2016) 292–298 <https://www.uscc.gov/Annual_Reports/2016-annual-report-congress> accessed 29 July 2019

[83] Oskar Morgenstern, 'Game Theory: Theoretical Aspects' in David L Sills (ed), *International Encyclopedia of the Social Sciences* (vol 6, Macmillan 1968) 62

[84] Moshe Hirsch, 'Game Theory, International Law, And Future Environmental Cooperation in the Middle East' (1998-1999) 27 Denver J of Intl L and Policy 75, 79–81

authority to force them to cooperate with each other',[85] which happens to be a definitive characteristic of anarchic international relations.[86]

As one can imagine, there are a number of possible strategies players can choose to follow in the iterative game. But the one that deserves special attention in the previously outlined theory of international relations and the context of compliance in the cyber era is the Downing's descriptive[87] strategy, marked by a selfish and pragmatic maximisation of outcomes. This strategy, corresponding to the behaviour of a selfish State focused on power-maximisation, tries to understand the reactions of the adversary and base its conduct in the bilateral game on this. The strategy judges the responsiveness of the other player; the actor utilising this strategy seeks maximum individual utility by estimating the probability of the other party to cooperate in the case of its own cooperation or defection. Based on this premise, the player will 'try to get away with whatever it can by defecting'[88] or, in the present context, by violating international law. To ensure compliance of these selfish utility maximisation actors, Axelrod's experiments have shown, that they must be met with a reaction or change in strategy; defecting actors will continuously choose defection when no alteration of strategy is observed on the other end.[89] The sooner the reaction, the better.[90] And what is most important in this context is that a successful strategy ensuring compliance of the selfish Downing's approach to Prisoner's dilemma is reciprocal. In the realm of game theory known as Tit-for-Tat, the reciprocity strategy is straightforward – a player utilising this strategy starts cooperatively and then meets each choice of the opponent thereafter with the equivalent response or put simply, the player will 'do whatever the other player did on the previous move'.[91]

---

[85] Robert Axelrod, *The Evolution of Cooperation* (Basic Books 1984) 6
[86] *See* ch 2
[87] The outcome maximisation strategy explains what actors do and not what they should do. *See* Leslie L Downing, 'The Prisoner's Dilemma Game as a Problem-Solving Phenomenon: An Outcome Maximisation Interpretation' (1975) 6(4) Simulation and Games 366, 366–367
[88] *Axelrod* (n 85) 34
[89] *Downing* (n 87) 374
[90] *Axelrod* (n 85) 184–185
[91] Robert Axelrod, 'More Effective Choice in the Prisoner's Dilemma' (1980) 24(3) J of Conflict Resolution 379, 382

Following the recipe of Axelrod, States injured by the cyber operation must therefore not remain passive but react to the selfish maximisers. To be effective in inducing compliance or cooperation of the wrongdoer, reactions must not only be swift but also reciprocal or equal to the initial wrongdoing; a violation must be met with a violation. Only reciprocal consequences will erase the power benefits of the unlawful act.

5. Countermeasures, their instrumentality and proportionality

Countermeasures, the final enforcement mechanism to be considered in this chapter, are the only feasible, lawful and effective enforcement mechanism having the potential to enforce compliance with international law in the event of the unlawful inter-State cyber operation below the use of force. Three arguments are put forward in support of this reasoning. Firstly, countermeasures are measures of self-help and, in contrast to international adjudication and multilateral sanctions, are unrestrained by the divisive state of international cyber affairs. Secondly, and unlike retorsion, countermeasures epitomise a reciprocal strategy advocated for by game theory, and are proven to be effective in inducing compliance of the rational, selfish actors in an anarchical international community. A reciprocal strategy, a violation for a violation, is truly effective insofar that it leads to the restoration of prior relative power relationship and hence renders non-compliance irrational. To achieve that, deprivations of power inflicted by countermeasures must be commensurate with the benefits enjoyed by the wrongdoer. However, because strict reciprocity is not practical nor a requirement of the law, countermeasures can also be proportional. Thirdly, being an established legal instrument of the restoration of power precluded from wrongfulness, proportional countermeasures are an instrument, employed to induce compliance without contributing to the erosion of law and escalation of the conflict. This cannot be claimed for the currently practiced restoration of

power by States injured by a cyber operation.[92] After a brief introduction to the doctrine of countermeasures, the following paragraphs explain the last pair of arguments in detail.

Countermeasures are an established compliance inducing mechanism of the international law of State responsibility; in the context of this chapter, countermeasures are not a technical measure intended to stop, deflect or even punish cyber perpetrators although there is admittedly a practical overlap between the two concepts of countermeasures. For the purpose of this thesis and in the context of international law, a countermeasure is a reciprocal conduct in contravention of the international rights of the responsible State, the wrongfulness of which is precluded by the preceding breach of obligations by that very State. Plainly, countermeasures are the reciprocal reactions of a State deprived of its legal right – a breach for a breach, a denial of the international legal rights for a denial of the international legal rights. Just what the game theory prescribed.

Countermeasures are an **instrumental** deprivation inflicted upon the internationally responsible State, employed by the injured State to procure compliance. This means they may not serve the punitive aim. Forming an enforcement mechanism through deprivation of legal entitlements, countermeasures are highly reminiscent of punishment[93] and analogous with the punitive enforcement methodology employed by domestic legal systems. While the deprivation inflicted by the countermeasures 'will come close to being a penalty inflicted by the injured State',[94] international customary law is clear – countermeasures are neither in service of retribution nor are to be employed for the purpose of punishment. Due to the primacy of the principle of sovereign equality of the States[95] and the nature of international law 'as a

---

[92] *See* ch 2

[93] The similarity is especially apparent when taken into consideration definitions of punishment. *See eg* Nicola Lacey, *State punishment* (Routledge 1988) 7–8, defining *punishment* as '[a]n imposition of unpleasant consequences on the State adjudicated to have breached the law as a response or with the purpose of enforcement'.

[94] ILC, 'Fourth report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur' (1992) ILC Ybk II(1) UN Doc A/CN.4/444 and Add.1–3, 7

[95] *ILC* (n 46) paras 140–141

law between, not above**,** sovereign States',[96] punishment is not an appropriate form of self-help.

The instrumental character of countermeasures also dictates that such measures are precluded from their wrongfulness only when 'carried out – after an unfulfilled demand – in response to an act contrary to the law of nations by the offending State'.[97] If not taken in reaction to a prior unlawful conduct, they constitute a violation of the international obligations; '[t]hey would be illegal if an earlier act, contrary to the law of nations, had not furnished the motive'.[98] The requirement of the pre-existing unlawful conduct has been confirmed by the Air Service Agreement[99] and Gabčikovo Nagymaros[100] and Cysne cases. In the latter case, the arbitration tribunal was explicit – countermeasures, 'which constitute an act in principle contrary to the law of nations, are defensible only insofar as they were provoked by some other act likewise contrary to that law'.[101] Following this rationale, normally unlawful State conduct becomes lawful; 'the wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State'.[102] Thus, otherwise unlawful coercion or compulsion of a responsible State in the form of countermeasures becomes a permitted enforcement method. In spite of the similarity in methodology and their shared objective, the lawful nature of countermeasures is what distinguishes them from the usual law-eroding reactive violations of international law currently practiced by the States injured by cyber operations.[103] In contrast to the popular reactions by the injured States indicated in the

---

[96] Lassa Oppenheim, *International Law: A Treatise* (vol 1, Ronald Roxburgh (ed), 3rd edn, Lawbook Exchange 2005) 249
[97] *Naulilaa Arbitration* (n 72) 1025
[98] ibid
[99] *Air Service Agreement of 27 March 1946 between the United States of America and France* [1978] XVIII UNRIAA 417, 493 para 84
[100] ibid para 83
[101] *The Cysne Arbitration (Portugal v Germany)* [1930] II UNRIAA (Sales No. 1949.V.1) 1011, 1056–1057.
[102] *ARSIWA* (n 8) art 22. See also *ILC* (n 64) 40
[103] *See* ch 2

preceding chapter, countermeasures, the instrumentality of which is communicated with the responsible State,[104] will not perpetuate the conflict or weaken the rule of law.

Although the ARSIWA provides that countermeasures are instrumental, and thus lawful, when taken with the objective of inducing compliance of the responsible State with its secondary obligations of cessation, non-repetition and reparations,[105] the exact mechanics of how compliance with secondary or primary obligations comes about is not addressed by the Articles or the accompanying commentary.

However, in the context of rational choice theory, instrumental countermeasures are a temporary and reciprocal denial of legal rights allowing the injured State to inflict a deprivation of power on the responsible State and restore the power relationship between the parties that existed prior to the conflict. By doing so, countermeasures change the cost benefit calculation of the responsible State and render non-compliance irrational, which forces the rational wrongdoing State to cease the unlawful conduct, thus restoring peace and security.

To claim that the inducement of the secondary obligations arising from State responsibility is the primary consequence of lawful countermeasures, is therefore a simplistic understanding of the instrumentality of countermeasures, ignoring the modalities of the rational actors' behaviour in anarchical international relations. It is hereby submitted that, by effectuating the aim of reparations, countermeasures induce compliance with the cessation and non-repetition thus ensuring present and future compliance with the primary obligations under the international law. In other words, by way of inflation of the costs of the wrongdoing State through countermeasures, the injured party itself fulfils the aim of reparations, which induce present and future compliance with the primary obligations, which is what the secondary obligations of cessation and non-repetition attempt to achieve.

---

[104] Which is also a requirement of the law. *See ARSIWA* (n 8) art 52; ch 6
[105] See eg *ARSIWA* (n 8) art 49(1)

Game theory prescribes reciprocal reactions because it is presumed that the countermeasure depriving the initially wrongdoing State of the equal legal right should indeed result in an equal deprivation of relative power and therefore effectively render the non-compliance irrational. It is presumed that qualitatively reciprocal countermeasures will result in quantitative reciprocity of the countermeasures, indeed wiping out all the relative power benefits initially claimed by the wrongdoing State during the unlawful cyber operation for which it is internationally responsible for.

If game theory prescribes reciprocity of countermeasures in the name of effectiveness, international law favours reciprocity in its effort to limit potential abuse of the legal instrument and prevent punitive or non-instrumental reactions by the injured State. The international legal doctrine indicates that the reciprocity of countermeasures – ones which 'correspond to, or are directly connected with, the obligation breached'[106] – is their preferred[107] characteristic. It is assumed that a reactive denial of the same international rights as violated by the initial wrongdoing will also bring about a relative power deprivation equal to the relative power gains of the wrongdoer. And nothing more.

Yet absolute reciprocity may hinder the effectiveness of countermeasures, a fact recognised also by the international customary law. Since it is not always possible or even permissible, strict reciprocity is not a necessity under the law of State responsibility; '[t]here is no requirement that States taking countermeasures should be limited to suspension of performance of the same or a closely related obligation'.[108] The State injured by RedOctober, for example, is not permitted to respond by way of reciprocal countermeasures and withhold the performance of its obligations part of the international diplomatic law related to the inviolability of foreign official agents, premises, archives and documents, which are considered

---

[106] ILC, 'Sixth report on the content, forms and degrees of international responsibility (part two of the draft articles); and "Implementation" (mise en oeuvre) of international responsibility and the settlement of disputes (part three of the draft articles), by Willem Riphagen, Special Rapporteur' (1985) II(1) Ybk of the ILC UN Doc A/CN.4/389 and Corr.1 & Corr.2, 10 art 8

[107] *ILC* (n 25) 306 para 5

[108] ibid

to be a self-contained regime and therefore not to be targeted by countermeasures.[109] Additionally, the game theory experimentation is of binary nature and hardly reflects every effective option of law enforcement. In the real world, absolute reciprocity of countermeasures may hinder their effective instrumentality if they do not result in a deprivation of power that has any significance to the wrongdoing State. And, frankly, the situation in which the reciprocal countermeasures inflicting power deprivations equal to the deprivations sustained during the unlawful cyber operation has more to do with fiction than reality; a violation of sovereignty in return for a violation of sovereignty, for example, may result in as small as a stolen PDF file or as large as a severe economic loss.[110]

Because of these shortcomings, international law permits a degree of flexibility and does not dictate absolute reciprocity of reactions or countermeasures but their proportionality. The requirement of proportionality has been stipulated in the several international adjudications[111] and was finally codified in the ARSIWA article 51. From a legal standpoint, limitation of proportionality is installed in order to prevent countermeasures from assuming the role of punishment and to avoid escalation of the conflict. The 'principle of proportionality and the other limitations placed on the injured State's *faculte* of [countermeasures] should be adequate to prohibit any qualitative or quantitative overreaction on the part of the injured State',[112] which would designate the punitive aim of the State employing them. In contrast to reciprocity, the principle of proportionality does not dictate strict equality between the countermeasures and the wrongful act which furnished the lawful motive for employing them but indicates harmony between them.[113]

---

[109] *ARSIWA* (n 8) art 50 (2b). Note that this absolutism has been a target of a convincing criticism by Bruno Simma & Dirk Pulkowski, 'Of Planets and the Universe: Self-contained Regimes in International Law' (2006) 17(3) EJIL 483

[110] *See* ch 1

[111] *Naulilaa Arbitration* (n 72) 1028

[112] *ILC* (n 94) 7 para 5

[113] Elizabeth Zoller, *Peacetime Unilateral Remedies* (Transnational Publishers 1984) 97

Since 'there is no uniformity […] in the practice or the doctrine as to the formulation of the principle'[114] at hand, proportionality of countermeasures is said to be 'an inexact science.'[115] Certainly, a universal definition or legal standard of proportionality cannot be precisely determined in a theoretical setting and should depend on the particular circumstances of the conflict. Be that as it may, a common denominator of proportionality conceptualised by international jurisprudence and the scholarly contributions is a delicate balance between the effectiveness of countermeasures and prevention of abuse of this self-help mechanism.

Franck, on one hand, argues that proportionality governs the relationship between the countermeasures and the initial wrongful act.[116] This approach, the primary concern of which is that countermeasures are not excessive[117] or punitive in their nature, is supported by the codification of the law of State responsibility by the ILC[118] and the international jurisprudence. Accordingly, considerations related to the proportionality must go beyond the quantitative assessment of their consequences on the State power or the consequences of the initial wrongdoing; besides the material aspects of the material injuries suffered, the State wishing to employ proportional countermeasures should take into account the scope of the legal injury or the contextual importance of the obligation breached.[119] In this sense, countermeasures and the initial violation ought to exhibit not only qualitative but also qualitative proportionality. This has been clearly expressed by the Air Services arbitration[120] and by the ICJ in the

---

[114] ILC, 'Report of the International Law Commission on the work of its forty-seventh session (2 May-21 July 1995)' (1995) II(2) UN Doc A/CN.4/SER.A/1995/Add.l (Part 2), 65

[115] Rodger O'Keefe, 'Proportionality' in James Crawford, Alain Pellet & Simon Olleson, *The Law of International Responsibility* (OUP 2010) 1165

[116] Thomas M Franck, 'On Proportionality of Countermeasures in International Law' (2008) 102(4) AJIL 715–767

[117] *Naulilaa Arbitration* (n 72) 1028; Michael Newton & Larry May, *Proportionality in International Law* (OUP 2014) 186: 'Proportionality in the law of countermeasures is best understood as a prohibition against excesses rather that a requirement for equivalence or mathematical equity.'

[118] *ARSIWA* (n 8) art 51; commentary in *ILC* (n 25)

[119] *Air Service Agreement of 27 March 1946 between the United States of America and France* (n 99) para 83. Crawford argues that a State wishing to take countermeasures has to consider 'the importance of the interest protected by the rule infringed and the seriousness of the breach'. James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries United Nations* (CUP 2002) 296

[120] In deliberating on proportionality, one needs to take 'into account not only the injuries suffered by the companies concerned but also the importance of the questions of principle arising from the alleged breach.' *Air Service Agreement of 27 March 1946 between the United States of America and France* (n 99)

Gabčíkovo-Nagymaros Project case,[121] where Czechoslovakia's countermeasure, breaching a well-established legal principle protecting every State's 'right to an equitable and reasonable share of the natural resources',[122] was considered to be disproportionate when put against the initial Hungarian violation of the bilateral treaty regulating the joint construction project on the Danube river.

In deliberating the qualitative and quantitative aspects of proportionality in countermeasures, the former takes precedence. Accordingly, quantitative disproportionality between the consequences inflicted by the initial wrongful act and the consequences of countermeasures does not necessarily result in disproportionate, thus unlawful, countermeasures. As stipulated in the Air Services arbitration award and reiterated in the ARSIWA commentary, countermeasures are proportional 'even if they were rather more severe in terms of their economic effect'[123] than the initial violation. What is more important is the approximate 'legal equivalence between the breach and response'[124] or, in other words, that the importance of the rights targeted by countermeasures is proportional to the importance of the rights protected by the initially violated obligation.

This is not to say that quantitative proportionality should be neglected; in the interest of effectiveness, consequences of countermeasures must be in fact proportional with the consequences of the initial wrongdoing, 'taking into account [not only the rights in question but also] the gravity of the internationally wrongful act'.[125] Since the real benefit of non-compliance is an inexpensive and fast inflation of State power, the injured State must make sure to fully effectuate the aim of the obligation of reparation, therefore depriving the wrongdoing State of the relative power gains consequential to the breach of international law by way of a cyber

---

[121] '[T]he effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.' *Gabčíkovo-Nagymaros Project (Hunngary/Slovakia)* [1997] ICJ Rep para 85
[122] ibid
[123] *ILC* (n 25) art 51 cmt 3
[124] Enzo Cannizzaro, 'The Role of Proportionality in the Law of International Countermeasures' (2001) 12(5) EJIL 889, 900
[125] *ARSIWA* (n 8) art 51

operation. It can only do so by way of countermeasures in quantitative proportion with the relative loss of power incurred during the cyber operation.

Therefore, lawful and effective countermeasures will be qualitatively and quantitatively proportional with the initial breach of the obligations by way of a cyber operation; it will deprive the responsible State of its legal right in proportion to the legal injury the targeted State sustained as well as of its relative power in proportion to the reduction of power caused by the initial breach. Only then will a countermeasure constitute an undesired cost of the rational State commensurate with the benefits of the breach, non-compliance with the law will lose the appeal and become irrational.

When the consequences of countermeasures are proportional with the consequences of the initial breach, they are also proportional with their purpose. As a matter of fact, a group of prominent scholars advanced the idea that proportionality does not denote the relationship between the violation and countermeasures but between the purpose of countermeasures and the countermeasures themselves. Zoller,[126] Elagab,[127] Riphagen,[128] Cannizzaro,[129] Dawidowicz[130] and Cassese are some of the authors emphasising the supreme importance of the effective instrumentality of countermeasures. Cassese, for example, argued that 'the proportionality must be appraised by establishing whether the countermeasure is such to obtain [the] purpose'[131] of compelling the wrongdoer to comply with its international obligations. In contrast to the position of the ILC,[132] the fact that the purpose of countermeasures, i.e. inducement of the restoration of legal and material relationship, is a

---

[126] *Zoller* (n 113) 135–136
[127] Omer Yousif Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Clarendon Press 1988) 64–79
[128] *ILC* (n 106) 11
[129] *Cannizzaro* (n 124) 899: 'Essence of proportionality resides in comparing the measures adopted with the proper function of the action of self-redress.'
[130] Martin Dawidowicz, *Third-Party Countermeasures in International Law* (CUP 2017) 362–365
[131] Antonio Cassese, *International Law* (2nd edn, OUP 2005) 306
[132] *ILC* (n 94) para 56

factor in determining the proportionality of the instrument is supported by several ILC members, *opinio juris* of States as well as State practice.[133]

Even though the difference between the theoretical approaches seems to be apparent, from a standpoint of a rational choice theory, the two are not all that dissimilar. Countermeasures that exhibit quantitative proportionality between the initial wrongdoing and the reactive deprivation of rights and power resources, revert the newly-established change of power ratio, rendering the non-compliance irrational and thus living up to their purpose of instrumentality. In other words, countermeasures that are quantitatively proportional with the initial wrongdoing are also effectively instrumental and therefore proportional with their purpose – to induce compliance.

Although some have argued that smaller States will find it nearly impossible to inflict sufficiently proportional deprivation of power resources to effectively coerce the hegemons to comply,[134] cyber means and the flexible nature of the principle of proportionality alleviate this concern. Due to the fact that cyber operations are a distinctively asymmetrical threat, they do allow even weak States to employ quantitatively proportional countermeasures and therefore inflict a proportional deprivation of power and secure compliance of the hegemon. These normative limitations on the scope of countermeasures do not need to be a disadvantage of the injured State but an opportunity to reactively withhold the performance of the obligation of its own choosing, one that not only corresponds to its (cyber) capabilities and resources but also holds superior potential to induce compliance of the wrongdoer. Additional flexibility and an opportunity to employ efficient countermeasures against the responsible State regardless of its might is a notable absence of a prescription dictating a particular form of countermeasures. This means that an inter-State cyber operation does not need to be countered by cyber means. Such interpretation of the law in the cyber domain finds support in

---

[133] *Dawidowicz* (n 130) 362–363

[134] Eliza Fitzgerald, Helping States Help Themselves: Rethinking the Doctrine of Countermeasures' (2016) 16 Macquarie L J 67, 81

the British *opinio juris*.[135] For instance, if the consequences of the initial cyber wrongdoing are a decrease of economic power, the injured State may consider appropriation of assets from the responsible State. In such cases, however, quantitative considerations in establishing proportionality become important and an injured State must make sure the consequences of countermeasures approximates[136] proportionality with the consequence of the initial violation and therefore alter the rational choice calculation of the non-compliance.

The momentary restoration of peace and relative power relationships is however not enough, especially if the breach has already concluded. Fortunately, countermeasures have the capacity to not only induce compliance but also deter violations of primary obligations therefore assuring peace provided by the rule of law also in the **future**. As such, countermeasures, by way of restoration of power relationship, do not only induce present compliance with the primary obligations of international law but also ensure non-repetition; regular employment of countermeasures and the subsequent cost inflation of the non-compliance should provide more assurance of the future behaviour of the rational States in comparison with their promises and guarantees consequential to the compliance with the secondary obligation of non-repetition. Until one day countermeasures become a 'self-fulfilling prophecy'[137] and are no longer needed.

As explained in the second chapter, it is not only the extent of costs but also the likelihood of incurring costs which determine whether the rational State will comply with its international obligations or not. Thus, a functional mechanism of countermeasures can have a deterrent effect on States wishing to pursue illegitimate power; 'a desire to avoid [the] costs is what provides the incentive to comply with the international law'.[138] Because the rational actors

---

[135] '[T]he UK could respond to a cyber intrusion through non-cyber means, and vice versa.' Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) <gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 12 August 2019

[136] '[J]udging the "proportionality" of countermeasures is not an easy task and can at best be accomplished by approximation.' *Air Service Agreement of 27 March 1946 between the United States of America and France* (n 99) para 83

[137] Michael W Reisman, 'The Enforcement of International Judgments' (1969) 63(1) AJIL 1, 7

[138] Andrew T Guzman, *How International Law Works: A Rational Choice Theory* (OUP 2010) 55

deciding whether to comply or not consider the potential of the costs to incur based on, *inter alia*, historical experience with the opposite side,[139] fear of negative consequences stemming from the established enforcement mechanism reinforced by the past behaviour of the target State 'will normally be a factor in the cost benefit-analysis of a State'[140] when considering an internationally wrongful act or omission. And established mechanism they are. As indicated in the previous chapter, States repeatedly claim application of international law in cyber domain and there is no real reason why the law of countermeasures would be excluded. In fact, the decision of the Council of the EU, for example, argues that 'clearly signalling'[141] the likelihood of countermeasures for the internationally wrongful cyber operations 'influences the behaviour of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States'.[142]

Due to the emergence of new technology-enabled methods of violations and consequential normative uncertainty, however, only employed mechanisms will fully assume the form of a deterrent. If employed regularly, countermeasures will aid in 'creating future expectations of effective enforcement in the international community'.[143] As already explained, rational States opt for non-compliance not only because of low costs but also because the possibility of incurring proportional costs is currently very low or not practiced by the injured States. Once the countermeasures in reaction to the unlawful inter-State cyber operations will be (consistently) employed, once countermeasures will move from theory to practice, their deterrence function will materialise. This will impact not only States wishing to repeat the unlawful maximisation of utility through cyber operations but also the ones considering taking this shortcut for the first time. By addressing the very motive behind the internationally wrongful

---

[139] *Downing* (n 87) 373
[140] *Giegerich* (n 78)
[141] Council of the European Union, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption' (Brussels, 7 June 2017) 9916/17, 5 <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> accessed 17 May 2019
[142] Ibid
[143] *Simma & Pulkowski* (n 109) 509

act, countermeasures as a deterrent, have a greater impact on the future rule of law than promises and doubtful guarantees of non-repetition.

6. Conclusion

Unlawful cyber operations negatively affect the relative power of the injured State and prompt the deterioration of the relevant international norms and the decline of peace. The present chapter finds a solution to both consequences from the international law of State responsibility, which, upon the occurrence of the unlawful breach of international obligations, imposes two corresponding secondary obligations, cessation and reparation.

The former is more or less a restatement of the requirement of present and future performance with the primary obligations breached by the unlawful cyber operation, while the latter aims to re-establish the power relationship between the parties prior to the conflict. Experience, however, indicates that the wrongdoing States are unlikely to admit the wrongdoing, let alone comply with the secondary obligations.

To enforce the obligations, the injured State has several lawful inducement mechanisms at its disposal. The chapter established that, only countermeasures are a feasible and appropriate compliance-inducing mechanism in the context of this thesis.

Countermeasures are not a punishment but an instrument to induce compliance with the international obligations. Whether they are reciprocal or proportional, the key is that they effectuate the objectives of the secondary obligation of reparation, therefore reverting the change in power relationship between the States consequential to the unlawful cyber operation and therefore altering the calculation of the non-compliance, rendering it irrational. Additionally, lawful countermeasures must also exhibit qualitative proportionality and as such be in approximate equivalence with the importance of legal rights violated by the initial breach.

By altering the cost benefit calculus of the wrongdoing States, proportional countermeasures remove the incentive of violation and thus enforce compliance with the primary legal

obligations of the nonperforming State. And, if employed regularly, even assume the role of a deterrent and promote the rule of law in the future.

This chapter centres more on the content and the corollary duties of State responsibility and less on the issues of implementation. This issue is addressed extensively in the following chapters.

Chapter 4

Attribution of cyber operations

1. Introduction

With the intention to induce compliance with international law, nations injured by internationally wrongful cyber conduct should turn to countermeasures. In the context of the rational theory of international relations, this legal self-help mechanism, previous chapters have established, is instrumental in reducing the profits of the perpetrating State and, consequentially in decreasing the occurrence of unlawful cyber events endangering peace and security.

In order to employ countermeasures, a cyber operation must be directly or indirectly attributed to a particular (group of) State(s). Following successful attribution of the cyber operation in question, the injured State has to establish the operation's unlawful character. There can be no exceptions to this dual structure of State responsibility for the internationally wrongful act.[1]

The following paragraphs contextualise and expose the limits that the established doctrine of the international law of State responsibility imposes on the injured State in the endeavour to employ countermeasures in reaction to the unlawful State sponsored cyber conduct. In other words, the present text evaluates whether the current legal framework allows for the attribution of unlawful inter-State cyber conducts.

Getting attribution right is important. Sophisticated malicious tools and techniques 'increase the risk of mistaken attribution and unintended escalation'[2] and countermeasures based on misattribution constitute a breach of international obligations. To avoid escalation, attribution must be supported by evidence. To establish what kind of evidence would satisfy the

[1] ILC, 'Materials on the Responsibility of States for Internationally Wrongful Acts' (UN Legislative Series, 2012) UN Doc ST/LEG/SER B/25, art 2 cmt 9

[2] UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98, 7

requirements of current relevant legal frameworks, the present text evaluates the existing interpretations – burden of proof, forms of evidence, reasoning by inferences and standards of proof – against the unlawful cyber operations.

2. Doctrine of attribution

Attribution[3] has attracted extensive legal debate[4] and the evolution of legal standards pertaining to State responsibility has been anything but painless.[5] What is more, the introduction of malicious inter-State cyber operations on the everyday agenda of international relations puts pressure on the existing doctrine to accommodate this new environment.

Attribution indicates an ascription of an unlawful act of a natural person to a State.[6] The State is an abstract concept and a social construct. To the jurist, it is 'commonly defined as a community which consists of a territory and a population subject to an organised political authority'.[7] As such, a State cannot conduct an unlawful act without the intermediate involvement[8] of individuals. Attribution is therefore the legal process of establishing whether a given conduct 'of a physical person […] is to be characterised […] as an act of State';[9] legal attribution seeks to establish the responsibility in law.

---

[3] The analysis of the evolution of the doctrine reveals early texts spoke of the *imputability* rather than of *attribution*. *See eg* ILC, 'Second report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The origin of international responsibility' (1970) II Ybk of the ILC, UN Doc A/CN.4/SER.A/1970/Add.1, 189: 'the term "imputability" has no other meaning than the general meaning of a term linking the wrongful action or omission with its author'. See also *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep paras 51, 53, 54. 'Attribution' is the preferred term of the modern international law. Crawford argued that, in order 'to avoid any suggestion that the legal process of connecting conduct to the State was a "fiction"', '[t]he term "attribution" should be retained.' ILC, 'First report on State responsibility, by Mr. James Crawford, Special Rapporteur' UN Doc A/CN.4/490 and Add. 1–7, 33.

[4] *Eg* Antonio Cassese, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' (2007) 18(4) EJIL 649–668

[5] *See eg* James Crawford, *State Responsibility: The General Part* (CUP 2013) 141–161

[6] *See* Luigi Condorelli & Claus Kress, 'The Rules of Attribution: General Considerations' *in* James Crawford, Alain Pellet & Simon Olleson (eds), *The law of international responsibility* (OUP 2010) 221

[7] Alain Pellet, 'The Opinions of the Badinter Arbitration Committee: A Second Breath for the Self-Determination of Peoples' (1992) 3(1) EJIL 178, 182

[8] *Crawford* (n 5) 113

[9] *Condorelli & Kress* (n 6) 221

The following paragraphs offer an insight into the process and challenges of legal attribution of cyber operations and attempt to elaborate why this particularly challenging task[10] remains 'one of the most significant challenges to deterring malicious operations in cyberspace'.[11]

2.1. Identification of the actors – reverse engineering of the cyber operation

Legal literature discussing attribution of cyber operations has largely focused on the theoretical association of the perpetrating entity with a State. While this is, due to the aforementioned cumulative double structure requirements of the international law of State responsibility, of absolute necessity, identification of the (group of) natural person(s) conducting the operation is a task of a significant if not higher importance. This is a first step in the attribution process, as the individuals are the ones that, by utilising a computerised system, create and/or send information packets with the intention to achieve a desired malicious action in a foreign computer network system.

While the establishment of such claims for the purpose of legal attribution in the context of State responsibility for the unlawful cyber operation may be achieved through different methods of proof,[12] State practice on this matter tends to rely mostly on the outcomes of technical analysis.[13] The attribution methodology in the following paragraphs shall follow suit

---

[10] Different legal scholars acknowledge the issue but do not discuss the matter in great detail. *See eg* Michael N Schmitt & Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) 1(2) Fletcher Security Rev 54; Scott Shackelford & Richard Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2014) 42(4) Georgetown J of Intl L 971; Katharine C Hinkle, 'Countermeasures in the Cyber Context: One More Thing to Worry About' Yale (2011) 37 Yale J of Intl L Online 17 <https://bit.ly/33I55TN> accessed 12 August 2019; Susan W Brenner, '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) J of Crim L & Criminology 379. See also *UNGA* (n 2) 6

[11] 'Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.3: Concept Framework' [MNE7] (Version 3.0, 3 October 2012) 19 [on file with the author]. The document is a product of Austria, Canada, Denmark, Finland, France, Germany, Great Britain, Hungary, Italy, Republic of Korea, Norway, Poland, Spain, Sweden, Switzerland, the United States and NATO.

[12] See the discussion on evidentiary issues below.

[13] US Federal Bureau of Investigation, for example, used the technical analysis outcomes to establish the individuals from Democratic People's Republic of Korea were behind the cyber operation which crippled Sony in 2014. FBI National Press Office, 'Update on Sony Investigation' (*Federal Bureau of Investigation*, 19 December 2014) <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> accessed 1 April 2016. Furthermore, US used 'verifiable and attributable data' of technical nature to attribute the cyber espionage to five members of the Chinese People's Liberation Army. US Department of Defence, 'The Department of Defense Cyber Strategy' (April 2015) 12

as well as present various attribution models sometimes considered an alternative to computer science.

In order to determine the natural person behind the cyber operation one needs to, first, identify the tool or the computer used to produce and launch the malicious operation, which is usually established by tracking the Internet Protocol (IP) addresses[14] or Autonomous System Number (ASN).

Transfer on the internet is conducted through the transmission of packets of data, each up to 65 kilobytes in size.[15] The properties information of each data packet contains, *inter alia*, the source and destination addresses. These are given as IP addresses where the first three numbers indicate the network number, while the following three number segments point to a participant at a local network.[16] Given that an IP address reveals (an approximate) geographical location of the network participant[17] as well as the identification of the corresponding Internet service provider (ISP), cyber operations are usually traced back to the author through this identifier.[18] Other methods, such as tracking the ASN, may point to the ISP and territory of origin but not the actual computer behind the operation.

---

[14] Harry Henderson, *Encyclopedia of Computer Science and Technology* (Infobase Publishing 2009) 468

[15] Information Sciences Institute University of Southern California, 'DOD Standard: Internet Protocol' (Prepared for US Defense Advanced Research Projects Agency, January 1980) 21 <https://tools.ietf.org/html/rfc760> accessed 1 April 2018

[16] ibid 7 & 14

[17] There are different technical approaches to this. *See eg* Chuanxiong Guo et al, 'Mining the Web and the Internet for Accurate IP Address Geolocations' in *2009 Proceedings IEEE INFOCOM* (Institute of Electrical and Electronics Engineers April 2009) 2841; Ethan Katz-Bassett et al, 'Towards IP geolocation using delay and topology measurements' in *IMC '06 Proceedings of the 6th ACM SIGCOMM* (ICM October 2006) 71; Brian Eriksson et al, 'A learning-based approach for IP geolocation' *in* Arvind Krishnamurthy & Bernhard Plattner (eds), *Passive and Active Measurement* (Springer 2010) 171; Yong Wang et al, 'Towards Street-Level Client-Independent IP Geolocation' in *Proceeding NSDI'11 Proceedings of the 8th USENIX conference on Networked systems design and implementation* (USENIX March 2011). Examples of commercial applications of IP-based geolocation data include Google location-specific services (https://support.google.com/websearch/answer/1696588) and Microsoft Windows location aware applications (http://goo.gl/KWJoKo).

[18] Don Cohen & K Narayanaswamy, 'Survey/Analysis of Levels I, II, and III Attack Attribution Techniques' (Cs3, April 2004) 6

IP address was used, for example, to officially attribute a cyber operation aimed at Sony.[19] Similarly, the United States (US) Department of Justice relied on the IP address when attributing various malicious cyber operations to members of the China's People's Liberation Army (PLA) in the indictment of 2014.[20] Moreover, private security company Mandiant accused PLA members of 'systematic cyber espionage and data theft'[21] based on the fact that 98% of the IP addresses that accessed the perpetrator controlled systems were Chinese and used by the PLA cyber Unit 61398.[22] Attribution claims based on the IP address of the cyber operation controlling system are particularly popular among journalists.[23] Similar reliance on the IP information for the purpose of attribution is present in a number of relevant academic writings.[24]

Be that as it may, besides the issues of potentially falsified IP information and a number of other ways[25] in which the source of the unlawful cyber operation can be decoupled from the IP address, the IP address of a computer changes, depending on the network participation. In the era of mobile computing and widely available public wireless connectivity, identification of a source computer based on IP tracing is especially problematic as IP information points at

---

[19] *FBI National Press Office* (n 13)
[20] *US v Wang Dong et al* (Indictment, No. 14–118 W.D. Pa., 1 May 2014) <https://goo.gl/RHm0Fh> accessed 1 April 2016
[21] Mandiant, 'APT1 – Exposing One of China's Cyber Espionage Units' (Mandiant, February 2013) 7 <http://goo.gl/H3IkzR> accessed 1 April 2016
[22] ibid 40
[23] *See* eg AP, 'South Korea traces cyber-attacks to Chinese IP address' *Guardian* (21 March 2013) <http://goo.gl/7FUKia>; Kim Zetter, 'Everything We Know About Ukraine's Power Plant Hack' (*Wired,* 20 January 2016) <http://goo.gl/DkScZ2>; Michael Gold, 'Taiwan a "testing ground" for Chinese cyber army' (*Reuters*, 18 July 2013) <http://goo.gl/tJ7Psp>; Nicole Perlroth, 'Hackers in China Attacked The Times for Last 4 Months' *New York Times* (30 January 2013 <http://goo.gl/OMxZ4u>; 'Estonia says cyber-assault may involve the Kremlin' *New York Times* (Tallinn, 17 May 2007) <http://goo.gl/tSSlxx>; 'China IP address link to South Korea cyber-attack' *BBC* (21 March 2013) <http://goo.gl/aL0NP7> all accessed 1 April 2016
[24] *See eg* Earl Boebert, 'A Survey of Challenges in Attribution' *in* National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (The National Academies Press 2010) 44–45; Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' *in* Jens David Ohlin, Kevin Govern & Claire Finkelstein (eds), *Cyber War* (OUP 2015) 235–237; Michael Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54(3) Virginia J of Intl L 698, 708
[25] For an overview of such techniques *see eg* Jeffrey Hunker, Robert Hutchinson & Jonathan Margulies, 'Attribution of Cyber Attacks on Process Control Systems' *in* Papa M & Shenoi S (eds), *Critical Infrastructure Protection II. ICCIP 2008* (vol 290, Springer 2008) 15

the geographical location of the network infrastructure used in the operation and not necessarily the computer utilised. Finding a specific computer used in a cyber operation is also problematic in denial of service (DoS) attacks, employed for example in 2007 to bring down the governmental systems of Estonia,[26] even though spoofing is usually not practiced in this type of cyber operations.[27] In a DoS attack, the so-called zombie machine[28] controlled by the perpetrator floods the target system with excessive data traffic and, by doing that, renders the target machine useless.[29] Advanced operations of such nature utilise a large collection of compromised computers or zombie machines, commonly known as botnet,[30] working in concert to overburden the targeted system. Quantity of participating machines in what is known as distributed DoS (DDoS) makes establishing the true origin of operation particularly difficult.

Under these circumstances, it is not surprising that the efforts to identify the computers used to conduct the Shamoon, RedOctober operations as well as the distributed DDoS launched on Estonia in 2007 provided no substantial outcomes.

In spite of the fact that Shamoon was an overt[31] cyber operation and, as such, rather unique, the authors of the operation left behind only an IP address of the proxy to the Command and Control server (CCS) and a computer network of 30,000 unbootable, unusable systems.[32] A malware module, reporting back to the CCS every five minutes[33] was connected to the

---

[26] *See eg* Christian Czosseck, Rain Ottis & Anna-Maria Talihärm, 'Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security' *in* Matthew Warren (ed), *Case Studies in Information Warfare and Security for Researchers, Teachers and Students* (Academic Conferences 2013) 73

[27] Jelena Mirkovic & Ezra Kissel, 'Comparative Evaluation of Spoofing Defenses' (2009) 8(2) IEEE Transactions on Dependable and Secure Computing 218, 218

[28] Susan Brenner, *Cyber Threats – The Emerging Fault Lines of the Nation State* (2009 OUP) 1

[29] Erik Rodriguez, 'HOWTO - Spoofed DoS Attacks' (*Skullbox*, 21 March 2011) <http://goo.gl/kwbq4K> accessed 1 April 2016

[30] 'Botnet' (*Radware*) <http://goo.gl/hcGg3Z> accessed 1 April 2016

[31] Instead of hiding the malicious code and its operation, the malware deleted portion of the computer disks, including all the information that would lead to the authors.

[32] Paul Roberts, 'Whodunnit? Conflicting accounts on ARAMCO hack underscore difficulty of attribution' (*Sophos*, 30 October 2012) <https://goo.gl/R8opxE> accessed 1 April 2016

[33] McAfee, 'W32/DistTrack, W64/DistTrack' (17 August 2012) 5 <https://goo.gl/mAZRTR> accessed 12 April 2016

machine internal[34] to the injured enterprise. Researchers believe the malware was introduced to the system via a removable media[35] while the alleged perpetrators claimed the operation was conducted remotely.[36] The aforementioned internal computer was therefore only a proxy and the address or location of the perpetrators' computer remains unknown.

More IP related information is known in relation to the RedOctober operation. Researchers were able to establish partial information related to the progression of the cyber operation while, as the following lines are being drafted, the identity of the perpetrators behind RedOctober still remain unknown. What is known however is that the perpetrators were likely to be Russian speaking individuals and that the malicious CCS domains were registered by email addresses of Russian origin. The IP addresses of some CSSs indicate that these machines were located in Germany and Russia[37] but only assumed the role of proxy CCSs; the location of the computer perpetrators actually operated from cannot be identified.

Similarly, the investigation into the exact computer source of the DDoS attack on Estonia proves to be a dead end. While the Tallinn government refrained from openly accusing the Russian authorities, its 'foreign ministry has published a list of IP addresses where the attacks were made from'[38] many of them pointing at cyber infrastructure located on Russian territory. Subsequent technical analysis indicates that the attacks came from no less than 20,000 computers spread across 178 different countries.[39] Considering the nature of the DDoS attack, IP addresses flooding the Estonian systems are of no definitive value when attempting to

---

[34] Dmitry Tarakanov, 'Shamoon The Wiper: Further Details (Part II)' (*Kaspersky Lab*, 11 September 2012) <https://goo.gl/7wPP44> accessed 1 April 2016

[35] US Department of Homeland Security, 'ICS-CERT Monthly Monitor' (September 2012) <https://goo.gl/ZzuDNZ> accessed 1 April 2016

[36] 'Untitled' (*Pastebin*, 17 August 2012) <http://pastebin.com/tztnRLQG> accessed 1 April 2016

[37] Global Research & Analysis Team, '"Red October" Diplomatic Cyber Attacks Investigation' (*Kaspersky Lab*, 14 January 2013) <securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/> accessed 19 April 2018

[38] 'The cyber raiders hitting Estonia' *BBC* (17 May 2007) <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> accessed 1 April 2016

[39] Roland Heickerö, 'Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations' (Swedish Defence Research Agency, 30 March 2010) 41 <http://goo.gl/bG6ljJ> accessed 1 April 2016

discover the exact source the aforementioned attack. While the initial IP address analysis designated that one of the attacks originated from Russian governmental network structures, the seemingly incriminating IP address 'could have just as easily been a spoofed address or [the machine was] compromised'.[40]

Even if the computer used to perpetrate an internationally wrongful cyber operation is successfully identified, according to the aforementioned prescribed legal process, attribution requires the identification of the natural person behind the keyboard. This is one of the most significant hurdles in establishing attribution to invoke State responsibility.

Since actions conducted through a computer do not include an identifier of a natural persons' authorship,[41] the link between a computer and the author of a cyber operation is formed through computer forensics which seeks to establish 'who was using the device at the time and whether they were in control of the device and responsible for actions taken on it'[42]. Relevant techniques include analysis of email natural language, keystroke timing analysis of the malware code and others.[43] Objects of a forensic analysis may be retrieved locally or remotely.

This stage in the attribution process is particularly problematic in the context of countermeasures; it is hard to imagine that the injured State would have the means to conduct a comprehensive forensic analysis on a computer network system located in the suspected wrongdoing State. Granted this may be performed remotely[44] but only with a limited degree of effectiveness.[45]

---

[40] Gadi Evron, 'Bating Bonets and Online Mobs' (2008) Winter/Spring, Georgetown J of Intl Affairs 121, 125

[41] Cyber actions are, therefore, again a *unicum*. Unlike, for example, US Supreme court judgment (Federal Republic of Germany et al vs. United States et al, 526 U.S. 111), which, according to the ICJ (*LaGrand (Germany v United States of America)* (Merits) [2001] ICJ rep paras 472–473) triggered a violation of international obligations, malware, as a tool of unlawful conduct, is not (explicitly) signed by the author.

[42] Andy Jones, T Martin, 'Digital forensics and the issues of identity' (2010) 15(2) Information Security Technical Report 67, 69

[43] *Cohen & Narayanaswamy* (n 18) 73

[44] *See eg* Jacob Pennock, Damon Smith & Geoffrey Wilson, 'Design and Implementation of a Remote Forensics System' (Mcafee Foundstone, 2 May 2005) <http://goo.gl/4eB7Bo> accessed 1 April 2016

[45] ibid

Attribution methodology does not need to be limited to technical analysis; there are a number of alternatives to attribution by means of computer science and related forensics. Tsagourias, for example, argues that attribution is a multifaceted process, which includes legal, technical and political aspects. According to the aforementioned scholar, these aspects combine technical investigation with intelligence and political assessments to form an attribution model fit for the cyber realm.[46] The attribution methodology includes the assessments of the political climate of the political entity suspected of the cyber operation orchestration and determines 'who benefited from the attack'.[47] Similar recognition of the political aspects of the attribution can be found in the Tallinn Manual on the International Law Applicable to Cyber Warfare.[48]

Beyond legal scholarship, the science of cyber security indeed offers a number of sophisticated threat agent modelling theories which, among many of the attack(er) parameters, also consider the political gains of the cyber operation orchestrator. For example, political attribution has been proposed by the Diamond Model of Intrusion Analysis. The approach focuses on the existing relationship between the perpetrator and the victim State and the motive of the perpetrator. The attribution is driven by the analysis of the social-political needs and aspirations of the perpetrator and the corresponding intentions of the malicious cyber operation in a wider political context.[49]

Furthermore, in seeking to attribute a cyber operation to a particular actor, Rid and Buchanan proposed the Q attribution model consisting of the technical, strategic and operational elements of the cyber operation. The political aspect of the attribution is apparent in the latter two elements, which include an evaluation of *inter alia* geopolitical context, examining 'specific regional, historical, and political knowledge about specific actors and their organisation'.[50]

---

[46] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' 17 (2012) J of Conflict and Security L 231–232
[47] ibid
[48] Michael Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 52
[49] Sergio Caltagirone, Andrew Pendergast & Christopher Betz, 'The Diamond Model of Intrusion Analysis' (Center for Cyber Threat Intelligence and Threat Research, Technical Report ADA586960, 5 July 2013) 20
[50] Thomas Rid & Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38(1–2) J of Strategic Studies 4, 23

However, these attribution attempts reach beyond the boundaries of political, technical and legal aspects. The aforementioned Q and Diamond models, in their pursuit of the attribution of cyber operations, take into account parameters such as targeting, infrastructure used in the operation, attributes of the malicious code and intrusion process, scope and stages of the operation as well as capability of the adversary. [51] Similarly, Vidalis and Jones developed an attribution model where the identification of the perpetrators follows the assessment of the nation State capability, opportunities and motivation.[52] Yet another example is the Threat Agent Library, a taxonomy of eight attributes which led the scholars to categorise 22 unique, theoretical perpetrators.[53] The classification of the agents was conducted after determining the intent and the access of the attacker, the outcome of the cyber operation (for example, theft, damage etc.), legal and ethical limits observed by the agent, human resources of the orchestrator, skill level, objective and visibility of the operation.[54]

States also seem to have recognised the attribution methodology not limited to technical analysis and computer science. The UN Group of Governmental Experts argued 'the perpetrators of [cyber] activities can only be inferred from the target, the effect or other circumstantial evidence'.[55]

Further analysis of the models, however, is of no significance. What is important are the outcomes or results the models offer. A combination of the aforementioned strategies may indeed lead to the specific State or natural person. And since inter-State cyber operations do not happen in a vacuum, political contextualisation is indeed a tempting attribution

---

[51] ibid 15–23; *Caltagirone, Pendergast & Betz* (n 49) 8–19

[52] Stilianos Vidalis & Andrew Jones, 'Analyzing Threat Agents & Their Attributes' in *Proceedings of the 5th European Conference on i-Warfare and Security* (Academic Conferences 2006) 10–14

[53] Cyber security science literature prefers the *(threat) agents* over *actors* or *persons*. 'The term threat agent is used to denote an individual or group that can manifest a threat.' ibid 6

[54] Timothy Casey, 'Threat Agent Library Helps Identify Information Security Risks' (Intel Information Technology White Paper, September 2007) 5–7 <https://goo.gl/I2d4bN> accessed 1 April 2016

[55] UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 July 2010) UN Doc A/65/201 1. Why the Group chose to use the word 'only', in spite of the fact that satisfactory technical evidence may very well emerge one day, remains unknown.

methodology. For instance, the 2007 DDoS operation was conducted in the wake of a political dispute between Estonia and the Russian minority, cyber operations targeting Georgia occurred during time of armed conflict with Russia, the attack on the Natanz uranium enriching facility accompanied the lasting conflict between the US, Israel et al and Iran concerning the latter's nuclear weapons ambitions. The political context in which the BlackEnergy malware erased a number of computer storage facilities pertaining to the Ukrainian electrical power industry[56] also provoked speculations that the operation had been consequential to the conflict between Ukraine and Russia and was thus attributed to the latter.

The limitations of the alternatives to technical attribution should however be noted. In fact, the inconclusive nature of the results has been recognised by the model authors themselves, leading many to claim attribution is more of an art than a science.[57] In particular, Intel's approach to attribution utilising the cross-referencing of the operations' attributes and the classified threat agents is limited to '[aiding] risk managers [to] identify which agents are relevant' and is not intended to identify individuals or to be used for investigating actual security events.[58] Rid and Buchanan, on the other hand, speak of high- and low-quality[59] attribution, but do not place their trust in their Q model to identify the perpetrators. And socio-political method results have been specifically criticised by the authors of Diamond model.[60] In fact, the shortcomings of the various attribution models have also been recognised by the Swiss national cyber security strategy, emphasising that the unambiguous legal attribution and conclusion on the motives of the perpetrators 'based on [various attribution] methods and tools, […] is often impossible'.[61] Socio-political methods of attribution can therefore point at the State that is *in fact* responsible for the unlawful cyber operation, at the State that *in fact*

---

[56] Chris Vallance, 'Ukraine cyber-attacks could happen to UK' *BBC* (London, 29 February 2016) <http://www.bbc.co.uk/news/technology-35686493> accessed 1 April 2016
[57] *Caltagirone, Pendergast & Betz* (n 49) 56; *Rid & Buchanan* (n 50) 7
[58] *Casey* (n 54) 5
[59] *Rid & Buchanan* (n 50) 7
[60] *Caltagirone, Pendergast & Betz* (n 49) 20
[61] Swiss Confederation, 'National strategy for the protection of Switzerland against cyber risks' (19 June 2012) 10

conducted or sponsored cyber operation and by doing so reaped the benefits in terms of relative power inflation. What socio-political approaches to attribution cannot reliably establish is the natural person behind the cyber operation.

Aside from the fact that results of non-technical attribution are of questionable quality, they can also be a product of subjective assessment and thus inappropriate in establishing legal responsibility. Since the international environment is populated by different cultures, values and factual perceptions, the socio-political approach to attribution is not a bias-free one. Consequently, countermeasures based on one's strategic assessments 'will often look like serious or hysterical misjudgement to some actors and like either cynical or self-deluded, naked aggression to others'.[62] Relying on the objective and neutral, science-based legal attribution has the potential to assure the otherwise self-interested and inherently biased injured States avoid misattribution and therefore unlawful countermeasures.[63]

Regardless of the methods employed, the decision whether to trust the outcomes of the legal attribution and to take countermeasures is ultimately on the injured State. Although socio-political attribution may indeed be useful and in fact frequently serves as a basis for taking measures of retorsion – unfriendly acts against the what is believed to be a responsible State – it is not an appropriate attribution method preceding the employment of countermeasures as it bears a serious potential to perpetuate and escalate the conflict. Since false attribution will result in unlawful countermeasures, it is of paramount importance that the injured State stays within the limits of the law. This means that the conclusions of any kind of attribution need to be evaluated against the legal framework of the attribution, including the law of proof to which I return shortly.

---

[62] Michael Reisman & Andrea Armstrong, 'The Past and Future of the Claim of Preemptive Self-Defense' (2006) 100 AJIL 525, 526

[63] For a critical evaluation of scientific contribution to the international law *see* Jacqueline Peel, *Science and Risk Regulation in International Law* (CUP 2010) ch 3 & 4

2.2. Establishing the nexus between the perpetrating actor with a State

Putting the aforementioned struggles of identifying the author of the unlawful cyber operation aside, the unlawful act of the (group of) individual(s) needs to be associated with a State before proceeding with countermeasures. As a 'general rule, the conduct of private persons is not attributable to the State'[64] and, as international jurisprudence indicates, 'a certain factual link between the State and the actor is required in order to attribute to the State acts of that actor'.[65]

Generally speaking, an unlawful cyber operation is attributable to a State if performed by an organ of the State, by actors exercising elements of governmental authority or organs placed at the disposal of a State by another State. This includes ultra vires acts. Additionally, a breach of international obligations performed by a movement, later becoming new government, and a conduct acknowledged and adopted by a State as its own also gives rise to State responsibility.[66]

In a world where 'the tendency for those in power to achieve their ends through private or non-State actors, thereby avoiding attribution'[67] is prominent, the establishment of the association of the perpetrating action with the State is especially important. In the light of this, special attention is paid to the attribution of unlawful conduct directed or controlled by a State.[68]

As established by international customary[69] law, the codification of the international law of State responsibility provides that '[t]he conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive,

---

[64] Alexander Kees, 'Responsibility of States for Private Actors' in *Max Planck Encyclopaedia of Public International Law* (March 2011) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1092> accessed 12 August 2019. See also *ILC* (n 1) ch II para 3

[65] *Noble Ventures, Inc. v Romania, Case No ARB/01/11* (award) ICSID (12 October 2005) para 82

[66] UNGA Res 56/83 'Responsibility of States for Internationally Wrongful Acts' (12 December 2001) UN Doc A/RES/56/83 (ARSIWA) arts 4, 5, 6, 7, 10, 11

[67] Gordon A Christenson, 'Attributing Acts of Omission to the State' 12 (1990) Michigan J of Intl L 312, 313

[68] *ARSIWA* (n 66) art 8

[69] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights* (Advisory opinion) [1999] para 62. *See* also *Claim of the Salvador Commercial Company ("El Triunfo Company")* [1902] UNRIAA XV 455, 477

judicial or any other functions'.[70] Such status shall be ascribed to a particular actor in accordance with the internal law pertaining to the State in question.[71] On this premise, the ICJ ruled that neither Republika Srpska nor its army, the perpetrators of the massacres in Srebrenica, 'were de jure organs of the [Former Republic of Yugoslavia], since none of them had the status of organ of that State under its internal law'.[72]

In that particular case, the contentious nature of the *internal law* and *State organ* definitions arose. The Court came to the abovementioned conclusion in spite of the fact that the Constitution of the Republika Srpska declared itself to be a part of Yugoslavia (later Serbia and Montenegro) and pronounced its citizens as nationals of Yugoslavia. The court argued perpetrators cannot be considered as organs of Yugoslavia in spite of the fact that the officers responsible for the atrocities were administered, paid and under the full control of the authorities of Yugoslavia.[73] All things considered, the conclusions the court arrived to were, according to Judge Mahiou, surprising and questionable.[74]

Several lessons can be learned from this. First and foremost, judicial standards indicate that internal legal provisions ought to be explicit in their recognition of the specific actor as the State organ. Additionally, control of the perpetrators by a particular State does not mean the actors in question are to be considered *de jure* organs of that State. Moreover, while the internal law includes 'laws and regulations adopted within the framework of the State, by whatever authority and at whatever level',[75] these legal provisions should be internal to the State the injured party is seeking to attribute an act to. In the abovementioned case Republika Srpska considered itself to be a part of Yugoslavia, although a reciprocal declaration was

---

[70] *ARSIWA* (n 66) art 4
[71] ibid. Tallinn Manual confirms the application of this legal provision. See *Schmitt* (n 48) 36
[72] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep para 386
[73] ibid para 238
[74] Constitution of the Republic of the Serb People of Bosnia and Herzegovina (28 February 1992) arts 3 and 6, *cited in* ibid (Dissenting opinion of Judge ad hoc Mahiou)
[75] *ILC* (n 1) art 3 cmt 9

absent from the law internal to the latter. For this very reason, the army of the Republika Srpska cannot be ascribed the status of an organ of Yugoslavia.

Taking into account the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) guidance on the subject matter, the Genocide decision of the ICJ may not be surprising after all. The ILC's codification commentary provides that the organs of a State are 'all the individual or collective entities […] of any territorial governmental entity *within the State* on the same basis as the central governmental organs of that State'.[76] Given the fact that Republika Srpska was part of Bosnia and Herzegovina[77] at the time of the Srebrenica massacres, its army could not have been an organ of the Federal Republic of Yugoslavia.

In the cyber context, internationally wrongful injurious acts performed by, for instance, the (members of the) US Army Cyber Command, a *de jure* organ established by the US Secretary of Defence Memorandum,[78] would give rise to the State responsibility of the US. Such agency could not however be established for the Cutting Sword of Justice, a group claiming responsibility[79] for the Shamoon operation. In spite of the absence of technical evidence,[80] submissions that Iranian authorities are to blame for the Shamoon operation have been proposed by scholars,[81] the abovementioned group does not enjoy the membership of the State apparatus and is not recognised by the legislation of the Islamic Republic of Iran. The

---

[76] ibid art 4 cmt 1 [emphasis added]
[77] ICJ argued 'The Republika Srpska never attained international recognition as a sovereign State, but it had de facto control of substantial territory, and the loyalty of large numbers of Bosnian Serbs': *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 235
[78] US Secretary of Defense, 'Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations' (23 June 2009) <http://goo.gl/TDTRLG> accessed 1 April 2016
[79] 'Untitled' (*Pastebin*, 15 August 2012) <http://pastebin.com/HqAgaQRj>; 'Separate cyber team to attack aramco, 12 days network down' (*Pastebin*, 25 August 2012) <http://pastebin.com/k2HFJ2LY> both accessed 1 April 2016
[80] *See* n 32 – n 37
[81] Christopher Bronk & Enken Tikk, 'Hack or Attack? Shamoon and the Evolution of Cyber Conflict' (James A Baker III Institute for Public Policy, Rice University Working Paper, February 2013) 22

group is nothing more but a self-proclaimed 'anti-oppression hacker group'.[82] As a matter of fact, Iran has explicitly denied[83] involvement in the cyber operation.

Similar absence of official inclusion in the State apparatus of the perpetrating entity can be assigned to the Russian government-sponsored non-governmental organisation[84] Nashi, suspected to have orchestrated the 2007 DDoS attacks on Estonia.[85] In spite of the fact that the organisation was conceived 'by Kremlin political technologists, patronised by leading figures in the presidential administration, and personally endorsed by President Putin',[86] Nashi cannot be labelled a *de jure* instrument of the State. Firstly, in the words of the Iran–US Claims Tribunal, the fact that 'the formation of the [perpetrating entity] was initiated by the State does not in itself imply that the [entities] were to function as a part of State machinery'.[87] Secondly, Nashi does not enjoy the same status and does not exhibit any degree of State authority as did the Foundation of the Oppressed in 1984 Iran.[88]

On the other hand, if it were true – in spite of the fact that the technical analysis does not provide for such evidence[89] – that the operation was conducted by the State Duma Deputy assistant Konstantin Goloskokov,[90] the responsibility of the Russian Federation may be established. This however remains subject to certain conditions. Before pointing

---

[82] *'Untitled'* (n 79)
[83] Al Arabiya, 'Iran denies role in cyberattacks against Gulf oil and gas companies' *Al Arabiya* (14 October 2012) <https://english.alarabiya.net/articles/2012/10/14/243682.html> accessed 1 April 2016
[84] Moises Naim, 'What Is a GONGO?' *Foreign Policy* (13 October 2009) <http://goo.gl/9FbNF1> accessed 1 April 2016
[85] According to some sources, Nashi 'has taken responsibility for the network attacks'. Noah Shachtman, 'Kremlin Kids: We Launched the Estonian Cyber War' (*Wired,* 13 November 2009) <http://goo.gl/OyIHL7> accessed 1 April 2016. Similar claims may be found in Jose Nazario, 'Politically Motivated Denial of Service Attacks' *in* Christian Czosseck & Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 163, 176. Note that on the other hand this has been officially denied by Nashi stating that '[i]f anything did happen, it was the personal initiative of Konstantin Goloskokov': Andrew Roche, 'Kremlin loyalist says launched Estonia cyber-attack' *Reuters* (13 March 2009) <http://goo.gl/Wcq4oe> accessed 1 April 2016
[86] Robert Horvath, *Putin's "Preventive Counter-Revolution": Post-Soviet Authoritarianism and the Spectre of Velvet Revolution* (Routledge 2013) 99
[87] *Schering Corporation and The Islamic Republic of Iran* [1984] 5 Iran-US CTR 361
[88] The Foundation of the Oppressed was found to be a *de jure* instrumentality of the State of Iran due to the fact that it was established by the State authorities, that its organs were appointed by the government and, most importantly, that it was empowered to perform certain degree of State functions. *Hyatt International Corporation v The Government of the Islamic Republic of Iran* [1985] 9 Iran-US CTR 88, 91–92
[89] *See* n 38 – n 40
[90] *Heickerö* (n 39) 42

countermeasures at Russia, Estonia would have to be able to present the evidence that Goloskokov, being an assistant[91] to the Duma deputy, was actually acting in the capacity of the Lower House of Federal Assembly of the Russian Federation, regardless of the fact if he was acting ultra vires or not.[92] Detailed analysis of the Russian internal law, proving that the Duma deputy assistant is indeed a State organ, would be essential. If the Russian Federation desired to avoid responsibility for the unlawful DDoS, it would have to prove that Goloskokov not only acted ultra vires but also that the State had no means to control his actions.[93] In reality, Goloskokov's claims of responsibility seem closer to provocative self-promotion rather than the truth.

Even when the perpetrator of the unlawful act cannot be equated with an organ of a particular State machinery, State responsibility may arise. This is well-established by the international customary law[94] as well as the relevant codification. Specifically, in 1996 the ILC recognised the State responsibility in the deeds of the perpetrating organs 'acting in fact on behalf of the State'.[95]

When internal law provides no indication of the nexus between the perpetrating entity and the allegedly responsible State, but the former is in complete dependence of the latter, attribution may still be established, and State responsibility claimed.

---

[91] The fact that Goloskokov was *only* an assistant to the Duma Deputy does not exclude him form the definition of a State organ. Acts of, for example, 'administrators of enemy property, mayors and police officers' have consistently been attributed to the State. See *ILC* (n 1) 33

[92] *Kenneth P. Yeager v The Islamic Republic of Iran* [1987] 17 Iran-US CTR 92, 110–111; *ARSIWA* (n 66) art 7. In fact, Goloskokov denied Moscow State infrastructure was used and that DDoS 'was his own initiative and he received no help either from Nashi or from Russian officials': *Roche* (n 85). *See also* Victor Yasmann, 'Russia: Monument Dispute with Estonia Gets Dirty' *Radio Free Europe* (4 May 2007) <http://goo.gl/fbSMLG> accessed 1 April 2016

[93] *Kenneth P. Yeager v The Islamic Republic of Iran* (n 92) 103–104

[94] See eg *Charles S. Stephens and Bowman Stephens (U.S.A.) v United Mexican States* [1927] UNRIAA IV 265, 267; *D. Earnshaw and Others (Great Britain) v United States* [1925] UNRIAA VI 160; Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (Advisory Opinion) [1999] ICJ Rep, para 62

[95] ILC, 'Draft Articles on State Responsibility with Commentaries Thereto' (adopted by the ILC on the first reading, January 1997) UN Doc 97-02583, 32

As pronounced by the ICJ in its 2007 judgment in the Genocide case, unlawful acts conducted by actors 'which are not formally recognised as official organs under internal law but which must nevertheless be equated with State organs because they are in a relationship of complete dependence on the State'[96] is sufficient to establish attribution to the State. In this particular judgement, the ICJ relied on the prior judgement of the same Court in the case concerning Military and Paramilitary Activities in and against Nicaragua.[97] In the context of this thesis and in accordance with the public information, neither the Cutting Sword of Justice nor Nashi exhibit complete dependence on the Iranian or Russian State. Acts of these non-State actors therefore cannot be attributed to either of the States.

In addition to the scenario where the perpetrating actor is *de jure* State organ or in complete dependence of the State, an unlawful act can be attributed to a particular State if it can be established that the perpetrating actor acted under the directions or control of that very State. This customary legal rule on attribution was codified in the final text of the ARSIWA; the article 8, believed to be 'particularly relevant in the cyber context',[98] asserts:

> The conduct of a person or group of persons shall be considered an act of a 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.[99]

The State responsibility may be invoked, it follows, when conditions of instruction, direction or control are fulfilled; the direction and control need to be integral to the unlawful act and not only 'incidentally or peripherally associated'.[100]

Judicial decision concerning State responsibility consequential to the State's instructions can be dated back to 1925. In the Zafiro case the court attributed an act of a civilian to the US on the basis of the fact that the ship captain was 'not to interfere particularly with the details of

---

[96] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 406
[97] ibid para 391
[98] *Schmitt* (n 48) 37
[99] *ARSIWA* (n 66) art 8
[100] *ILC* (n 1) art 8 cmt 3

the ship's routine, but to receive the Admiral's orders for the ship and see them carried out'.[101] Instructions imply orders in other decisions as well. Militants in Iran, for example, would be considered to be acting on behalf of the State of Iran should they have been 'charged by some competent organ of the Iranian State to carry out a specific operation'.[102] To raid the US embassy in Tehran and consulates in Shiraz and Tabriz that is. It follows that the instructions are given in relation to the specific act. The reasoning was explicitly confirmed by the ICJ in 2007; the State responsibility arises on the occasion when an organ of the State giving 'the instructions or [providing] the direction pursuant to which the perpetrators of the wrongful act acted'.[103] In the same vain Judge Ago spoke of the actors being 'specifically charged by the [State] authorities to commit a particular act'.[104] Instructions therefore 'establish an ad hoc relationship'[105] between the perpetrating party and the State.

Similar to an instruction, a direction involves a direct and specific order to perform a certain conduct.[106] Direction 'does not encompass mere incitement or suggestion but rather connotes actual direction of an operative kind'[107] yet it does not, like in some other languages than English, assume complete power over the actor.[108] According to Crawford it 'implies a continuing period of instructions, or a relationship between the State and a non-State entity'.[109] Although slight differences therefore exist, Courts have repeatedly chosen to impose direction

---

[101] *D. Earnshaw and Others (Great Britain) v United States* (n 94) 161
[102] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* [1980] ICJ Rep 58
[103] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 210
[104] *Military and Paramilitary Activities in and against Nicaragua* (n 3) (separate Opinion of Judge Ago) 16
[105] *Tsagourias* (n 46) 9
[106] Discussing the Nicaragua case, *Cassese* ((n 4) 653) argued that the 'issuance of directions to the contras […] that is to say, the ordering of those operations by the [US]' would have provided the foundation for the responsibility of the latter State. The fact that directions should be issued in relation to a specific conduct was expressed by ICJ which recognised a State responsibility where an 'organ of the State […] provided the direction pursuant to which the perpetrators of the wrongful act acted.' Cf *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 406
[107] *ILC* (n 1) art 17 cmt 7
[108] ibid
[109] *Crawford* (n 5) 146 fn 28

and control as a single standard of attribution,[110] and similar approach has been taken by various academics.[111]

There is no reason for a deviation in reasoning in the cyber context; State responsibility would arise if the perpetrating entity conducted the specific act on the basis of instruction or direction from that particular State. Instructions or directions in the cyber realm are likely to take the form of provisions of contract of hire or the subsequent instruction of the commanding State party designated in such contract.[112] No public information substantiating the existence of any specific ad-hoc instructions or prolonged directions to Nashi or the Cutting Sword of Justice provided by Russia or Iran substantiates that. Note that encouragement of the unlawful cyber behaviour by Russia[113] in the case of 2007 DDoS, does not constitute instructions.[114]

In addition to the aforementioned situations, the responsibility of a State may arise when the author of the injurious act is subject to the effective or overall control of that State. Considering past prominent judicial decision on the subject matter, the first standard that arose was of the effective variety. In the Nicaragua case, the so called contras were not a *de facto* organ of the accused US since they did possess a certain degree of independence and were not under the effective control of the US.[115] For such actions to be attributed to the State though the test of effective control, the State should have 'directed or enforced the perpetration of the acts contrary to [international] law'.[116] In other words, 'specific instructions concerning the

---

[110] ibid
[111] *See eg* Hannah Tonkin, *State control over PMSC in Armed Conflict* (CUP 2011) 59
[112] Argued, for example by Tonkin, *State control over PMSC in Armed Conflict* (CUP 2011) 114; *and* 'Expert Meeting on Private Military Contractors: Status and State Responsibility for their Actions' (The University Centre for International Humanitarian Law, Geneva 29–30 August 2005) 19
[113] See eg *Nazario* (n 85) 173; Phillips, 'Estonia Charts Legal, Military Future of Cyber Warfare (Including Applicability of NATO's Article V)' (Cable 08TALLINN326_a, 22 September 2008) <https://goo.gl/QiY4gK> accessed 1 April 2016
[114] See eg *Schmitt* (n 24) 38
[115] *Military and Paramilitary Activities in and against Nicaragua* (n 3) para 115
[116] ibid

performance of each action were required in order to attribute the action to the instructing state'.[117]

The second standard evident in the international jurisprudence is the so-called overall control standard of attribution. According to the International Criminal Tribunal for the former Yugoslavia (ICTY), a non-State actor may be regarded a *de facto* State organ and its unlawful conduct can be attributed to that State not only when the State is found to have equipped and financed the perpetrator but also when it coordinated or helped in the general planning of the activity[118] or '[provided] operational support to that group'.[119]

The ICTY argued that the overall control standard is more appropriate in the context of the acts of 'armed forces or militias or paramilitary units'[120] and international humanitarian law as opposed to the general rules on State responsibility. Also an inspiration for the Tallinn Manual, the degree of organisation seems to be the main distinction criterion between the two control standards in the Tadić case. The effective control standard may be used in the deliberation of the attribution of the acts performed by the 'unorganised group of individuals',[121] while the overall control standard is to be used in situations where 'individuals [make] up an organised and hierarchically structured group, such as a military unit or, […] armed bands of irregulars or rebels'.[122] An organised group is different from the individuals 'in that the former normally has a structure, a chain of command and a set of rules as well as the outward symbols of authority'[123] to which the member conforms. Both, 'practice and case law'[124] support the distinction, argued Cassese.

---

[117] *Cassese* (n 4) 657
[118] *Prosecutor v Duško Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995) para 131
[119] Ibid para 137
[120] ibid
[121] ibid para 118
[122] ibid para 120
[123] ibid
[124] *Cassese* (n 4) 657

Several authors have discussed the application of the two standards in the cyber domain. Shackelford attempts to solve the issue of attribution in the cyber realm by adopting the less stringent, less rigid control standard deriving from the ICTY jurisprudence. According to Shackelford, the attribution of the cyber operations, by adopting the overall State control over the perpetrator, would become more achievable because it does not require the unrealistically high standards of proof. Embracing the overall control standard would prevent the governments from 'hid[ing] their information warfare operations under the effective control standard'.[125] An argument in favour of the overall control standard based on *inter alia* the evidentiary considerations has also been made by Cassese.[126] Tsagourias, on the other hand, adopts a pragmatic control standard theory in the context of cyber attacks and questions of self-defence. 'Any form or degree of control by a State over a non-State actor that goes on to attack another State will suffice as for the victim State to use force by way of self-defence against the host State'[127] argues the author. The Tallinn Manual, on the other hand, does not go beyond the description of both standards though it argues that the overall control standard is not applicable to the conduct of individuals and insufficiently organised[128] or unorganised groups.[129]

In the context of unlawful inter-State cyber operations below the use of force, the injured State wishing to employ countermeasures against the State sponsoring a cyber operation should be able to prove effective State control for the purpose of attribution. A few reasons substantiate this argument.

First, the ICTY has not devised the overall control standard in order to answer the question of State responsibility but to establish whether an armed conflict was international or internal.[130] As the ICJ declared in the Genocide case, the ICTY 'was not called upon in the Tadić case,

---

[125] *Shackelford & Andres* (n 10)
[126] *Cassese* (n 4) 665–667
[127] *Tsagourias* (n 46) 12
[128] *Schmitt* (n 48) 37, 38, 73
[129] ibid 38
[130] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 404

nor is it in general called upon, to rule on questions of State responsibility, since its jurisdiction is criminal and extends over persons only'.[131]

Second, accepting a lower standard of control with the intention to make it 'less difficult'[132] to attribute an act to a particular State, proposed by the two aforementioned scholars, may very well be convenient but not necessarily prudent. Legal standards should not be lowered just because evidence is more difficult to obtain. In the Corfu Channel case, the court did not allow for a lower standard of proof only because the United Kingdom faced issues in collecting the evidence held under the exclusive control of Albania.[133] What is more, in the Genocide case, the ICJ argued in favour of the effective control standards as it deemed the overall control standard to be 'unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility'.[134] Indeed, attribution in the context of countermeasures needs to be correct, not easier, or else the self-help measures of the injured State will be unlawful and escalation of the conflict may occur.

It is not hard to imagine a State organ providing specific instructions for conduct of an unlawful cyber operation.[135] It is quite possible, for example, that the Cutting Sword of Justice was a recipient of specific instructions for conduct relating to the unlawful Shamoon cyber operation against Aramco. It is also possible that the instructions came from Iran. Nevertheless, public information does not support that and whether Saudi Arabia can prove that and employ countermeasures remains unknown. Furthermore, in spite of the connections to the Russian authorities elaborated beforehand, there are no indications that the Nashi group was

---

[131] ibid para 403
[132] *Cassese* (n 4) 666
[133] *Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania)* (Merits) [9 April 1949] ICJ Rep 4
[134] *Prosecutor v Duško Tadić* (n 118) para 406
[135] See also *Schmitt* (n 48) 37

completely dependent on the State nor that it received specific instructions to conduct the DDoS operation.

This certainly does not mean that the overall control standard should be dismissed altogether. On the contrary, this standard may be useful in attempting to establish State responsibility for acts conducted by hierarchically organised armed groups. This implies a conduct of forceful nature, something that the present text is not concerned with. After all, the ICTY did argue that the overall control standard is appropriate when attempting an attribution of the acts of 'armed forces or militias or paramilitary units',[136] a language clearly of international humanitarian law origin.[137] In the context of self-defence and cyber attacks, information warfare or perpetrators in the form of terrorist groups (argued by Tsagourias, Shackelford and Cassese respectively)[138] advocating for the overall control standard is therefore an understandable position.

While it remains unknown who orchestrated the cyber operations under consideration, the acts, which are the subject of this text, were not of forceful nature[139] and labelling the perpetrators orchestrating cyber operations below the use of force as organised armed groups would be dangerous. None of the suspected groups behind the cyber operations analysed in the present text constitute an armed group. Nashi, the alleged perpetrating party behind the 2007 DDoS operation, for example, is a self-proclaimed 'socio-patriotic movement' with the mission of spreading 'ideological influence among the younger generation'[140] and not a military unit, armed band of irregulars or rebels. Moreover, the Cutting Sword of Justice is, as already mentioned, an anti-oppression hacker group which cannot be equated with an organised

---

[136] *Prosecutor v Duško Tadić* (n 118) para 137. The view is shared with *Cassese* ((n 4) 654), asserting the 'effective control test, to the extent that it is also applied to organised armed groups, is inconsistent with a basic principle underpinning the whole body of rules and principles on state responsibility.'

[137] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (Geneva, 8 June 1977) art 43

[138] See *Tsagourias* (n 46); *Shackelford & Andres* (n 10); *Cassese* (n 4)

[139] *See* ch 1 on distinction between a *cyber operation* and *cyber attack*.

[140] Danya Spencer & Michael Smeltzer, 'Nashi: Russian Youth Movement' (translation, *School of Russian and Asian Studies*, 6 December 2011) <http://goo.gl/FNRTXK> accessed 1 April 2016

armed group with outward symbols of authority, what would justify utilising the overall control standard. The same can be argued for the similar cyber groups such as CyberBerkut, behind the attack on German governmental systems.[141] What is more, empirical research has shown malicious cyber groups lack the structure of 'traditional, hierarchical organised crime groups'.[142]

All things considered, the overall control standard is not an appropriate legal standard when considering the control of a State for the purpose of the attribution of a cyber operation below the use of force.

3. Evidentiary issues plaguing efforts to prove the breach and the attribution of an unlawful cyber operation

The injured party to the dispute needs to be able to prove both elements of State responsibility – the occurrence of the unlawful act as well as attribution to the State.[143] While evidentiary issues related the former are unlikely to arise, the same cannot be said for the exercise of proving the latter.[144]

While evidence and proof are rarely subjects of deliberation outside of the context of international adjudication, in the attempt to attribute an unlawful cyber conduct, an injured State must not only resort to principles of the international law of State responsibility but also to take into account the law of evidence. To avoid taking wrongful countermeasures, the

---

[141] Trend Micro, 'Hacktivist Group CyberBerkut Behind Attacks on German Official Websites' (*Trend Micro*, 20 January 2015) <http://goo.gl/lDtt3W/> accessed 1 April 2016

[142] Roderic Broadhurst et al, 'Organisations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime' (2014) 8(1) Intl J of Cyber Criminology 4

[143] *Military and Paramilitary Activities in and against Nicaragua* (n 3) para 57: '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 occurrence of the act itself may however have been shrouded in secrecy. In the latter case, the Court has had to endeavour first to establish what actually happened, before entering on the next stage of considering whether the act (if proven) was imputable to the State to which it has been attributed.' See also eg *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 208

[144] Various public sources of evidence, pointing at the fact that cyber operations have indeed injured certain States or State-owned private entities, have been referenced in the paragraphs above.

attribution should be evaluated in the light of the legal framework governing proof, especially the burden and standards of proof, as well as the permitted forms of evidence and methodology of reasoning. For this reason, the following paragraphs focus on burden, methods and standards of proof in support of the attribution of the unlawful cyber operation.

There is however no coherent international treaty law to which one could turn for guidance on matters of proof and evidence. What is more, there is also no well-established, uniform customary evidence law to speak of[145] and codification of the law of State responsibility in a form of the ARSIWA offers very limited guidance on the subject of evidence and proof.[146]

Consequently, the focus of the following paragraphs is on other sources of international law, namely judicial decisions and the writings of notable international legal scholars. These sources, provided by the impartial parties in various of contexts, offer a neutral, value-free framework which is crucial in the context of self-help measures, especially considering that the intention countermeasures is to induce compliance and not to escalate the conflict. With the passage of time, State practice and *opinio juris* will undoubtedly contribute to the gradual development of the international customary law governing proof and evidence in the context of countermeasures.

3.1. Burden of proof

The burden of proof or 'the obligation on a party to show that they have sufficient evidence on an issue to raise it in a case',[147] generally rests on the injured party alleging State responsibility.[148] In other words, the State injured by the cyber operation bears the burden of

---

[145] Mary E O'Connell, 'Evidence of Terror' (2002) 7(1) J of Conflict and Security L 19, 21

[146] This was the intention of the ILC: 'Questions of evidence and proof of such a breach fall entirely outside the scope of the articles' *ILC* (n 1) 97

[147] Anna Riddell & Brendan Plant, *Evidence Before the International Court of Justice* (BIICL 2009) 81

[148] 'In a bilateral dispute over State responsibility, the onus of establishing responsibility lies in principle on the claimant State' *ILC* (n 1) ch 5 cmt 8. See also *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ rep para 162: 'it is the duty of the party which asserts certain facts to establish the existence of such facts'; *Military and Paramilitary Activities in and against Nicaragua* (n 3) para 101: 'it is the litigant seeking to establish a fact who bears the burden of proving it'; Mojtaba Kazazi, *Burden of Proof and Related Issues: A Study on Evidence Before International Tribunals* (Kluwer Law International 1996) 222

proving that the act in question is attributable to another State as well as its unlawful character. A number of international lawyers support this assertion; Roscini argues that the reversal is unlikely to be allowed in the international adjudication process,[149] while Gervais argues that the 'burden of proof should remain with the targeted State'.[150] This is particularly true when an injured State is attempting to justify the countermeasures, acts in contravention of the international rights of the responsible State.[151]

In the latter case, the injured party invoking State responsibility has no obligation to in fact produce or disclose proof substantiating its allegation, although it must be ready to do so in case its assertions of attribution are disputed by the allegedly perpetrating State that is the target of countermeasures. Being able to produce proof (meeting the appropriate legal standards) prevents the injured State from taking countermeasures against a State that is not responsible for the cyber operation after all and from taking a course of action that would constitute a violation of its own international duties.

This rule, however, is not an absolute one.[152] In fact, it has been proposed that shifting the burden of proof 'from the investigator and accuser to the nation in which the attack software was launched'[153] would solve evidentiary issues in the cyber context, since burden of proof 'shifting has been used in dealing with international crime and with terrorism'.[154] While the authors of this proposition do not offer a more in depth explanation of the argument, the reversal of the burden of proof doctrine does indeed occur in the international legal scholarship.

---

[149] *Roscini* (n 24) 247
[150] Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 1(8) J of L & Cyber Warfare: The New Frontier of Warfare 85
[151] *ILC* (n 1) ch 5 para 8
[152] *Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo)* (Merits) [2010] ICJ Rep para 54
[153] Richard A Clarke & Robert K Knake, *Cyber War: The Next Threat to National Security and What to do about it* (Ecco 2012) 249
[154] ibid

Reversal of the burden of proof has been recognised in certain human rights cases. Namely, European law provides that it 'shall be for the respondent to prove that there has been no breach of the principle of equal treatment'.[155] A confirmation of this may be found in a number of cases before the Court of Justice of the European Union[156] and the European Court of Human Rights. For example, in the case of Ribitch v Austria, the Republic of Austria bore the burden of proving that the 'applicant's injuries were caused otherwise than – entirely, mainly, or partly – by the treatment he underwent while in police custody'.[157] The principle has been confirmed by the UN Human Rights Committee, rejecting the argument of Cameroon that the burden of proof for the allegations of torture lies with the victim.[158] The rationale behind the aforementioned cases where the burden of proof reversal was allowed lies in the fact that the individual was unable to substantiate violations conclusively, since the evidence was exclusively controlled by the State.[159] It is not hard to see that the context of the above instances is significantly different from the context of inter-State cyber operations below the use of force. Besides, evidence of cyber operations is not exclusively controlled by the perpetrating State.

Reversal has also been proposed in the context of the precautionary principle[160] and its potential to address 'scientific or technological uncertainty [for] managing cyber-based activities'[161] has been recognised. The principle, not yet part of the international customary

---

[155] Lilla Farkas & Orlagh O'Farrell, *Reversing the Burden of Proof: Practical Dilemmas at the European and National Level* (European Commission 2014) 88

[156] *Danfoss A/S and Sauer–Danfoss ApS v Skatteministeriet* [2011] CJEU Rep 2011 I-09963

[157] *Ribitsch v Austria* App No 18896/91 (ECHR 4 December 1995) 34

[158] *Womah Mukong v Cameroon* [1994] (Communication No 458/1991) UN Doc CCPR/C/51/D/458/1991 paras 9.1 & 9.2

[159] See a discussion on this in Juliane Kokott, *The Burden of Proof in Comparative and International Human Rights Law: Civil and Common Law Approaches with Special Reference to the American and German Legal Systems* (Kluwer Law International 1998) 198

[160] Roberto Andorno, 'The Precautionary Principle: A New Legal Standard for a Technological Age' (2004) 1(1) J of Intl Biotechnology L 11

[161] Thilo Marauhn, 'Customary Rules of International Environmental Law – Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace' *in* Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE 2013) 475

law,[162] encourages pre-emptive actions (of protection) even when the scientific evidence supporting the unacceptable risk or anticipated harm is inconclusive.[163] It challenges the traditional legal doctrine 'by proposing to shift the burden of proof towards those whose actions may seriously threaten the public health or the environment'.[164] While the application of the precautionary principle to cyber incidents is certainly tempting, its origins are particularly associated with situations likely to inflict damage to the 'environment, human, animal or plant health'.[165] The principle found its way also into the Declaration of the UN Conference on Environment and Development[166] and Framework Convention on Climate Change.[167]

Consequences of cyber operations below the use of force by definition do not pose a threat to any of the aforementioned categories. Thus, the application of the principle routed in the international environmental law is hardly appropriate. Even if we disregard its evident environmental origins, the Pulp Mills judgment by the ICJ rejected the argument of Argentina that the precautionary approach implies a reversal of the burden of proof.[168]

Under those circumstances, States whose infrastructures were targeted by the RedOctober[169] and wish to employ countermeasures, are the ones having the responsibility to prove the attribution of the operation to a particular State. Moreover, when attempting to attribute the Shamoon and 2007 DDoS cyber operations, it is Saudi Arabia and Estonia, respectively, which need to be able to provide proof in support of their claims.

In judicial settings, once the injured party has discarded its burden of proof it is up to the respondent to produce evidence of rebuttal. In the courtroom 'the burden of producing

---

[162] Caroline E Foster, *Science and the Precautionary Principle in International Courts and Tribunals* (CUP 2013) 21

[163] European Commission, Communication from the Commission on the precautionary principle (COM/2000/0001 final, 2 February 2000)

[164] *Andorno* (n 160) 11 & 19

[165] *European Commission* (n 163) para 3

[166] Declaration of the UN Conference on Environment and Development (Rio de Janeiro, 14 June 1992) UN Doc A/CONF.48/14, 11 ILM 1416, Principle 15

[167] Framework Convention on Climate Change (Rio de Janeiro, 9 May 1992, 31 ILM 851) art 3(3)

[168] *Pulp Mills on the River Uruguay* (n 148) 164

[169] For a full list of targets see *Global Research & Analysis Team* (n 37)

evidence may shift back and forth throughout'[170] the progress of the case. This is certainly not always the case in the context of countermeasures and particularly so when an injured State decides to employ urgent countermeasures – unilateral self-help measures which may be initiated without any notification to the targeted State.[171]

3.2. Standard(s) of proof

The standard of proof, a decisional threshold,[172] is the quantum of evidence necessary to substantiate the factual claims made by the party.[173] Even in the case of circumstantial proof, the inference must lead 'logically to a single conclusion'[174] or leave 'no room for reasonable doubt'.[175] Therefore, a differentiation between the effects of direct as well as indirect evidence on the standard of proof should not be attempted.[176] Nevertheless, insisting on the standard beyond reasonable doubt in the cyber realm would be premature, particularly without further investigation.

Legal scholarship, including the investigations of cyber operations,[177] has been recently discussing the standard of proof, seeking a rigid, unequivocal framework to be applied in the context of the new environment. However, this certainly is not a simple task and, what is more, it is likely to fail.

As a matter of fact, flexibility governs the international legal approach to the standard of proof.[178] The consistent or uniform international standard of proof has yet to be established by

---

[170] Roger Dworkin, 'Easy Cases, Bad Law, and Burdens of Proof' (1972) 25 Vanderbilt L Rev 1151, 1159
[171] *ILC* (n 1) art 52 cmt 6
[172] Ho Hock Lai, *A Philosophy of Evidence Law* (OUP 2008) 174
[173] James A Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice' (2009) 58(1) ICLQ 163, 165
[174] *Corfu Channel case* (n 133) para 18
[175] ibid
[176] Kazazi, rightly so, argued that 'the effect of inferences […] is not different from that of any other types of evidence'. *Kazazi* (n 148) 266
[177] For example, *Roscini* (n 24)
[178] Daniel Joyce, 'Fact-Finding and Evidence at the International Court of Justice: Systemic Crisis, Change or More of the Same' (2007) 18 Finnish Ybk of Intl L 283, 286. The lack of transparency as of what standard is to be expected by the claimant from the ICJ has been criticised by the entities of the court itself. See *Oil Platforms* (*Islamic Republic of Iran v United States of America)* (Separate Opinion of Judge Higgins) [2003] ICJ rep

jurisprudence.[179] Whether this is desirable is questionable. In the words of Judge Higgins, proof is 'to an extent in the eye of the beholder; what was a fact for one person was not a fact for another'.[180] Furthermore, evaluation of evidence is an intellectual process dependent on the specific circumstances[181] of an individual case and an 'attempt to itemize broad principles governing such subjective mental activity must perforce be somewhat hazardous.'[182]

In a quest to resort to extrajudicial measures of self-help, the State injured by an unlawful cyber operation finds itself in a curious position. The State in question is not only the victim but also the judge as well as the aspiring executioner. Being a victim, it is naturally inclined to be a liberal and subjective judge and hasty executioner or to be overly concerned with the aggregate fact-finding cost versus the risk of error.[183] As a victim and the executioner, it is inclined to accept the lower standard of proof, disregard the authenticity and reliability issues or find proof in evidence of questionable quality, with questionable chain of custody or corroborated with evidence of questionable format. In a desire to employ (urgent) countermeasures during an unlawful cyber act – which can cease or change the attributes in an instant – the danger is especially prominent.

High standards should be self-imposed at least for two reasons. First, the State interested in employing countermeasures must be certain of its claims or face countermeasures itself for the ill-founded and consequently unlawful countermeasures it subjected onto another State.[184]

---

[179] 'In general, international law does not have a clear benchmark against which the persuasiveness or reliability of evidence may be gauged for the purposes of attributing responsibility or assessing legal claims': *Green* (n 169) 165

[180] ILC, 'Summary record of the 2899th meeting' (10 August 2006) UN Doc A/CN.4/SR.2899, 17

[181] '[T]he importance of freedom of evaluation, through which the probative value of each piece of material evidence shall be determined given the overall circumstances of the case.' *Kazazi* (n 148) 212

[182] Bib Cheng, *General Principles of Law as Applied by International Courts and Tribunals* (CUP 1994) 303. This, according to *Kazazi* ((n 148) 212), is why 'experience, knowledge, and a high degree of impartiality' of international judges and arbitrators is essential.

[183] For more on the cost-efficiency doctrine of the evidence law *see* Alex Stein, *Foundations of Evidence Law* (OUP 2005) 141–143

[184] Eg *Roscini* (n 24) 229 argues '[t]he standard of proof exists not to disadvantage the claimant, but to protect the respondent against false attribution'.

What is more, abiding by the standards set by the international case law would protect the State in a potential subsequent adjudication.[185]

Three standards have been recognised in most common law jurisdictions; beyond doubt, clear and convincing proof and the balance of probabilities. While the first two standards are usually found in criminal cases, the latter is common to civil litigations.[186]

Presuming the intention to avoid unlawful countermeasures, the balance of probabilities standard receives no attention below. Should we choose to avoid 'specious claims and false or erroneous attribution',[187] State responsibility for an unlawful cyber operation should be proved beyond the threshold of balance of probabilities which requires the injured State to produce evidence proving that a particular State is 'more likely than not or more probable than not'[188] responsible for the cyber operation.

The other extreme end of the spectrum is occupied by the standard which requires a fully *conclusive*[189] proof *beyond reasonable doubt.*[190] The standard requires the probability of the alleged attribution and unlawful character of cyber operation to approach certainty or the 'elimination of all evidenced and case-specific […] scenarios'[191] in which the allegedly perpetrating State is not responsible for the alleged cyber violation of international law. The origins of the standard may be found in the criminal proceedings of common as well as civil law. For example, the German legal system 'always requires persuasion beyond reasonable

---

[185] Inter-State disputes over the countermeasures which were subject to international adjudication include *Air Service Agreement of 27 March 1946 between the United States of America and France* [1978] XVIII UNRIAA 416; *Naulilaa Arbitration (Portugal v Germany)* [1928] II UNRIAA (Sales No. 1949.V.1) 1012; *Corfu Channel case (n 133); Military and Paramilitary Activities in and against Nicaragua* (n 3); *Gabčíkovo-Nagymaros Project (Hunngary/Slovakia)* [1997] ICJ Rep

[186] *Lai* (n 172) 175

[187] *Roscini* (n 24) 252

[188] *R v Swaysland* [1987] BTLC 299, 308. See similar assertions made by Denning in *Miller v Minister of Pensions* [1947] 2 AII ER 374

[189] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 276, 277 334, 319; *Oil Platforms* (n 178) para 71

[190] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 422

[191] *Stein* (n 183) 178

doubt'[192] and similar assertion may be made for English[193] and international[194] criminal law. The rationale behind this high standard of proof lies in the fact that 'although it may mean that some guilty people go unpunished, it is more important that the innocent are not wrongly convicted'.[195] Clearly, establishing State responsibility is not about criminal liability of an individual, let alone about sending anyone behind bars. It is perhaps why States are not particularly inclined to consider this standard to be relevant in cyber space; only Italy has come on the record arguing in favour of this most exacting standard of proof, conditioning attribution of an inter-State cyber operation by unequivocal[196] and 'irrefutable digital evidence'.[197]

Also, for the purpose of the present research, and potentially even for cyber context in general,[198] this standard is overly demanding. Where the allegation is responsibility for an unlawful cyber operation short of producing physical damage or injury to human being, this standard is in contradiction with the principle that the proof has to be 'appropriate to the seriousness of the allegation'.[199] Accordingly, the international jurisprudence indicates that fully conclusive proof may only be required when testing charges 'of exceptional gravity against a State',[200] which cyber operations below the use of force certainly are not.

Because the balance of probabilities standard exposes the State wishing to take countermeasures to a risk of aiming at the wrong State and because the beyond reasonable doubt standard is inappropriate in the context of this thesis, the argument for a third standard of proof is put forward.

---

[192] *Kokott* (n 159) 196
[193] *Lai* (n 172) 175
[194] Rüdiger Wolfrum, 'International Courts and Tribunals, Evidence' *in* Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (OUP 2012) 552, 569. See also *Prisoners of War–Eritrea's Claim 17 (Ethiopia v Eritrea)* [2003] (Partial Award), XXVI UNRIAA paras 45–47, requiring a proof not higher than a clear and convincing proof, because the Commission was 'not a criminal tribunal'.
[195] Lord Woolf CJ in *R v B* [2003] 2 Cr. App. R. 13 para 27
[196] Comitato Parlamentare Per La Sicurezza Della Repubblica, 'Relazione Sulle Possibili Implicazioni E Minacce Per La Sicurezza Nazionale Derivanti Dall'utilizzo Dello Spazio Cibernetico' (2010) 26 cited in *Roscini* (n 24)
[197] ibid
[198] *Roscini* (n 24) 253
[199] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 210
[200] *Corfu Channel case* (n 133) para 18. See also *Oil Platforms* (n 178) (separate opinion of Judge Higgins) para 33: 'the graver the charge the more confidence must there be in the evidence relied on'.

The third international legal standard of proof required to substantiate the allegations of attribution is the one requiring *sufficiently clear and convincing* proof. It has been recognised by the Military and Paramilitary Activities in and Against Nicaragua[201] as well as the Armed Activities on the Territory of the Congo[202] ICJ judgments. Furthermore, other international judicial conclusions confirm the standard,[203] which is also maintained by various legal scholars discussing the standard of proof in the context of cyber operations.[204] State practice is supportive of this. The US Air Force Doctrine for Cyberspace Operations asserts that attribution should be proved with 'sufficient confidence and verifiability', [205] while American *opinio juris* points at the standard of proof requiring a 'definitive'[206] proof when attempting to establish attribution of a cyber operation. Similarly, Dutch official records require 'sufficiently certain'[207] attribution while the UK House of Lords indicated that successful attribution of cyber operations would require a 'conclusive analysis'.[208] For the aforementioned reasons, injured States wishing to take countermeasures against the State responsible for an unlawful cyber operation below the use of force should be able to provide sufficiently clear and convincing proof substantiating the attribution claims.

---

[201] *Military and Paramilitary Activities in and against Nicaragua* (n 3) paras 24, 29, 62, 109

[202] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep paras 72, 91, 136

[203] For example, *Case of Velásquez-Rodríguez v Honduras* (Reparations and Costs) [1989] (Judgment of 21 July 1989) Inter-American Court of Human Rights para 79; *The MOX Plant Case* (*Ireland v United Kingdom)* (Separate Opinion of Judge Mensah) [2001] ITLOS 3

[204] '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.' Michael Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56(3) Villanova L Rev 595; *Roscini* (n 24) 252: '[C]lear and convincing evidence seems the appropriate standard not only for claims of self-defense against traditional armed attacks, but also for those against cyber operations'.

[205] US Air Force, 'Cyberspace Operations: Air Force Doctrine Document 3–12' (15 July 2010) 10

[206] Sean Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*Just Security,* 14 October 2016) <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack> accessed 13 August 2019

[207] Government of Netherlands, 'Government response to the AIV/CAVV report on cyber warfare' (26 April 2012) 5 <http://cms.webbeat.net/ContentSuite/upload/cav/doc/advies_22_reg_reactie_EN.pdf> accessed 1 April 2016

[208] European Union Committee, 'Protecting Europe Against Large-Scale Cyberattacks' HL (Paper 68, 2009–10) 42

3.3. Classification and forms of evidence

Evidence, an 'information, medium or means by which the facts tend to be proved or disproved',[209] comes in a direct or indirect form. Due to the clandestine nature of cyber operations, the latter one deserves special attention. Indirect or circumstantial evidence, 'admitted in all systems of law, and […] recognised by international decisions',[210] constitutes 'facts which, while not supplying immediate proof of the charge, yet make the charge probable […] with the assistance of reasoning'.[211]

In the attempt to attribute the unlawful cyber operation to a particular State, proof stemming from a combination of circumstantial evidence and reasoning by inferences should not be neglected.[212] Indeed, it is expected that the State injured by a cyber operation will consider filling the inevitable gaps of direct evidences by drawing inferences. However, international judiciary has 'demonstrated an increasing resistance to the drawing of inferences'[213] and some noncumulative and considerable limitations should be observed; inferences are to be appreciated only in the absence of the rebuttal by the alleged perpetrator or in the exercise of proving the knowledge of the existence of the wrongful conduct and not attribution of the wrongful conduct itself.

Reasoning by inferences has been utilised previously by the Iran–US Claims Tribunal and other international tribunals. However, the practice was always out of the framework of countermeasures and the tribunals allowed for inferences only 'when the respondent has

---

[209] 31A C.J.S. Evidence para 8 (1964). For more on the difference between the proof and evidence see Rüdiger Wolfrum, 'International Courts and Tribunals, Evidence*' in* Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (OUP 2012) 552, 552

[210] *Corfu Channel case* (n 133) para 18

[211] ibid (dissenting opinion of Judge Pasha)

[212] 'The proof may be drawn from inferences of fact.' ibid para 18. See also *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain)* (separate opinion of Judge Bustamante) [1964] ICJ Rep para 80: '[It may] be possible to arrive at a conclusion on the basis merely of inferences or deductions forming part of a logical process'.

[213] Ruth Teitelbaum, 'Recent Fact-Finding Developments at the International Court of Justice' (2007) 6(1) L & Practice of Intl Courts and Tribunals 119, 157. Similar claims may be found in *Kokott* (n 159) 189

offered no evidence in rebuttal',[214] be it due to silence or failure to submit satisfactory counterevidence.[215] This has 'been largely accepted as fair'.[216] Nevertheless, States regularly reject responsibility for cyber operations; Russia has repeatedly rejected their involvement in 2007 DDoS against Estonia, for example.[217] What is more, in a quest for urgent countermeasures, the State accused of the wrongdoing has no opportunity to offer a rebuttal evidence. In these two cases, reasoning by inferences would be unfair.

Furthermore, inferences may be drawn from indirect evidence pointing at the territory of origin. Provided that one choses to trust in the technical evidence pointing at the location of the original perpetrator's machine, exclusive control over the territory or information communication infrastructure may be indicative[218] of the State's knowledge of the unlawful act but it does not establish a responsibility of that State for the unlawful (cyber) conduct.[219] Accordingly, a combination of an indirect evidence and inferences has been previously utilised by the ICJ to prove Albanian knowledge of unlawful act of mine-laying.[220] The principle has also been recognised by the authors of the Tallinn Manual, arguing that the 'fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure

---

[214] *William A. Parker (U.S.A.) v United Mexican States* [1926] IV UNRIAA 39. See similar claims made also in *Flexi-Van Leasing, Inc. v Islamic Republic of Iran* [1982] Iran-US CTR 457; *Combuslion Engineering, Inc., et al and The Islamic Republic of Iran, et al* [1991] (Partial Award No 506-308-2) 26 Iran-US CTR para 70.

[215] See, generally, Howard M Holtzmann, 'Fact-finding before the Iran-United States Claims Tribunal*' in* Richard Lillich (ed), *Fact-finding before international tribunals* (Transnational Publishers 1992) 126–128

[216] Jamison Selby, 'Fact-finding before the Iran-United States Claims Tribunal: The View from the Trenches*' in* Richard Lillich (ed), *Fact-finding before international tribunals* (Transnational Publishers 1992) 143

[217] Ian Phillips & Vladimir Isachenkov, 'Putin: Russia doesn't hack but "patriotic" individuals might' (*Associated Press*, 1 June 2017) <https://apnews.com/281464d38ee54c6ca5bf573978e8ee91/Putin:-Russian-state-has-never-been-involved-in-hacking?utm_campaign=SocialFlow&utm_source=Twitter&utm_medium=AP> accessed 13 August 2019

[218] '[I]t cannot be concluded from the mere fact of the control exercised by a State over its territory […] that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein.' *Corfu Channel case* (n 133) para 18

[219] This narrative has been affirmed by the ICJ, refusing to attribute the attack on Sea Isle City to Iran even though the missile was fired from the territory under the control of the aforementioned State. *Oil Platforms* (n 178) para 61. Or succinctly put by Crawford: 'Under international law, the fact that something occurs on the territory of a State, or in some other area under its jurisdiction, is not a sufficient basis for attributing that event to the State, or for making it responsible for any injury caused.' *ILC* (n 3) 33

[220] '[I]t has been established by means of indirect evidence that Albania has knowledge of minelaying in her territorial waters': *Corfu Channel case* (n 133) para 22

is not sufficient evidence for attributing the operation to that State'[221] as well as other scholars.[222] For instance, circumstantial evidence including a technical report[223] asserting that certain cyber operations originated from a Chinese network, evidence of a nationwide monitoring on the ISP level,[224] the two million State-employed individual Internet monitoring agents[225] and elaborate network monitoring activities of the PLA specialised departments,[226] leads to a logical conclusion that the People's Republic of China knew of the cyber operations in question. Similarly, considering the mandate of the Federal Security Service of the Russian Federation Information Security Center is to monitor Russian Internet networks and identify threats 'using hardware and software installed at Russian [ISPs], Internet access points, and Internet exchanges',[227] public statements of acknowledgement of the DDoS attack by the Russian official Goloskokov and a list of IP addresses pointing at the fact that majority of attacks came from the Russian systems, leads to a rational deduction that Russia was aware of the 2007 DDoS operation against Estonian governmental systems. In both cases, knowledge of the undergoing internationally wrongful cyber activity however does not establish a State responsibility for the act itself.

Evidence may come in all forms and sizes;[228] documents, witness and expert testimony, official statements and official enquiry outcomes have been historically considered by

---

[221] *Schmitt* (n 48) rule 7

[222] In the case of 'repeated instances of hostile computer activity emanating from a State's territory directed against another State, it seems reasonable to presume that the host State had knowledge of such attacks.' Richard Garnett & Paul Clarke, 'Cyberterrorism: A New Challenge for International Law' *in* Andrea Bianchi (ed) *Enforcing International Law Norms Against Terrorism* (Hart Publishing 2004) 465, 479

[223] *Mandiant* (n 21)

[224] Human Rights Watch, '"Race to the Bottom" Corporate Complicity in Chinese Internet Censorship' (vol 18, no 8 (c), August 2006) <https://www.hrw.org/reports/2006/china0806/china0806web.pdf> accessed 13 August 2019

[225] 'China employs two million microblog monitors state media say' *BBC* (4 October 2013) <http://goo.gl/zMqlAr> accessed 1 April 2016

[226] For an overview of Chinese cyber monitoring activities see, for example, Mark Stokes, Jenny Lin & LC Russell Hsiao, 'The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure' (The Project 2049 Institute, 11 November 2011) <https://goo.gl/LuWhZN> accessed 1 April 2016; Peter Mattis, 'The Analytic Challenge of Understanding Chinese Intelligence Services' (2012) 56(3) Studies in Intelligence 47

[227] 'Russian Federal Security Service (FSB) Internet Operations Against Ukraine' (TAIA Global Report, 2015) 4–5 <https://goo.gl/PMDY58> accessed 1 April 2016

[228] Sandifer argues that '[t]he International Court of Justice has construed the absence of restrictive rules in its Statute to mean that a party may generally produce any evidence as a matter of right'. Durward V Sandifer,

international judicial entities as evidence. Similar forms of evidence can be used by the injured party to assert attribution of an inter-State cyber operation.

In the context of the present research, it is worth noting that documentary evidence, defined as 'anything in which information of any kind has been recorded'[229] includes digital formats.[230] The ICTY has confirmed the assertion in the Orić Trial judgment.[231] Interestingly enough, scholars have opined that documentary evidence includes 'published and unpublished diplomatic correspondence'[232] which would include the diplomatic records published by the notorious WikiLeaks.

Given the nature of electronic documentation, I feel compelled to spend a few lines discussing the authenticity and reliability of this type of evidence. For the (electronic) document to be considered sufficiently authentic an indication of reliability must be provided. In order to achieve that, 'consideration may be given to factors including the extent to which the document's content is corroborated by other evidence, the location where it was obtained, whether it is an original or copy, […] or certified [in] any way'.[233] When considering a reliability test, however, one 'is to establish whether a piece of evidence is what it purports to be'.[234] Considering that electronic information may be easily manipulated, that technical means for the attribution of a cyber operation 'are inherently limited',[235] that they rely on unreliable

---

Evidence before international tribunals (University Press of Virginia 1975) 184. See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 72) para 211

[229] *Prosecutor v Karemera et al* (Decision on Prosecutor's Motion for Admission of Certain Exhibits into Evidence) [2008] ICTR-98-44-T (25 January 2008) para 5

[230] *See eg* Jeffrey Waincymer, *Procedure and Evidence in International Arbitration* (Kluwer Law International 2012) 847–853

[231] *Prosecutor v Naser Orić* (Trial judgment) [2006] ICTY IT-03-68-T (30 June 2006) para 31

[232] Shabtai Rosenne, *The Law and Practice of the International Court 1920–2005* (4th edn, Brill/Nijhoff 2006) 1246

[233] Karim Khan, Rodney Dixon & Adrian Fulford, 'Archbold International Criminal Courts' (Sweet & Maxwell 2014) 726. The claims seem to be supported by the case law. See *Prosecutor v Karemera, et al* (n 229) paras 169–173, 205; *Prosecutor v Bagosora* (Trial Judgment and Appeals Judgment) [1998] ICTR-98-41-T paras 2029–2031

[234] Aida Ashouri, Caleb Bowers & Cherrie Warden, 'An Overview of the Use of Digital Evidence in International Criminal Courts' (Salzburg Workshop on Cyberinvestigations, October 2013) 4

[235] David A Wheeler & Gregory N Larsen, 'Techniques for Cyber Attack Attribution' (IDA Paper P-3792, US Government Institute for Defense Analyses, 2003) 66

traceback via IP address or on limited remote computer forensics, the requirement of corroboration seems to be especially prominent in the context of this thesis. When considering the employment of self-help measures, the presumption of authenticity and reliability[236] is certainly a dangerous principle to live by.

Various news outlets are often quick to point fingers but the weight of news reports has attracted mixed feelings by the international judiciary. In the Armed Activities on the Territory of the Congo judgment the ICJ considered various news reports, 'unreferenced and unsourced'[237] extracts from a specific book, 'certain internal military intelligence documents, [lacking] explanations as to how the information was obtained',[238] oral pleading claims without citing a source,[239] and unsigned reports internal to the claimant[240] to be not 'weighty and convincing'[241] or unsatisfactory.[242] Furthermore, in the Nicaragua case, the ICJ judged that the evidence consisting of 'no more than newspaper reports'[243] does not successfully establish attribution. On the other hand, the US–Iran Claims Tribunal accepted news stories as proof attributing the acts of the Iranian Revolutionary guards to the newly formed government[244] and considered an interview published in the press in assigning the governmental control over the Foundation of the Oppressed.[245] Regardless, if an injured State desires to consider news reports as appropriate evidence in the struggle to attribute a cyber operation to a particular State, it should be conscious of the fact that public sources 'are by definition secondary

---

[236] Proposed by *Waincymer* (n 230) 828
[237] *Case Concerning Armed Activities on the Territory of the Congo* (n 202) para 137
[238] ibid
[239] *Case Concerning Armed Activities on the Territory of the Congo* (n 202) para 140. Similarly, US argued during the Island of Palmas Arbitration that '[the] statements without evidence to support them could not be taken into consideration by the international tribunal'. *Island of Palmas Arbitration (Netherlands v US)* [1928] II UNRIAA 829
[240] *Case Concerning Armed Activities on the Territory of the Congo* (n 202) para 139
[241] ibid para 136
[242] ibid para 146
[243] *Military and Paramilitary Activities in and against Nicaragua* (n 3) para 117
[244] *Kenneth P. Yeager v The Islamic Republic of Iran* (n 92) paras 39–41
[245] *Hyatt International Corporation v The Government of the Islamic Republic of Iran* (n 88) 90–91

evidence; […] and an indication of what was the original source, or sources, or evidence on which the public sources relied',[246] would be required.

Electronic evidence and newspaper sources indeed attributed Shamoon, although their value to the injured State is insignificant. For instance, Shamoon was explicitly attributed to Iran by the New York Times on at least one occasion,[247] and the assertion was supported by some commentators arguing that 'Iran is at the center of every significant aspect of this attack'.[248] Others, on the other hand, maintained that the operation was conducted by Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, or the United Arab Emirates.[249] Given these claims, it is not hard to recognise the speculative character of the listed evidence; none offer a source of information to corroborate the assertions and as such cannot be labelled as a satisfactory evidence for establishing attribution in line with the law of State responsibility. Electronic evidence provides even weaker proof of attribution. Not one but two perpetrating groups claimed responsibility for the Shamoon operation online – Cutting Sword of Justice[250] and Arab Youth Group.[251] The information was published on the Pastebin website, frequently used by various cyber groups to anonymously 'store pieces of sources code or configuration information'[252] and communicate with the general public. In a legal context, such evidence enjoys even less trust than newspaper articles.

Last but not least, there seems to be an appreciation for evidence produced by private entities. The Flexi-Van and General Motors judgment was based on reports compiled by an independent certified public accountants firm and an annual report of the New York Stock

---

[246] *Oil Platforms* (n 178) para 60
[247] Nicole Perlroth & David Sanger, 'New Computer Attacks Traced to Iran, Officials Say' *New York Times* (24 May 2013) <http://goo.gl/NF01cW> accessed 1 April 2019
[248] Jeffrey Carr, 'Who's Responsible for the Saudi Aramco Network Attack?' (*Digital Dao*, 27 August 2012) <http://goo.gl/gfsvL3> accessed 1 April 2019
[249] John Bumgarner, 'Decapitating Saudi Aramco with the Sword of Justice' (*DefenceIQ*, 22 January 2013) <http://goo.gl/2axlJ7> accessed 1 April 2019
[250] *'Untitled'* (n 79); *'Separate cyber team to attack aramco, 12 days network down'* (n 79)
[251] 'Arab Youth Group' (*Pastebin*, 15 August 2012) <http://pastebin.com/PUHqDQnd> accessed 1 April 2016
[252] 'Frequently Asked Questions' (*Pastebin*) <http://pastebin.com/faq> accessed 1 April 2016

Exchange, a private entity.[253] Under these circumstances, an injured State may very well use the reports of private entries such as Mandiant or Kasperski Lab to assist in building a case in favour of the employment of countermeasures. States indeed seem to be interested in private attribution capabilities. The US Defence Department, for example, announced they 'will continue to collaborate closely with the private sector and other agencies of the US government to strengthen attribution'.[254] The private sector's role has been reiterated by US officials stating that '[g]overnmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions'.[255]

This development is certainly in line with the modernisation of international relations as well as international law where States remain the key actors but surely not the only actors.[256] The reports are however inevitably subjective in their analysis and hardly contribute to the proof of convincing value. Private security company FireEye, for example, attributed various cyber operations to the so called ATP28 cyber group based on attributes such as 'targeting, malware [properties], language, and working hours [of the perpetrating group]'.[257] Similarly, Mandiant concluded PLA was behind a plethora of cyber operations based on circumstantial technical evidence and the similarity in 'mission, capabilities, and resources'[258] of the perpetrating group and the Chinese army. Such conclusions, if incorrect, have no impact on private companies besides reputational and consequential financial costs yet may profoundly worsen the relationship between the two States if presented as a proof of attribution and used as a foundation for countermeasures.

---

[253] *Holtzmann* (n 215) 112
[254] *US Department of Defence* (n 13) 12
[255] ibid 2
[256] See for example, Duncan B Hollis, 'Private Actors in Public International Law: Amicus Curiae and the Case for the Retention of State Sovereignty' (2002) 25 Boston College Intl & Comp L Rev 235, 235–238; Jack Goldsmith, 'Review: Sovereignty, International Relations Theory, and International Law' (2000) 52 Stanford L Rev 959, 959
[257] FireEye, 'APT28: A Window into Russia's Cyber Espionage Operations?' (2014) 28 <https://goo.gl/BeXhoK> accessed 1 April 2016
[258] *Mandiant* (n 21) 2

4. Conclusion

It will be up to the injured State to decide whether the evidence at its disposal amounts to the standard of convincing proof and allows for the attribution and employment of countermeasures. But, as an observant reader may have noticed, sufficiently clear and convincing proof for all three cyber operations is non-existent – as established above, technical evidence is unreliable or misleading while attribution provided by the socio-political threat agent modelling remains subjective and, at best, useful only in determining the State *in fact* responsible for the cyber operation in question.

This has a profound effect on legal attribution. Due to the clandestine nature of cyber operations as well as of the perpetrating groups, direct or indirect legal attribution appears to be impossible. No convincing evidence establishing the fact that any of the discussed perpetrating cyber groups are indeed *de facto* or *de jure* State organs exists.

News reports, webpage entries, private entity reports and various circumstantial evidence certainly do not amount to convincing proof. These more often than not rely on anonymous or unverified sources, can easily be created or altered by anyone and heavily rely on socio-political analysis as well as circumstantial evidence. In fact, all of the evidence in support of the attribution of unlawful inter-State cyber operations available to the public nowadays is of circumstantial nature. Establishing proof would therefore require reasoning by inference, which is only appreciated in establishing knowledge of an unlawful act and in the absence of a rebuttal.

Without attribution there is no State responsibility. And without State responsibility there are no countermeasures. In the absence of countermeasures, the profits of the perpetrating State remain disproportionally high compared to the costs and an alarming frequency of unlawful inter-State cyber operations is a rational consequence.

For this very reason, the following chapter investigates the potential of the attribution of toleration instead of the attribution of orchestration. It moves from a State responsibility for

unlawful cyber operations to the responsibility for the omission of diligent behaviour States owe to the international community. In contrast to the attribution of an unlawful of cyber operation, a violation of the due diligence obligations of prevention and termination will likely be a more attainable task for the injured State, allowing it to take countermeasures and thus restore security by inducing compliance with international law.

Chapter 5

State responsibility for violation of the due diligence obligations in cyberspace

1. Introduction

To change the rational calculation of the unlawful cyber operations and thereby compel the wrongdoing State into compliance with its international legal obligations and restore security, injured States should invoke State responsibility and employ countermeasures against the internationally responsible State for its malicious cyber conduct. Due to the state of technology and the legal requirement of attribution, employment of countermeasures is most often impossible. This has been established in the preceding chapter, which sought to establish State responsibility on the basis of agency, consequential to the unlawful operation conducted by either the State (agents) or non-State actors controlled or directed by the latter.

Based on the premise that the State *in fact* responsible for the unlawful cyber operation has also failed to diligently prevent or terminate it, the objective of this chapter is to establish that State responsibility can be invoked, and countermeasures undertaken, in response to violations of the obligations of due diligence contained within the customary international law.

The first part introduces the well-established international legal principle of due diligence, which includes the obligations of prevention and termination. It presents a plethora of State sources indicating that due diligence and the corresponding obligations are becoming a part of customary international law in cyberspace. Since due diligence obligations are obligations of conduct, this part also explains the flexible nature of the standard of due diligence, revealing the factors that affect this standard and argues in favour of an international minimum standard.

The second part applies due diligence and the corresponding obligations to inter-State cyber operations. It presents a theory of a diligent State and exposes the international minimum

standards of compliance. In other words, it explains what States *can* do and what they *should* do to abide by their due diligence obligations.

The third part places due diligence in the context of the law of State responsibility. It argues that the invocation of State responsibility and the employment of countermeasures against the State for the known cyber operation which it occasioned by its non-diligent performance is, in comparison to the failed invocation of State responsibility on the grounds of agency presented in the previous chapter, significantly more feasible.

This is due to the fact that an injured State, wishing to establish State responsibility for the non-diligent performance, is not required to establish attribution; instead, it must be able to prove actual or constructive knowledge on the part of the allegedly non-diligent State and the fact that the resulting cyber operation emanated from the territory of that State. While this is by no means an easy task, it is certainly more likely to be established in the current legal and technological landscape. The injured State can then proceed to taking countermeasures against the non-diligent State and to restoring power, peace and security.

2. The principle of due diligence

In accordance with the principle of due diligence, States are not only to refrain from violating the rights of other States but also to do their utmost to thwart the subjects under their jurisdiction from doing so. Put in the context of this thesis, States should not only abstain from unlawful selfish utility maximisation but also attempt to prevent and terminate the internationally wrongful minimisation of other States' power and security. The investigation of the principle is rationalised by the fact that every State which utilises cyber means to break the international rule to abstain from, for example, intervening in matters within the domestic jurisdiction of another State, is equally responsible *in fact* for violating the obligation to prevent or terminate the acts denying the sovereign rights of the other State.

Due diligence is a well-established international legal principle and early scholarly pronouncement of due diligence can be dated back to the 18th century, initially argued for as

a means of protection of aliens abroad.[1] The doctrinal concern with the diligent protection of aliens persisted in the following decades, even centuries, but with a decline of State power and the rise of global civil society,[2] due diligence has seen in kind adaptations and reached a status of, as Lauterpacht illustrated while discussing the State responsibility for acts of private entities, the cornerstone of the system of mutual international assurance.[3]

Under the conditions of anarchical constellation of the international relations where no central enforcement entity exists, principle of due diligence imposes a proactive, decentralised and reciprocal protection of legal rights *of* States *by* States, thus reinforcing the rule of law and promoting peace and security. In the contemporary world order, which is organised around the idea of nations being united in the virtues of peaceful cohabitation, scholarship and the international judiciary have recognised the potential of the due diligence principle to ensure the accountability of States, even when the perpetrators have no apparent connection to the governments and the traditional models of State responsibility struggle to accommodate the changing reality of international relations.[4] Due diligence, therefore, goes beyond restricting the maximisation of power by way of unlawful cyber operations conducted by the States; it imposes a responsibility to not only refrain from illegitimate power deprivation by way of cyber operations but also to make sure no one under its jurisdiction does so. As such, due diligence prevents the States to hide their illegitimate power maximisation activities behind the non-State actors, which has been an increasingly more prominent international practice in cyber era.[5]

---

[1] *See eg* Emmerich de Vattel, *The Law of Nations* (Joseph Chitty trans., Gaunt 2001) bk II ch VI, 164, para 78; Christian Wolff, *Jus Gentium Methodo Scientifica Pertractatum* [Argument on Scientific Methodology Regarding the Principles of Law Applicable to All People] (Joseph H Drake trans., William S. Hein & Co. 1995) 317

[2] Jessica T Mathews, 'Power Shift' (1997) 76(1) Foreign Affairs 50–66

[3] Hersch Lauterpacht, 'Revolutionary Activities by Private Persons Against Foreign' (1928) 22 AJIL 105

[4] *See* Robert P Barnidge Jr, 'The Due Diligence Principle Under International Law' (2006) 8(1) Intl Community L Rev 81; Vincent-Joël Proulx, *Transnational Terrorism and State Accountability: A New Theory of Prevention* (Hart Publishing 2012); Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011) 54–80; Nigel D White, 'Due diligence obligations of conduct: developing a responsibility regime for PMSCs' (2012) 31 (3) Criminal Justice Ethics 233; Carsten Hoppe, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 EJIL 989

[5] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018)

The principle of due diligence has been conceptualised in several international judgments. One notable judicial decision based on the due diligence principle was the Island of Palmas case of 1928. Judging on a territorial dispute between the Netherlands and US, the arbitration held that there is no such thing as absolute territorial sovereignty; the latter is indeed limited by the sovereign rights of other nations. The arbitrator Max Huber held that the '[t]erritorial sovereignty … has as corollary a duty: the obligation to protect within the territory the rights of other States'.[6] What is more, in the oft cited Corfu Channel case, the ICJ reached similar conclusions in support of the principle of due diligence. Tasked to judge the dispute between Albania and the United Kingdom and to provide an answer on whether the former incurred State responsibility for the act performed not by its agents but on its territory, the Court argued that it is 'every State's [customary] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[7] And most recently, judging the dispute between Argentina and Uruguay, on the other hand, the ICJ asserted a State is 'obliged to use all the means at its disposal in order to avoid [injurious] activities which take place in its territory, or in any area under its jurisdiction'.[8]

Accordingly, due diligence does not concern itself with the question of who perpetrated the unlawful act but with the jurisdictional origin of the unlawful act. Because, as previously established, the natural person behind the cyber operation is more likely than not to remain unknown, this thesis centres on the territorial jurisdiction. The concept of territorial jurisdiction may however seem in contradiction with the idea that cyber operations occur in 'an abstract realm of data representation',[9] in the mythical and notional[10] domain called cyberspace, which

---

[6] *Island of Palmas Arbitration (Netherlands v US)* [1928] II UNRIAA 839. See also *Affaire Du Lac Lanoux* [1957] UNRIAA XII 281, 296–297

[7] *Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania)* (Merits) [9 April 1949] ICJ Rep 22

[8] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ rep para 101

[9] Ramberto A Torruella Jr, 'Determining Hostile Intent in Cyberspace' (2014) 75 Joint Force Quarterly 117

[10] 'Cyberspace' in *Oxford Dictionaries* (OUP 2018) <https://en.oxforddictionaries.com/definition/cyberspace> accessed 6 January 2018

is a global common and a domain where national jurisdictional concepts do not apply.[11] In reality, cyberspace consists of more than a virtual dimension; it is a 'set of interconnected information systems and the human users that interact with these systems'.[12] And cyber operations occur through the utilisation of cyberspace elements being *inter alia* servers, working stations, routers, switches and firewalls, satellites and all its elements which are physically present in a specific territory. Territory does nevertheless constitute 'all those spaces where the sovereign exercises formal jurisdiction or factual authority.'[13]

While the injured State may not be able to identify the particular natural person behind the malicious cyber operation and establish the connections to the responsible State as required by the stringent legal standards of attribution, the evidence of jurisdictional origin of malicious cyber operations is more often than not available. This is the source of the potential utility of due diligence in establishing accountability for the unlawful minimisation of power and security of the injured State and the subsequent employment of compliance-inducing countermeasures. Perhaps this is why several scholars recognised and attempted to apply the principle of due diligence to cyberspace. Tsagourias, for example, asserts that due diligence 'places an obligation on states to interfere with private actors and private conduct within their jurisdiction in order to streamline their behaviour in line with the State's international law obligations'[14] while Schmitt argues that it imposes taking 'measures to ensure [State's] territories are not used to the detriment of other states'.[15] A similar characterisation

---

[11] *See eg* Mark Barrett et al, 'Assured Access to the Global Commons Final Report' (NATO 2011); Gerald Stang, 'Global commons: Between cooperation and competition' (2013) 17 European Union Institute for Security Studies Brief 1; US Department of Defense, 'Home and Defense and Civil Support Joint Operating Concept' (version 2.0, 1 October 2007) ES-3

[12] Rain Ottis & Peeter Lorents, 'Cyberspace: Definition and Implications' in *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April* (Academic Publishing Limited 2010) 267–270

[13] *Al-Skeini v UK* [2011] ECtHR 55721/07

[14] Nicholas Tsagourias, 'Economic cyber espionage and due diligence' (Syracuse University, May 2015) 1 <http://insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf> accessed 7 January 2018

[15] Michael Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale L J Forum 68

is offered by Sklerov.[16] In fact, these definitions are analogous to the Tallinn Manual, affirming States 'shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.[17] States too have been more and more vocal in supporting (at least in theory) the existence of due diligence in cyberspace. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) agreed that nations 'should seek to ensure that their territory is not used by non-State actors to commit [internationally wrongful acts using ICTs]'.[18] Similarly, the Council of the EU argued in 2017 that '[States] should not knowingly allow their territory to be used for internationally wrongful acts using [information communication technology (ICT)]'.[19] Additionally, a Multinational Experiment 7 (MNE7) Outcome 3, a product of 16 States and NATO, declared that tolerance, passiveness and indifference towards the malicious (group of) individuals, even if not under the control of the government, 'implies that the State does not respect the duties of due diligence over activities on its territory'.[20] Individual States have also spoken in favour of the requirement of due diligence in cyberspace. Australia argues that, as much as 'a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states'.[21] Furthermore, the US Cyber Diplomacy Bill, (only) introduced in the Congress in 2017, affirms '[c]ountries should take all

---

[16] 'States have an affirmative duty to prevent cyberattacks from their territory against other states.' Matthew J Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 Military L Rev 1, 62–63

[17] Michael Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 26. The assertion has been restated in Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

[18] UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 13

[19] Council of the European Union, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption' (Brussels, 7 June 2017) 9916/17, 4 <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> accessed 17 May 2019

[20] 'Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.3: Concept Framework' (MNE7) (Version 3.0, 3 October 2012) 8 [on file with the author]

[21] Australia, 'Australia's International Cyber Engagement Strategy' (Annex A: Australia's position on how international law applies to state conduct in cyberspace, 4 October 2017) 91

appropriate and reasonable efforts to keep their territories clear of intentionally wrongful acts using ICTs in violation of international commitments'.[22] In a similar vein, Germany argued nations are to 'take all necessary measures to ensure that their territories are not used'[23] for the purpose of an unlawful cyber operation against other State(s). India recognised States' responsibility to ensure that their ICT is not utilised 'to target or attack the ICT infrastructure of another nation'.[24] Similarly, the Russian Federation argued States 'bear responsibility at international level for [the unlawful] actions in information space, carried out directly, under their jurisdiction or in the framework of international organisations of their membership'.[25] Finland,[26] Spain,[27] France[28] and the Netherlands,[29] echoing the Corfu Channel judgment text and Tallinn Manual definition, also recognised the principle of due diligence in the cyber space.

2.1. Due diligence obligations to prevent and to terminate

Due diligence imposes upon States an obligation to prevent and an obligation to terminate the known unlawful acts emanating from their territories. The existence of this pair of obligations is supported by international jurisprudence. In the Alabama Claims arbitration, for example,

---

[22] HR 3776 Cyber Diplomacy Act of 2017, 115th Congress (2nd Sess 2018) SEC.3 (5)(c)
[23] UNGA 'Developments in the field of information and telecommunications in the context of international security' (9 September 2013) UN Doc A/68/156/Add.1, 9
[24] *Cited in* Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law' (2010) 88 Texas L Rev 1591
[25] Ibid. Note also the statement by Andrey Krutskikh, the Russian representative to the UN: 'States should not use go-betweens to carry out [cyber] attacks or allow their territories to be used for such purposes'. UNGA 'Potential Security Impacts of Cyberspace Misuse Considered in First Committee, as Speakers Warn of Arms Race, Emergence of New Theatre of Warfare' (30 October 2015) UN Doc GA/DIS/3537 <https://www.un.org/press/en/2015/gadis3537.doc.htm> accessed 4 June 2019
[26] 'Sovereignty also includes responsibility. A state must see to it that its area will not be used in an attack against another state.' Government of Finland, 'Finland's Cyber Security Strategy - Background Dossier' (Government Resolution 24 January 2013) 33 <http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/48-finlandas-cyber-security-strategy-background-dossier> accessed 4 June 2019
[27] '[N]ot knowingly allow their territory to be used to commit internationally wrongful acts using [information and communications technologies] technologies.' UNGA 'Developments in the field of information and telecommunications in the context of international security' (19 July 2016) UN Doc A/71/172, 19
[28] François Delerue & Aude Géry, 'France's Cyberdefense Strategic Review and International Law' (*Lawfare*, 23 March 2018) <https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law> accessed 9 June 2019
[29] Netherlands called for an 'examination of 'the question of the application of the principle of due diligence, i.e. not to knowingly allow a State's territory to be used for acts contrary to the rights of other States.' Kingdom of the Netherlands, 'Developments in the field of information and telecommunications in the context of international security' (Resolution 69/28, 2015) 4

the British Government was found to have failed to exhibit due diligence in relation to the performance of its obligation of neutrality. Britain, the decision reads, failed to 'take in due time any effective measures of prevention'[30] and consequently violated the principle of due diligence, 'a diligence proportioned to the magnitude of the subject and to the dignity and strength of the power which is to exercise it'.[31] The ICJ reiterated the due diligence and the corresponding obligation of prevention in the Corfu Channel Case judgment, where the Court held Albania responsible for its failure to take all necessary steps to prevent the internationally wrongful act of mine laying.[32] Further international judicial decisions,[33] international agreements[34] as well as the legal scholarship,[35] substantiate the prominence of the due diligence principle and the accompanying obligation of prevention in the modern international legal system. A significant doctrinal development of the principle of due diligence can be observed in the domains of international humanitarian, investment, criminal, environmental and maritime law.

The principle of due diligence also dictates an obligation of termination; once the unlawful act materialises, States are under the due diligence obligation to terminate or stop the violation of the rights of the other State. For instance, Iran, which had an obligation to prevent the violation of the US' rights granted by the Vienna Convention on Diplomatic Relations, was found to be

---

[30] *Alabama Claims of the United States of America Against Great Britain* [1871] UNRIAA XXIX 130

[31] *Alabama case* (United States of America v Great Britain) (decision of 14 September 1872) *in* John B Moore, *History and Digest of the International Arbitrations to which the United States has been a Party* (vol I, GPO 1898) 572

[32] *Corfu Channel case* (n 7) 23

[33] See eg *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep; *Case Concerning Gabčíkovo-Nagymaros Project (Hungary v Slovakia)* [1997] ICJ Rep

[34] *Eg* ILC 'International Liability for Injurious Consequences Arising out of Acts not Prohibited by International Law (Prevention of Transboundary Harm from Hazardous Activities)' (2001) II (Part Two) Ybk of the ILC, UN Doc A/CN.4/SER.A/2001/Add.1 (Part 2) 144; Convention on the Law of the Non-Navigational Uses of International Watercourses (New York, 21 May 1997) art 7

[35] *Eg* Pierre-Marie Dupuy, 'Due Diligence in the International Law of Liability' *in* OECD, *Legal Aspects of Transfrontier Pollution* (OECD 1977) 369–379; *Barnidge* (n 4); Jan Hessbruegge, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law' (2004) 36(2) NYU J Intl L & Pol 265

internationally responsible by the ICJ because it did not make any efforts 'to stop or impede'[36] the militants from overrunning the American embassy in Tehran.

A wealth of national and international pronouncements suggest that States indeed recognise the existence of the aforementioned due diligence obligations also in cyberspace. In fact, a study conducted by ENISA and the European Parliament noted that '[m]ost norm proposals from governments and international organisations'[37] recognise the obligation of prevention as part of the applicable principle of due diligence in cyberspace. Also, a group of States under the umbrella of the MNE7 argued 'States have a duty to prevent cyber attacks as a matter of law',[38] while China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan have recognised 'the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security'.[39] The requirement of prevention in the context of due diligence in cyberspace has been further recognised by Finland,[40] Belarus,[41] Estonia[42] and Spain.[43]

Opinio juris also suggests that due diligence requires more than an attempt to prevent an unlawful cyber operation in violation of the rights of other States; it requires the States to do utmost to terminate an ongoing cyber operation. The Council of Europe (COE), for example,

---

[36] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* [1980] ICJ Rep para 18

[37] European Parliament, 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU' (2017) EPRS/STOA/SER/16/214N 18

[38] *MNE 7* (n 20) 7

[39] UNGA 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (13 January 2015) UN Doc A/69/723, 3

[40] '[A State] must, therefore, also try to prevent attacks beyond its national borders perpetrated by private entities.' *Government of Finland* (n 26) 19

[41] Belarus submitted that the international information security depends on the 'the need to prevent the possible misuse of information and communications technology (ICT) so as to undermine national security and stability and international security. UNGA 'Developments in the field of information and telecommunications in the context of international security' (11 August 2017) UN Doc A/72/315, 6

[42] Kersti Kaljulaid, 'President of the Republic at the opening of CyCon 2019' (Office of the President of Estonia, 29 May 2019) <https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/> accessed 4 August 2019

[43] *UN Doc A/71/172* (n 27) 19

maintained that the due diligence principle in the cyber domain encompasses not only the requirement to prevent the unlawful cyber operations emanating from one's territory but also to 'respond to disruptions or interferences, or to minimise risk or consequences'.[44] Additionally, Australia noted that even though prevention is not always possible, States are to do their utmost 'to put an end to the harmful activity'.[45]

Prior to discharging the obligations of prevention and termination when the circumstances demand, due diligence principle dictates the development of capacity, enabling the States to do so. In other words, due diligence requirements are twofold – States are **to develop** the capacity of performance prior to the occurrence of the cyber incident **and to utilise** the capacity or to act when circumstances demand or when the actual cyber operation is underway. Even from a standpoint of terminology, as understood by the UN Office for Disaster Risk Reduction, prevention indicates 'the intention to completely avoid potential adverse impacts through action taken *in advance'*.[46] According to Pisillo Mazzeschi, an obligation to prevent requires the States to develop 'a legal and administrative apparatus normally able to guarantee respect for the international norm on prevention'[47] as well as to utilise the aforementioned apparatus when the need arises. The same holds true for the obligation of termination: discussing due diligence in the context of the law of the non-navigational uses of international watercourses, the ILC argued "[t]he State may be responsible ... for not enacting necessary legislation, for not enforcing its laws ..., or for not preventing or terminating an illegal activity'.[48] In other words, States are legally bound by the due diligence duties before, as well as, during the occurrence of the unlawful cyber operation. Although this may be true, the need

---

[44] Council of Europe, 'International and multi-stakeholder co-operation on cross-border Internet' (Directorate General of Human Rights and Legal Affairs, 2010) para 73
[45] *Australia's International Cyber Engagement Strategy* (n 21)
[46] United Nations Office for Disaster Risk Reduction, '2009 UNISDR Terminology on Disaster Risk Reduction' (May 2009) 22 [emphasis added]
[47] Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 GYIL 9, 26–30
[48] ILC, 'Report of the Commission to the General Assembly on the work of its forty-sixth session' (1994) 2(II) Ybk of the ILC 103 *citing* Restatement of the Law, Third, Foreign Relations Law of the United States, vol. 2 (St. Paul, Minn., American Law Institute Publishers 1987) 105, section 601(d)

for capacity building goes beyond the legislation and administrative apparatus. Dupuy, for example, claimed States are required to possess not only a legal system but also the material resources necessary to comply with the obligations of due diligence.[49] Also, to be able to prevent or terminate the unlawful acts emanating from their territory, States are required to diligently control the cyber infrastructure on their territory or under their jurisdiction. As maintained by Judge Alvarez in his dissenting opinion in the Corfu Channel case, it is the obligation of every State 'to preserve in its territory such order as is indispensable for the accomplishment of its international obligations'[50]. In other words, States are to do their utmost to develop and possess jurisdictional capacity[51] which will in turn allow the performance of the obligations stemming from the due diligence principle.

There is no real reason to limit oneself to legislative and administrative measures, material resources or territory control or monitoring when considering the requirement of capacity building in terms of due diligence for what it prescribes are obligations of conduct and not the methodology of performance. For instance, in the Alabama Claims award the tribunal did not specify the measures required to comply with the obligation of prevention; Great Britain was found to be responsible for failing to employ 'measures *adequate* to prevent the violation of [its international obligations]'.[52] The relevant ICJ judgments similarly made no attempt to restrict the due diligence capacity building requirement to legislative and administrative measures.[53] Also, in the cyber context, the UN General Assembly argued 'States should ensure that their laws *and practice*'[54] do not incite unlawful cyber behaviour.

---

[49] *Dupuy* (n 35) 373: 'Government or a State should possess on a permanent basis, a legal system and material resources sufficient to ensure the fulfilment of [its] international obligations under normal conditions.'
[50] *Corfu Channel case* (n 7) (Dissenting Opinion by Judge Alvarez) 44
[51] *Tsagourias* (n 14) 2
[52] *Alabama Claims* (n 30) 131 [emphasis added]
[53] *United States Diplomatic and Consular Staff in Tehran* (n 36) 12; *Corfu Channel case* (n 7) 23; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep para 292
[54] UNGA Res 55/63 (22 January 2001) UN Doc A/RES/55/63 para 1(a)

Additionally, writings of several prominent scholars recognised the due diligence obligations of prevention and termination as well as their dual structure in the cyber context. Tsagourias rightly argues that States are, firstly, expected to build institutional, resource and jurisdictional capacities. Specifically, States are expected to prevent malicious cyber operations by developing the 'legal, administrative and institutional mechanisms', assuring 'human, financial and technical resources' and, subject to resources available, to exercise control over the activities within its territory.[55] Secondly, the aforementioned capacity is to be employed through act of termination when the specific situation arises. Buchan similarly contends that States are to 'equip themselves with the means to detect, prevent, mitigate and punish [internationally wrongful] conduct by non-state actors within their territory'[56] as well as attempt termination when a cyber threat occurs. Bannelier, discussing the international law of low-intensity cyber operations, claims the States are to employ best efforts to prevent and stop malicious cyber operations emanating from one's territory, which includes enacting preventive domestic normative measures, protecting cyber infrastructure (from misuse) and reacting to the occurrence of such operation by way of investigating and punishing the authors.[57] The clear dual structure of due diligence in cyberspace that dictates the development as well as the deployment of the capacity to prevent and terminate has been emphasised by other scholars.[58] Other, less structured approaches to due diligence in cyberspace are also available. Due diligence in the cyber context, so argues Sklerov, can be decompiled into several duties – enacting 'stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and […] cooperating with the victim-states of cyberattacks that originated from within their borders'.[59] Lastly, focusing exclusively on the obligations of

---

[55] *Tsagourias* (n 14) 2
[56] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) J of Conflict & Security L 429, 439
[57] Karine Bannelier, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2014) 14 Baltic Ybk of Intl L 32, 37–39
[58] *See eg* Jutta Brunnée & Tamar Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (2015) 58 GYIL 129, 137–144
[59] *Sklerov* (n 16) 62–63

developing capacity, Kolb argues States are under the obligation to 'create and maintain'[60] an effective system of internal security (supplied with necessary personal, financial, and technical instruments), to adapt the enabling and appropriate legislation, and to seek international cooperation and information exchange.

2.2. The condition of knowledge

Due diligence is conditioned by knowledge of an emanating conduct in contravention to the legally protected international rights of another State. In other words, the omission of the appropriate prevention and termination steps constitutes a violation of international law only if the non-diligent State of emanation had or ought to have had knowledge of the unlawful cyber operation in question. To illustrate, Iranian authorities 'were fully aware'[61] of their obligation to exhibit diligence in the efforts to prevent and terminate the violation of the foreign diplomatic premises as well as the urgency of the situation, established the United States Diplomatic and Consular Staff in Tehran case. In fact, the requirement of knowledge as the precondition for the materialisation of the obligations of due diligence was previously emphasised also in the Alabama Claims arbitration and Corfu Channel case. Specifically, the ICJ in the Corfu Channel case asserted that 'the laying of the minefield which caused the explosions could not have been accomplished without the knowledge of the Albanian Government'.[62] Under these circumstances, the 'knowledge of the minelaying as such imposed on the Albanian authorities the duty to act. Knowledge was the test of imputability of unlawful omissions.'[63] Generally, scholars of international law in the context of cyberspace have not disputed the idea that knowledge is what triggers the obligation of due diligence. A State 'had or ought to have had the knowledge and the means to avert the situation' argues Bannelier.[64] Similar assertions

---

[60] Robert Kolb, 'Reflections on Due Diligence Duties and Cyberspace' (2015) 58 GYIL 113, 117
[61] *United States Diplomatic and Consular Staff in Tehran* (n 36) para 68
[62] *Corfu Channel case* (n 7) 22
[63] Il Y Chung, *Legal Problems Involved in the Corfu Channel Incident* (Librairie Droz 1959) 168
[64] *Bannelier* (n 57) 6

were made by many other legal scholars.[65] CoE also confirmed the reasoning by stipulating that the States are under no obligation to prevent or terminate the cyber operations of which they have or had no knowledge. [66]

Doctrinal development points in two different directions – a State is responsible for failing in its due diligence obligations either because it knew or because it should have known of the cyber operation against the rights of another State. For State responsibility to arise, therefore, 'actual or, at least, constructive knowledge on the part of the [State] is essential'.[67] On one hand, the authors of the Tallinn Manual conditioned the duty of due diligence with the actual knowledge of the malicious cyber operation.[68] The obligation arises only if State organs 'have detected a cyber operation […] originating from its territory or if the aggrieved party to the conflict has credibly informed the [State] that a cyber operation has originated from its territory'.[69] The responsibility for lack of vigilance in the prevention or termination efforts was established on the basis of actual knowledge in the case of Alabama Claims arbitration[70] and the ICJ Teheran Hostages case,[71] where the United Kingdom and Iran were, respectively, informed of the lack of prevention and termination measures or the danger of the unlawful act by the parties injured in the course of the contentious events.

Nevertheless, a widely held understanding holds that State responsibility will arise also on the basis of constructive knowledge. 'To incur responsibility on this basis it is enough that the State was aware, or should normally have been aware, of the serious danger that [the unlawful act] would be committed'[72] argued the ICJ in the Genocide case. Formulated on the reasoning

---

[65] See *Buchan* (n 56) 16; *Tsagourias* (n 14); *Kolb* (n 59) 123–124; Christian Walter, 'Obligations of States Before, During, and After a Cyber Security Incident' (2016) 35 GYIL 67, 74
[66] *Council of Europe* (n 44) 74
[67] Georg Schwarzenberger, 'The Principle of International Responsibility (087)' in Hague Academy of International Law (ed), *Collected Courses of the Hague Academy of International Law* (Brill Nijhoff 1955) 352
[68] *Schmitt 2013* (n 17) rule 5 (10)
[69] ibid rule 93 (5)
[70] *Alabama Claims* (n 30)
[71] *United States Diplomatic and Consular Staff in Tehran* (n 36)
[72] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 53)

offered by the ICJ in the latter as well as the Corfu Channel case, Buchan, Tsagourias, Pirker[73] and Heintschel von Heinegg[74] recognised the prevalence of the theory arguing in favour of the permissive constructive knowledge sufficiency in establishing State responsibility for the omission of prevention and termination. CoE offered similar view.[75]

In determining the appropriate test of knowledge, one has to, however, take into consideration the circumstances of the omission[76]. Placing the dispute in the context of countermeasures for the violation of the due diligence leads to the appreciation of both – actual as well as the constructive knowledge test.

Considering that countermeasures are only to be employed after the injured party has notified the responsible State of its intentions to do so and has invited it to fulfil its international obligations,[77] the targeted entity has the opportunity to make the non-diligent State actually aware of the malicious unlawful act emanating from its territory. A notification, and with it the potential to reduce the benefits of the unlawful conduct, is likely to induce the responsible State to attempt to terminate the outgoing cyber operation. Depending on how diligent the State was in the development of its performance capacity, this scenario could compel the wrongdoing State into compliance with international law. If, on the other hand, the responsible State persists with the non-diligent behaviour related to the obligation of termination or has not reached the minimum standard pertaining to the development of the termination capacity, countermeasures can follow.

---

[73] Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', *in* Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCD COE 2013) 204–206

[74] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 Intl L Studies 123, 136

[75] *Council of Europe* (n 44) para 74

[76] ILC, 'Report on International Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur' (1956) II Ybk of the ILC, UN Doc A/CN.4/96, 216

[77] ILC, 'Materials on the Responsibility of States for Internationally Wrongful Acts' (UN Legislative Series, 2012) UN Doc ST/LEG/SER B/25, art 52 para 1(a) & art 43

On the other hand, States may wish to employ urgent countermeasures and omit the prior notification of the allegedly responsible State. The condition of knowledge, however, persists and the inured States wishing to take urgent countermeasures against the non-diligent State should examine the existence of the constructive knowledge. Founded on the Corfu Channel case reasoning, the constructive knowledge test is determined upon the consideration of two aspects – a general attitude of the State towards acquiring knowledge of similar events and the feasibility of acquiring knowledge of the particular event. In a first deliberation the Court concluded that, *inter alia*, the past Albanian actions and diplomatic communication in support of its surveillance of the Corfu strait, confirm Albania was normally aware of the happenings in the area. Secondly, the Court established that, upon conducting a practical test, the occurrence of the unlawful act in the area 'could hardly fail to have been observed by the Albanian coastal defences'.[78] In other words, the Court sought to determine the general attitude of the State towards acquiring knowledge of similar events and the theoretical feasibility of it acquiring the knowledge of the particular event.

As already established, the first element of the constructive knowledge test is a prerequisite for discharging the due diligence obligations of prevention and termination, which expects States to diligently control and monitor their respective territories and the cyber infrastructure under their jurisdictions. It is no secret that regular monitoring of computer networks is indeed an established practice among States. Particularly in the cyber era, States do normally exhibit vigilant observance of the activities in their respective cyber "channels".

The second part of the constructive knowledge test is of a more technical nature and therefore not detailed here. Suffice to say, the State wishing to attribute constructive knowledge to a particular nation, must be certain of the fact that the latter has the capacity to spot the specific (or comparable) outgoing malicious cyber operation. Even though not all cyber operations are alike, a well-developed general capacity to acquire the knowledge of an outgoing cyber

[78] *Corfu Channel case* (n 7) 20

operation would nevertheless imply the ability of a State to do so also in specific circumstances. Recently, former US Secretary of State Tillerson argued that a well-developed intelligence apparatus of a State can indicate the existence of a constructive knowledge which puts the State under the obligation to terminate a conduct in violation of the rights of another State. After several members of the US diplomatic corps in Havana were injured, the Secretary of State said: '[w]hat we've said to the Cubans is: small island. You've got a sophisticated intelligence apparatus. You probably know who's doing it. You can stop it, it's as simple as that.'[79] As a matter of fact, many States do commit to the development or the utilisation of exiting capabilities of detection, the analysis of national cybersecurity strategies indicates. Hungary, for example, vowed to develop 'efficient capabilities to prevent, detect, manage (react), respond to and recover any malicious cyber activity, threat, attack or emergency'.[80] Singapore, on the other hand, committed to 'upgrading of existing detection and analysis capabilities and strengthening preventive and recovery measures',[81] while the Norwegian CERT already does operate the Early Warning System for Digital Infrastructure and has 'the ability to prevent, detect and analyse data related to serious incidents on the Internet'.[82] The implied knowledge of the malicious interstate cyber operation would have been even more apparent when the national legalisation requires ISPs to report such incidents to one of the organs of the State and thus aid the State in its capacity to acquire knowledge. Theoretically, technology is not a limitation here and particularly so in the case of DDoS attacks; computer science scholarship provides that ISPs can indeed spot not only an incoming but also an outgoing DDoS attack.[83]

---

[79] Josh Lederman, 'Cuba mystery: U.S. doctors find brain abnormalities in victims' *CBC* (6 December 2017) <http://www.cbc.ca/news/world/cuba-mystery-brain-1.4435900> accessed 14 January 2018

[80] Hungary, 'Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary' (21 March 2013) Annex, 4

[81] Singapore, 'National Cyber Security Masterplan 2018' (2013) 12

[82] Norway, 'Cyber Security Strategy for Norway' (2012) 21

[83] *See eg* Tao Peng, Christopher Leckie & Rotagiri Ramamohanarao, 'Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring' *in* Nikolas Mitrou et al, *Networking 2004 - Lecture Notes in Computer Science* (vol 3042, Springer 2004) 771–782; Jelena Mirkovic, Gregory Prier & Peter Reiher, 'Attacking DDoS at the Source' *Network Protocols* 2002 (Proceedings of the 10th IEEE International Conference); Brent

With this in mind, it would be acceptable to infer that States with a well-developed cyber intelligence apparatus and an extensive history of Internet censorship or monitoring involving 'constantly [keeping] a close watch over the'[84] ISPs and Internet traffic in general should indeed possess knowledge of the malicious cyber activity using the Internet infrastructure under its jurisdiction.

2.3. Standard of due diligence

The standard of due diligence is a flexible concept. Historically, 'the standard according to which international law has held its subjects accountable for actions of individuals has varied greatly'.[85] Generally speaking, due diligence requires a State to 'deploy adequate means, to exercise best possible efforts, to do the utmost'[86] to prevent or terminate an internationally wrongful conduct emanating from its territory. It requires an honest attempt at prevention or termination; the State exercises due diligence if it 'honestly gives so much care as may seem to an average intelligence to be proportional to the state of things existing at the time'.[87] In other words, States have common but different responsibilities.

The due diligence standard, due to the lack of internationally agreed upon standards regarding cyber operations, admittedly lacks exactness. Nevertheless, lessons from international diplomatic and environmental law point to the fact States are generally expected to observe the standard of a reasonable State or good government.

Rowe et al, 'The Role of Internet Service Providers in Cyber Security' (Institute for Homeland Security Solutions, 2011). See also *Nigerian Communications Commission* n (193) and the accompanying text.

[84] *Corfu Channel case* (n 7) 18

[85] *Hessbruegge* (n 35) 266

[86] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (Advisory Opinion) 34 [2011] ITLOS Rep 10 34

[87] William E Hall, *A Treatise on International Law* (2d edn, Clarendon Press 1884) 196 § 65

In the context of the due diligence principle, States are to exhibit 'reasonable prudence'[88] which is an 'overarching'[89] due diligence standard. The ILC[90], the ICJ[91] as well as other international tribunals[92] and arbitral awards[93] have also confirmed this reasoning. Legal literature also seems to be just as unified.[94] The due diligence standard, specific scholarship asserts, will be no different in the context of unlawful cyber operations.[95] To narrow down the concept of a reasonable commitment by a State, several elements and variables need to be clarified.

Firstly, the due diligence standard is **era-sensitive** and will vary according to the state of the technology (available to a particular State). The International Tribunal for the Law of the Sea (ITLOS)[96] as well as the ILC[97] texts recognise the standard is of variable nature and may change over time. To live up to the standard of a good government, States are required to stay vigilant and informed of various technological and scientific developments.[98] The need to stay up to date is especially prominent in the cyber context. Threat detection methods are progressively more effective. For example, recently a combination of the machine-learning driven modelling and human analysis has proven to be a far more effective method of cyber

---

[88] *In re Eastern Transportation Co. (The T.J. Hooper),* 60 F.2d 737 (2d Cir. 1932) Judge Learned Hand
[89] Tim Stephens & Duncan French, 'ILA Study Group on Due Diligence in International Law' (Second Report, ILA 2016) 7–10
[90] 'Obligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring'. *ILC* (n 77) 114 para 14
[91] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 53) para 430
[92] '[It] is the duty of Contracting States to take reasonable and appropriate measures to enable lawful demonstrations to proceed peacefully.' *Plattform "Ärzte für das Leben"' v Austria* App No 10126/82 (ECHR 21 June 1988) 12 para 34
[93] *L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States* [1926] UNRIAA IV 61–62
[94] *Barnidge* (n 4) 118 recognised 'a flexible reasonableness standard adaptable to particular facts and circumstances.'
[95] See eg *Bannelier* (n 57) 34; *Kolb* (n 60)*; Schmitt 2013* (n 17) 27; *Tsagourias* (n 14) 6; *Buchan* (n 56) 20–21; *Schmitt* (n 15) 68 & 75
[96] According to ITLOS, '[t]he content of "due diligence" obligations may not easily be described in precise terms. Among the factors that make such a description difficult is the fact that "due diligence" is a variable concept. It may change over time.' *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 85) para 117
[97] *ILC* (n 34) art 3 cmt 11
[98] Due diligence 'requires a State to keep abreast of technological changes and scientific developments'. ibid

threat detection than the usual methods.[99] At the same time, the sophistication of cyber operations, in particular the well-funded, State-sponsored ones, is on the rise.[100] Proactive cyber vigilance, including cooperation with other nations and the private sector, reasonable investment in cybersecurity research and development efforts, as well as regular review and evaluation of specific cybersecurity practices, regulatory or legislative measures, is therefore crucial in meeting the ever-changing due diligence standard.

A plain example of what seems to be a lack of an informed and current vigilance is provided by the list of the State-owned Aramco servers attacked in the Shamoon operation; the majority of servers ran on an outdated operating system released in 2003, no less than nine years before the attack.[101]

Secondly, the due diligence standard depends on the **circumstances** surrounding the unlawful act. When considering circumstantial variables of the due diligence standard, due diligence obligations must be satisfied in a timely manner while the required action depends on the target, foreseeability, magnitude and probability of harm. Whether the (re)action of the State amounted to this requirement is 'not measured by any absolute standard, but depending on the relative facts of the special case'.[102]

Specifically, the State must 'inform itself of factual or legal components that relate foreseeably to a contemplated procedure and [must] take appropriate measures in timely fashion, to address them'.[103] Similarly, when the State is equipped with knowledge of the imminence of

---

[99] *See eg* Kalyan Veeramachaneni et al, 'AI^2: Training a big data machine to defend' (2016) IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (New York, 9–10 April 2016)

[100] Seung Hyun Kim, Qiu-Hong Wang & Johannes B Ullrich, 'A comparative study of cyberattacks' (2012) 55(3) Communications of the ACM 66–73

[101] 'Saudi Aramco digital explosion Six days passed, network still down' (*Pastebin*, 20 August 2012) <http://pastebin.com/cTJeeTat> accessed 7 January 2019

[102] UN Human Rights Office of the High Commissioner, 'The Corporate Responsibility to Respect Human Rights: An Interpretive Guide' (HR/PUB/12/02, 2012) 4 <https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf>

[103] *ILC* (n 34) art 3 cmt 10

an unlawful act and 'does not take timely steps to prevent such act',[104] international responsibility arises. In fact, because the orders to its State agent were not only delayed but also impractical, the Alabama Claims tribunal ruled that the British government failed to exhibit due diligence in the performance of its neutral obligations.[105] On the other hand, the ICJ did not find Iran internationally responsible for the early attacks on American diplomatic premises by the mob, since Iranian authorities, though failing to in fact prevent the attack, 'they acted *promptly* in response to the urgent appeal for assistance made by the Embassy during the attack.'[106] The CoE has applied this doctrinal requirement to cyberspace.[107]

Considering the aforementioned requirement, diligent behaviour, materialised in the form of appropriate legislation, technical capacities, organisational measures, capacity building and (inter)national cooperation, would have to be taken prior to the occurrence of the transboundary cyber incident. Only these actions, taken in a timely manner or without necessary hesitation, would realistically allow taking actions of prevention and termination.

Another circumstantial variable comes distilled from the international diplomatic law; the required standard of vigilance depends on the foreseeability or probability of the unlawful act. The arbitral award in the case of Chapman v United Mexican States made it clear – Mexico was expected to meet a higher standard of diligence in relation to the obligation of the protection of aliens due to the fact that serious threats had been made against the safety of an American consular official and that 'such threats had been brought to the attention of the appropriate Mexican authorities'.[108] A more recent confirmation of the reasoning comes from ITLOS; the tribunal emphasised due diligence obligations may 'change in relation to the risks involved in the activity'.[109] When assessing the risk, States are to consider the nature and

---

[104] ILC, 'Second Report on International Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur' (1957) II Ybk of the ILC, UN Doc A/CN.4/106, 109
[105] *Alabama Claims* (n 30) 130
[106] *United States Diplomatic and Consular Staff in Tehran* (n 36) para 14
[107] *Council of Europe* (n 44) para 73
[108] *William E. Chapman (U.S.A.) v United Mexican States* [1930] UNRIAA IV, para 634
[109] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 86) para 117

magnitude of the action in question.[110] It goes without saying that riskier activities demand a more stringent standard of vigilance. When considering the level of required diligence in the cyber context, the authors of the Tallinn Manual argue that variables such as '[t]he nature, scale, and scope of the (potential) harm'[111] of the cyber operation should be considered. The CoE, too, discussing due diligence in the cyber context, felt the scope *and* risk of an injurious cyber operation define the required standard of care.[112] Some scholars have offered similar views.[113]

It is safe to say States are generally aware of the probability of malicious cyber operations originating from their infrastructure. Whether this holds true for a specific cyber operation, making it foreseeable, is another matter and remains unknown. Still, a higher standard of care would be expected with the probability of a cyber operation targeting foreign critical (network) infrastructure or systems vital to the wellbeing of the society. The aforementioned targets not only imply a significant scope of harm inflicted by the malicious cyber operation but also cater to the proponents of the necessity for greater vigilance when targeted subjects (and objects) are of special interest to the State.[114] On the other hand, notwithstanding the potential of a swift propagation of the malicious code, an operation targeting a smaller number of personal computers or workstations would, require a more lenient standard of diligence.

Thirdly, the standard of due diligence is subjective and depends on the State's **capacity** to fulfil its obligations. The Corfu Channel judgment opined that 'vigilance depends on the means available to a given State.'[115] Indeed, a State cannot be expected to 'exercise greater vigilance

---

[110] *Pulp Mills on the River Uruguay* (n 8) para 205
[111] *Schmitt 2013* (n 17) 33
[112] 'The required degree of care should be proportional to the degree of risks involved or consequences incurred.' *Council of Europe* (n 44) 18 para 74
[113] *Walter* (n 65)
[114] Deriving from international diplomatic law, where, so Garcia-Amador, '[due diligence] standard varies according to the persons concerned, in the sense that the State has a special duty of vigilance, and has therefore a greater responsibility, in respect of persons invested with a recognised public status.' *ILC* (n 76). *See also* James Crawford, *Brownlie's Principles of Public International Law* (8th edn, OUP 2012) 403 arguing there is 'a special standard of care over and above the normal obligation to show due diligence in protecting aliens within the State'.
[115] *Corfu Channel case* (n 7) (Individual Opinion of Judge Alvarez) 44

than is consistent with the means at its disposal'[116], a notion that fits in the concept of the reasonableness of due diligence. The notion is implicit in the observations that States are to do everything in their power to prevent and terminate the occurrence of unlawful acts; in the words of Kunz, inspired by the writings of the ILC, a 'State which has used all the means at its disposal to prevent a violation of its [international obligations] but is unable to prevent it, has fulfilled its international duty'.[117] A similar notion can be observed in the William E. Chapman (USA) v United Mexican States[118] judgment, in the Article 194(1) of the UN Convention on the Law of the Sea (UNCLOS)[119] and, specifically in the context of due diligence in cyberspace, by the CoE[120] and different authors.[121] Specifically, the level of scientific knowledge,[122] the technological[123] and economic[124] capacities are oft-considered variables of due diligence standard in the cybersecurity context.

It is not hard to sympathise with the advocates of the wholly variable standard. Cyberspace indeed is a (relatively) new domain and achieving the international minimum standard, especially for developing countries, may seem everything but possible. It involves long-term effort, human capital of specialists and, due to the fact that much of technological development in the domains of security and prevention is conducted by private entities, significant financial resources. Indeed, meeting an international standard of diligence in the current context, with its technological underpinning, is a complex task. For this reason, the developing States may

---

[116] ibid
[117] Josef L Kunz, 'Sanctions in international law' (1960) 54(2) AJIL 331–332
[118] *William E. Chapman (U.S.A.) v United Mexican States* (n 108) 632
[119] United Nations Convention on the Law of the Sea (Montego Bay, 10 December 1982) art 194(1)
[120] State duties standard is 'commensurate with the overall capabilities of the country' *Council of Europe* (n 44) para 74
[121] *Tsagourias* (n 14); *Schmitt* (n 15) 75–76; Martin Ney & Andreas Zimmermann, 'Cyber-Security Beyond the Military Perspective: International Law, "Cyberspace", and the Concept of Due Diligence' (2015) 58 GYIL 51; Michael Schmitt, 'Cyber Responses "By The Numbers" in International Law' (*EJIL: Talk!*, 4 August 2015) <http://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/> accessed 7 January 2018
[122] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 86) para 162
[123] Oliver Dörr, 'Obligations of the State of Origin of a Cyber Security Incident' (2015) 58 GYIL 87
[124] August Reinisch & Markus Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State' (2015) 58 GYIL 101

be 'permitted to exercise less diligence'[125] compared to its counterparts with 'a well-developed economy and human and material resources and with highly evolved systems and structures of governance'.[126]

Be that as it may, the principle of due diligence has been explicitly linked to the international standard of justice.[127] In the cyber context, considering the extraordinary interdependency of the national cybersecurity environments, States are therefore required to meet the standard of common prudence[128] or an international minimum standard.[129] Tsagourias, applying the ITLOS advisory opinion rationale,[130] addressed the topic of due diligence in the context of cyber espionage and argued in favour of the international minimum standard; the lack of it would allow 'private or public actors [to] operate from States with lesser capabilities and in doing so jeopardise international law'.[131]

International responsibility arises when the State fails to meet the expected international minimum standard attached to duties related to either the development of capacity building or discharging the due diligence obligations. Support for this assertion may be found in the, for example, Neer L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States decision, where the General Claims Commission concluded that an insufficient State conduct in the context of due diligence obligations will give rise to State responsibility regardless of '[w]hether the insufficiency proceeds from deficient *execution* of an intelligent law or from the fact that the laws of the country do not *empower* the authorities to measure up to international standards'.[132] Due to the technical nature and relative novelty of cyber operations, the

---

[125] Duncan French & Tim Stephens, 'ILA Study Group on Due Diligence in International Law' (1st Report, 7 March 2014) 18
[126] *ILC* (n 34) 155
[127] *ILC* (n 104) 122 para 8. See also *Pisillo-Mazzeschi* (n 47) 44; *Dupuy* (n 35) 369, 372
[128] 'Reasonable prudence is common prudence' *In re Eastern Transportation Co. (The T.J. Hooper)* (n 88)
[129] *L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States* (n 93) 61
[130] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 86) para 159
[131] *Tsagourias* (n 14) 6
[132] *L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States* (n 93) 62 [emphasis added]

development of capacity allowing for prevention and termination should encompass more than only the legislative frameworks; this is well elaborated in the following section.

When an international minimum standard is not embedded in the primary obligation, it can be deduced from the 'the applicable principles of international law [and] analogous principles of justice generally recognised by States'.[133] Due to the embryonic state of the international law in the context of cyberspace, the present text will source cyber due diligence minimum standard development trajectories from the standards of due diligence found in various analogous legal regimes and from the habitual performance of States. The latter, articulated in various national strategies, can be interpreted as their 'recognition of [the] commitment'[134] to compliance with the obligation and 'an important legal foundation'[135] of the relevant international minimum standard.

3. Content and the international minimum standard of due diligence in cyberspace

3.1. Developing the capacity of performance

The above-exposed lack of unity among international lawyers regarding the content and minimum standards of the capacity required to diligently prevent and terminate malicious inter-State cyber operations emanating from a particular territory may be overcome by looking beyond the boundary of legal scholarship.

[133] American Law Institute, *Restatement of the law, second: foreign relations law of the United States* (American Law Institute Publishers 1965) para 165.2
[134] ILC, 'Draft Articles on the Protection of Persons in the Event of Disasters, with commentaries' (2016) II(2) Ybk of the ILC, UN Doc A/71/10, art 9 cmt 6
[135] ibid art 9 cmt 5

If due diligence requires States to remain vigilant, to 'exercise good faith'[136] and 'honestly intending to fulfil the obligations'[137] of prevention and termination, a serious and diligent national commitment to cybersecurity is required; only a serious commitment to cybersecurity will amount to a capacity which will enable the State to effectively prevent and terminate an incoming as well as an outgoing cyber operation. Several attempts to conceptualise (and assess) national commitments to cybersecurity have been made.[138] The most authoritative and comprehensive one comes from a specialised UN agency, the International Telecommunication Union (ITU). The Global Cybersecurity Index (GCI) was compiled to assess 'each nation state's level of commitment to cybersecurity'[139] and 'foster a global culture of cybersecurity'.[140] It is based on the ITU Resolution 130 and the agency's mandate to assist in building 'confidence and security in the use of information and communication technologies'[141] of the ITU member States.

The framework rests on five pillars of cybersecurity commitment and is supported by various forms of strategic and legislative commitments of different States. The GCI elements form a theoretical model of a flawlessly diligent State with an absolute commitment to cybersecurity. It indicates which areas of capacity building should be considered by the diligent States if they want to prevent and terminate malicious cyber operations emanating from their respective territories. Addressing all the pillars of capacity building does not guarantee a successful prevention or termination, nor is this a legal requirement by the due diligence obligations of conduct, demanding a genuine effort rather than a result. However, by addressing all the areas

---

[136] Eric T Jensen, 'Cyber Sovereignty: The Way Ahead' 50 (2) Texas J of Intl L 298

[137] 'Sir Alexander Cockburn's dissenting opinion in the Alabama Claims Arbitration of September 14th, 1872' in *Papers Relating to the Treaty of Washington* (US GPO 1872) 230, 255. In fact, in the Alabama case, the failure to meet the standard of due diligence was established on the basis of the fact that the orders to the sailors to fulfil the duties of prevention (in this case the detention of the vessel) 'were issued so late that their execution was not practicable'. *Alabama Claims* (n 30) 130

[138] *For an overview see eg* International Telecommunication Union & ABI Research, 'Cybersecurity Index of Indices' (Geneva, 2 July 2015) <goo.gl/DljNto> accessed 30 September 2016

[139] ITU BDT Focal Point for Question 3/2, 'Global Cybersecurity Index – Reference Model' (Second Meeting of ITU D Study Group 2, Document 2/164 E, 22 July 2015)

[140] ibid

[141] ITU 'Final Acts of the Plenipotentiary Conference (Guadalajara, 2010)' (2011) 271, 277

of capacity required for cybersecurity, a State has the biggest potential to succeed in prevention and termination. Hence, it is submitted that States are under the obligation to strive towards the ultimate commitment to cybersecurity or the satisfaction of all the elements of cybersecurity commitment listed below rather than to succeed in preventing or terminating the unlawful cyber act. This is not to say that there is no minimum threshold of performance required by the law; the section elaborates the international minimum standards pertaining to the specific elements of due diligence.

3.1.1. Legal measures

As explained, the requirement of legislative measures in the attempt to observe the due diligence obligation of prevention and termination has been recognised by the customary international law as well as general and cyber-inspired legal scholarship. The function of appropriate cyber legislation is an enabling one. It not only allows the State to perform its duties of prevention and termination in terms of developing the capacity of performance by 'providing a harmonised framework for entities to align themselves to a common regulatory basis'[142] but also to utilise the capacity by setting the 'response mechanisms to breaches, such as through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law'.[143] This could include so called soft law instruments including, voluntary Internet service provider (ISP) Code of Practice with specific provisions related to the prevention and termination of the malicious cyber operations targeting the infrastructure of another State.[144]

Due diligence obligations require the States to enact as well as to enforce the appropriate legal frameworks, which will subsequently allow the prevention or termination of the unlawful cyber operations. This dual structure is clearly expressed in the Pulp Mills judgment where the

---

[142] ITU 'Global Cybersecurity Index & Cyberwellness Profiles' (2015) 31
[143] ibid
[144] *See eg* Internet Service Providers Association of Ireland, 'Code of Practice and Ethics' (2013) para 7.5 <http://www.ispai.ie/wp-content/uploads/2013/09/Code-of-Practice-and-Ethics.pdf> accessed 7 January 2018

ICJ argued the obligation of prevention 'entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement'.[145]

To enact or to possess a sufficient and up to date legislative framework is the least a State can do to conform to the capacity development duties dictated by the due diligence obligations. '[H]aving in place a legal framework that anticipates the taking of "appropriate measures" is a sine qua non for [due diligence obligations]'[146] argued the ILC in its commentary to the Draft Articles on the Protection of Persons in the Event of Disasters and the provisions prescribing the due diligence obligations of disaster risk reduction. A similar argument may be made in relation to the due diligence obligations of prevention and termination in the cyber context. Save for the failed States, the legislative function is indeed in the capacity of every State. Besides a clear agreement in the legal scholarship elaborated above, States too have argued in favour of the requirement, in the context of due diligence, to enact a specific cyber law. Germany, for example, has previously maintained that States should avoid facilitating 'areas of lawlessness in cyberspace' and take 'appropriate national legislative and regulatory frameworks needed to meet international responsibilities'[147] to ensure their territories are not used contrary to the interests of other States. The CoE echoed the German attitude – the due diligence principle in the cyber domain encompasses a requirement to '[formulate and implement] policies'[148] designed to prevent and terminate cyber interferences. Such a prevalence of opinions points to the fact that the enactment of the related legislation constitutes an international standard of diligent behaviour in the prevention and termination

[145] *Pulp Mills on the River Uruguay* (n 8) para 197. The view has also been adopted by the ITLOS advisory opinion *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 86) paras 109–112
[146] *Draft Articles on the Protection of Persons in the Event of Disasters* (n 134) 9 cmt 13 [emphasis added]
[147] UNGA 'Developments in the field of information and telecommunications in the context of international security' (9 September 2013) UN Doc A/68/156/Add.1, 9
[148] *Council of Europe* (n 44) para 73

efforts. Habitual performance of the States supports and confirms the conclusion – as of 2017, 159 UN member States have enacted legislative measures related to cyber conduct.[149]

The subjective nature of due diligence obligations allows States a degree of discretion and thus does not prescribe which areas must be addressed by national legislation. Generally, diligent States with a serious commitment to the prevention and termination of cyber operations targeting a foreign State would enact the legislation related to, *inter alia*, prevention of unauthorised access, protection of domestic infrastructure from manipulation and abuse, prohibition of interference,[150] breach notification,[151] extradition,[152] obligations of ISPs[153] or any other legislation enabling the performance of international obligations of prevention and termination. Considering that due diligence obligations prescribe control over the specific territory, enabling legislation authorising various investigative measures including real time collection of real time content and traffic data[154] would also be necessary.

What is important however, is that the national laws are up to date and reasonably sufficient to allow the State to discharge the obligation of prevention and termination. To this end, the national legislation, 'once adopted, may not be appropriate in perpetuity';[155] what it should be is **synchronised** with the relevant international standards and the state of technology. As much as it is true that the State will incur international responsibility by reason of the omission

---

[149] United Nations Office on Drugs and Crime, 'Cybercrime Repository – Database of Legislation' (*UNODC*) <https://www.unodc.org/cld/v3/cybrepo/legdb/search.html?lng=en> accessed 7 January 2018

[150] *See eg* Cybercrime Act 2007 (Sudan) arts 8–9

[151] *See eg* United States Guam Crimes and Corrections, ch 48, § 48.30, 48.40, 48.50; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art 33

[152] *See eg* Cybercrime and Computer Related Crimes Act 2007 (Botswana) arts 4–16 & 29; Convention on Cybercrime (23 November 2001, entered into force 1 July 2014) ETS 185 art 24; Colombia, 'Policy Guidelines on Cybersecurity and Cyberdefense' (draft, 4 July 2011); Swiss Confederation, 'National strategy for the protection of Switzerland against cyber risks' (19 June 2012) 10; Finland, 'Finland´s Cyber Security Strategy' (24 January 2013)

[153] *Eg* Advance Fee Fraud and other Fraud Related Offences Act 2006 (Nigeria) art 13

[154] *Eg* Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (South Africa) arts 7(2), 8(3), 28(1)(2), 30(1) or 39(4), 50, 40, 62.

[155] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 86) para 222

of the legislation, the act of the 'enactment of a law which conflicts with some particular international obligation of the State'[156] may equally trigger international responsibility. Additionally, due diligence 'requires a State to keep abreast of technological changes and scientific developments',[157] to 'inform itself of factual and legal components'[158] and, on the basis of this, formulate appropriate policies 'expressed in legislation and administrative regulations and implemented through various enforcement mechanisms'[159] opined the ILC. The requirement to stay up to date is especially prominent in the fast-paced cyber domain. Thus, national legislation should be periodically reviewed and adapted. In the context of the time-sensitive standard of due diligence and especially in the context of cyberspace, the obligation to enact and enforce a sufficient legislation is 'of continuous nature'.[160]

Additionally, national laws need to be reasonably **sufficient**. The standard of legal capacity, in case of unlawful cyber operations, may not prescribed by the law but it is quite clear that the State is within the limits of the law '[so] long as these laws are reasonably sufficient to prevent'[161] malicious cyber operations. Sufficiency of domestic legislation in observing the due diligence, has indeed been required before in the Alabama Claims arbitration tribunal.[162] Moreover, in the dispute between Germany and Switzerland regarding the pollution of the Rhine River, the Swiss acknowledged their lack of due diligence in preventing the accident through adequate regulation of its own pharmaceutical industries.[163] In relation to this, Lauterpacht previously offered a similar argument; the State has performed the duty 'so long as these laws are reasonably sufficient'[164] to comply with the obligations stemming from the

---

[156] *ILC* (n 104) 108
[157] *ILC* (n 34) art 3 cmt 11
[158] ibid art 3 cmt 10
[159] ibid
[160] *Council of Europe* (n 44) para 74. The idea is present also in the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities: 'the duty of prevention based on the concept of due diligence is not a one-time effort but requires continuous effort'. *ILC* (n 34) art 12 cmt 2
[161] *Lauterpacht* (n 3) 128
[162] *Alabama Claims* (n 30) 113
[163] ILC, 'Draft articles on the law of the non-navigational uses of international watercourses and commentaries thereto and resolution on transboundary confined groundwater' Ybk of the ILC (1994) II(2) 104
[164] *Lauterpacht* (n 3) 128

due diligence principle. Insufficiency of national legislation is not an excuse to escape the international responsibility; a State 'cannot justify itself for a failure in due diligence on the plea of insufficiency of the legal means of action which it possessed'.[165] Writings of prominent scholars have also confirmed this point of view.[166] Whether the legislation can be considered as sufficient or not depends on the circumstances of a specific cyber operation.

It is also important that the legislation in question is **enforced**. Because cybersecurity and the ability of the State to prevent and terminate a cyber operation depend on the participation of a variety of stakeholders, States must make sure that the specific laws are observed by the subjects under its jurisdiction. Only then will the legislation serve its purpose and provide the desired effect – enabling the State to prevent and terminate an internationally wrongful cyber operation. In the words of the ICJ in the Pulp Mills case, due diligence requires 'a certain level of vigilance in their enforcement and the exercise of administrative control applicable to public and private operators'.[167]

3.1.2. Technical measures

Considering that cyber operations are conducted through the utilisation of computerised telecommunication infrastructure, it is reasonable to submit that technical measures are of vital importance in diligent prevention and termination efforts. Similar to legislation, the technical and procedural measures are an enabling factor in the process of the development of the capacity of performance allowing for the prevention or subsequent termination of the unlawful cyber act. In addition to this, they allow a State to control and monitor the deeds of all subjects within its jurisdictional domain, imperative to diligent State conduct.

---

[165] *Alabama Claims* (n 30) 131
[166] *See eg* Horst Blomeyer-Bartenstein, 'Due diligence' in R Bernhardt (ed), *Encyclopedia of Public International Law* (Elsevier Science Publishers 1987) 140
[167] *Pulp Mills on the River Uruguay* (n 8) para 197

'Technical measures can be evaluated based on the existence of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation State.'[168] Examples of such measures include, but are certainly not limited to, the establishment of national, governmental or sectoral Computer Emergency Readiness Team (CERT), which is responsible for monitoring, warning and response in the event of an incident. The recognition of the vital function of such an entity in national cybersecurity commitments may be deduced from the vows States made in their respective national cybersecurity strategies – no less than 38 of 72 strategies elaborate the responsibilities and organisation of CERTs in different formats.[169] Other data corroborate the deduction; as of October 2016, 102 out of the 193 ITU member States confirmed the existence of an entity and the authority of a CERT.[170]

For the above reasons, the fact that the establishment of a CERT is indeed an international standard in diligent capacity building prescribed by the obligation of prevention and termination of the unlawful inter-State cyber operations should not be contentious proposition. The seemingly high standard is attainable for several reasons, even for less developed States. (Developing) States do have a plethora of international assistance mechanisms at their disposal and meeting this international standard may not be as unachievable as it may first appear. ITU, for example, conducts assessments and assists in the establishment of CERTs for all of its members.[171] The Organisation of American States[172] and the EU Agency for Network and Information Security (ENISA)[173] also support their members in the establishment

---

[168] *ITU BDT Focal Point for Question 3/2* (n 139)
[169] These include cybersecurity strategies pertaining to the following States: Afghanistan, Austria, Brazil, Colombia, Cyprus, Czech Republic, Egypt, Finland, Georgia, Germany, Hungary, India, Ireland, Italy, Jordan, Lithuania, Luxembourg, Malaysia, Mauritius, Moldova, Montenegro, Morocco, Netherlands, New Zealand, Nigeria, Norway, Philippines, Poland, Qatar, Romania, Saudi Arabia, Singapore, Slovakia, Spain, Sweden, Switzerland, Uganda and United States.
[170] International Telecommunication Union, 'National CIRTs world-wide' <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf> accessed 7 January 2018
[171] International Telecommunication Union, 'CIRT Programme' <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx> accessed 7 January 2018
[172] OAS, 'Best Practices for Establishing a National CSIRT by the Organisation of American States' (2016) <https://www.thegfce.com/documents/publications/2016/04/01/best-practices-for-establishing-a-national-csirt> accessed 7 January 2018
[173] Henk Bronk, Marco Thorbruegge & Mehis Hakkaja, 'CSIRT Setting up Guide in English' (ENISA, 22 December 2006) <https://www.enisa.europa.eu/publications/csirt-setting-up-guide> accessed 7 January 2018

of CERTs, while the National Cyber Security Centre of the Netherlands offers a dedicated service aptly named CERT-in-a-box[174] and the Forum of Incident Response and Security Teams offers a medium for sharing best practices related to the operation and establishment of CERTs.[175]

Another technical capacity building international minimum standard associated with the due diligence obligations aimed at preventing the negative effects of acts with transboundary consequences is the 'installation and operation of early warning systems'.[176]

This certainly is a technically viable measure in the domain of cybersecurity. Even though early warning systems are traditionally operated by CERTs, this can be done also at the ISP level. A German ISP Deutsche Telekom, for example, checks all outgoing queries for IP spoofing, thereby blocking bogus data traffic, which could constitute (part of a) distributed denial of service (DDoS) flood or participation in another malicious act.[177] Extensive State practice corroborates the argument in favour of this minimum standard of capacity building. The US President's Commission on Critical Infrastructure Protection, for example, envisions a set of technical tools establishing the monitoring system which 'scan[s] the network in real-time to identify patterns of behaviour that were anomalous or abhorrent'[178] to the pre-established baseline level of a normal network operation, where anomalies imply the occurrence of a (outgoing or incoming) malicious cyber operation. In fact, in 35 national cybersecurity strategies States recognise the importance of such tools and proclaim a dedication to implementing a form of a warning system.

---

[174] NCSC-NL (National Cyber Security Centre of The Netherlands), 'CERT-in-a-box' <https://www.first.org/resources/guides/cert-in-a-box.zip> accessed 7 January 2018

[175] FIRST, 'FIRST Best Practice Guide Library (BPGL)' <https://www.first.org/resources/guides> accessed 7 January 2018

[176] *Draft Articles on the Protection of Persons in the Event of Disasters, with commentaries* (n 134) art 9

[177] Deutsche Telekom, 'Security on the Internet: Report on Information and Internet Security' (October 2013) 17

[178] Brian Fuller, 'Federal Intrusion Detection, Cyber Early Warning and the Federal Response' (SANS Institute InfoSec Reading Room, version 1.4b, 2013) <https://www.sans.org/reading-room/whitepapers/warfare/federal-intrusion-detection-cyber-early-warning-federal-response-1095> accessed 7 January 2018

In spite of this, a proposition that the establishment and operation of such systems indeed constitutes an international minimum standard remains problematic. Establishing an early warning system in the cyber domain involves either considerable technical expertise or an allocation of significant financial resources to acquire commercially available products. Considering the due diligence obligation only expects a State to act within its means, these factors certainly pose a limitation on the expected (and flexible) standard of behaviour.

3.1.3. Strategic and organisational measures

To achieve a comprehensive and inclusive cybersecurity commitment to due diligence, States need to adopt a broad strategic objective in the form of cybersecurity strategy, including a robust governance model. This model will create or designate the entities responsible for the nation's cybersecurity policy coordination and implementation. Unlike the previous two elements of a diligent approach to cybersecurity, the strategy with a governance model is a central element to the implementation of the cybersecurity commitment in a given State.

More than one third of all UN member States currently possess a document or series of them, taking form of a national cybersecurity strategy.[179] Whether this is enough to pronounce the possession of a cybersecurity strategy to be an international minimum standard of capacity building pertaining to the due diligence obligations in cyber context remains unanswered. On the one hand, the lack of a national cybersecurity strategy may not be interpreted as *de facto* proof of a government acting in bad faith or a definitive indication of its negligence since it can be substituted with the comprehensive legislation or a set of other polycentric policy mechanisms. After all, due diligence does impose best efforts, implying flexibility and discretion in observing the law. Nevertheless, it does hold true that without the strategy 'efforts in different sectors and industries become disparate and unconnected, thwarting efforts to

[179] ITU, 'National Strategies Repository' <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx> accessed 7 January 2018

reach national harmonisation in terms of cybersecurity capability development.'[180] Cybersecurity strategy is a vital harmonisation instrument in the facilitation of intra-agency, cross-sector and cross-border coordination, which is crucial in a complex and relatively new domain such as cybersecurity. It is for this reason that the Resolution 45 of the ITU's World Telecommunication Development Conference recognised 'the need for Member States to develop national cybersecurity programmes centred around a national plan'.[181] The existence of such national strategic plan indicates 'States are prepared to face serious risks, are aware of their consequences, and are equipped to appropriately respond to breaches in the network and information system' argued ENISA.

To support the global commitment to a secure cyberspace, a number of intergovernmental organisations offer assistance to governments in their efforts to draft, implement or evaluate their national cybersecurity strategies.[182] Incapacity or lack of resources is therefore unlikely to be accepted as a reason for a State to have no cybersecurity strategy.

3.1.4. Inclusive capacity building

While inclusive capacity building cannot be considered a minimum standard of conduct, such devotion would certainly point towards a wholesome commitment to cyber due diligence. Particular measures in this context include, *inter alia*, the creation of standardisation bodies,

---

[180] *ITU BDT Focal Point for Question 3/2* (n 139)

[181] ITU 'Resolution 45 (Rev. Dubai, 2014) – Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam' (The World Telecommunication Development Conference 2014) 2(d)

[182] *See eg* Global Cyber Security Capacity Centre (University of Oxford), 'Cybersecurity Capacity Maturity Model for Nations (CMM)' (revised edition, 31 March 2016); Commonwealth Telecommunications Organisation, 'Commonwealth Approach for Developing National Cyber Security Strategies' (Revised 2015); ENISA, 'An evaluation Framework for National Cyber Security Strategies' (November 2014); ENISA, 'National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace' (May 2012); Cristin Flynn Goodwin & Paul Nicholas, 'Developing a National Strategy for Cybersecurity – Foundations for Security, Growth, and Innovation' (Microsoft, October 2013); OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy' (2012); Alexander Klimburg (ed), 'National Cyber Security Framework Manual' (NATO CCD COE, 2012)

research and development programs, public awareness campaigns, and support for the domestic cybersecurity industry.[183]

The CoE, in the context of due diligence, does consider wider societal capacity building measures as part of the assortment of reasonable measures aimed at the prevention and termination of malicious cyber operations; States 'should also participate in the development and implementation of Internet user education and public awareness programmes, promotion and facilitation of dialogue with stakeholders as well as other appropriate measures'[184] argues the CoE report.

By all means, the aforementioned efforts are indicative of a general commitment to cybersecurity and widely recognised by various national cybersecurity strategies. The Australian national cybersecurity strategy, for example, recognised the importance of the awareness building measures in the effort to minimise the risk of cyber incidents; 'there is a reasonable expectation that governments and the private sector, including the Internet industry, will educate users and their customers on the risks and the steps they can take to minimise them.'[185] In like manner, Japan vowed to foster the 'efforts of cyberspace users, including individuals, enterprises, and organisations, to raise their cybersecurity awareness and literacy, and take cybersecurity measures voluntarily'.[186]

Two positive implications of the compliance with due diligence may be recognised. Firstly, awareness coupled with diligent cybersecurity measures, or sometimes called cyber hygiene,[187] of all stakeholders could hold potential to reduce the likelihood of an outgoing malicious cyber operation. To illustrate, diligent individuals, attentive in their cyber hygiene

---

[183] *ITU BDT Focal Point for Question 3/2* (n 139)
[184] *Council of Europe* (n 44) 17. The view has been endorsed by *Brunnée & Meshel* (n 58)
[185] Australia, 'Cyber Security Strategy' (2009) 10
[186] Government of Japan, 'Cybersecurity Strategy' (4 September 2015) 22
[187] Cyber hygiene encompasses teaching 'individuals and organisations basic prevention techniques to defend against low-level cyberattacks (which are the vast majority) and allow resources to focus on large attacks or develop national cybersecurity strategies.' OAS & IDB, 'Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report' (2016) 28

undertakings, are less vulnerable to assume the role of a zombie machine in an outgoing DDoS cyber operation. Secondly, State support of private sector research programs and domestic cybersecurity industry can indeed lead to the development of the technical capacity aiding the advancement of the State's cybersecurity commitment efforts.

Any positive effects of inclusive capacity building on the ability to prevent or to terminate a cyber operation are, however, far from guaranteed. Lessons from the 2007 DDoS attack on Estonia, for example, indicate botnets can be sourced from around the globe.[188] This indicates that the implication of cyber hygiene of individuals in a particular State is a very negligible contribution to the prevention of an outgoing DDoS attack. Also, considering the fact that a machine is a participant zombie in a botnet is usually not apparent to an end user, a similar argument can be made about the role of cyber hygiene in the efforts to terminate such cyber operation.

It is therefore submitted that, in their efforts to remain diligent in the observation of the duties to prevent and terminate, States *may* indeed wish to consider the inclusive capacity building measures but it certainly does not constitute a minimum standard of the obligations of prevention and termination.

3.1.5. (Inter)national cooperation

An international and intra-national cooperation in the context of the diligent prevention and termination of inter-State cyber operations is vital for a number of reasons. It is not only an implicit duty rooted in due diligence and the corresponding principle of good neighbourliness but also, due to the borderless nature of cyberspace, a prerequisite for successful prevention or termination of a transboundary cyber interference. The cooperation prescription is an

[188] *See eg* Jose Nazario, 'Politically Motivated Denial of Service Attacks' *in* Christian Czosseck & Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 163

established legal doctrine and has received wide recognition in various national cyber policies and international cyber agreements.

In essence, cooperation is indispensable for the satisfaction of the obligations of prevention and termination. The importance of international cooperation has been well documented; the Pulp Mills judgment stipulated that cooperation between nations is no less than 'necessary in order to fulfil the obligation of prevention'.[189] Other, more specific, international legal regimes stress the pivotal role of international cooperation in truly diligent prevention or termination of activities detriment to other States or the environment.[190]

Considering the fact that the Internet service and hosting providers as well as domain name registrars, central to the process of (a malicious inter-State) cyber operation, are often owned and operated by non-State actors, diligent governments should enact and employ measures enabling the communication, cooperation and assistance of all the national stakeholders which are vital to the performance of the diligent prevention and termination of the cyber operation. The Estonian experience from 2007 shows that communication and cooperation between all stakeholders is of vital importance.[191] As per the recommendation of ENISA, States should in their termination efforts 'encourage [ISPs] to quickly contact technical experts, incident response teams (like national CERTs), crisis coordination groups, and other organisations relevant in the response phase'.[192] Nigerian ISPs, for instance, are legally required to cooperate with enforcement and regulatory agencies, and must contact the

---

[189] *Pulp Mills on the River Uruguay* (n 8) para 102

[190] Prevention of transboundary harm 'require States to engage in cooperation.' (*ILC* (n 34) art 1 cmt 6). *See also* UNGA Res 69/283 (23 June 2015) UN Doc A/RES/69/283 III, para 19 (a); *UN Convention on the Law of the Sea* (n 119) art 145. See the discussion on the cooperation requirements by MWC Pinto, 'The duty of Co-Operation and the United Nations Convention on the Law of the Sea' *in* Adriaan Bos & Hugo Siblesz, *Realism in Law-Making: Essays on International Law in Honour of Willem Riphagen* (Martinus Njihoff 1986)

[191] *See eg* the methods employed by the Estonian government in 2007 DDoS attack elaborated by Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations* (CCD COE 2010) 24. Though Estonia was on the receiving end of the malicious cyber operation, the measures taken should be indicative of the possibilities a State has in the attempt to terminate the cyber operation. *See also* US Presidential Executive Order 13010 (15 July 1996) 'Critical Infrastructure Protection'

[192] ENISA, 'Cyber Incident Reporting in the EU – An overview of security articles in EU legislation' (August 2012) 9

Nigerian Communications Commission, 'in the event they become aware of any complaint or activity indicating Internet use for the commission of [a malicious cyber activity]'.[193] This is in addition to the obligation part of the Cybercrimes (Prohibition, Prevention, etc) Act, stipulating that that '[a]ny person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National [CERT] Coordination Center of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues.'[194] To facilitate cooperation in prevention, ISPs are required to 'provide contact details for the ISP representative(s) responsible for addressing cybercrime issues [which] must include one or more means of contacting the identified individual(s) outside of normal business hours.'[195]

The transboundary nature of cyber operations necessitates not only internal but also international cooperation. States shall cooperate to ensure 'international information security to maintain world peace and security'[196] and to prevent or repel a malicious cyber operation 'originating from their own territory or using the information infrastructure under their jurisdictions'[197] stipulates the Draft Convention on International Information Security, drafted by the Russian Federation and several other States. Moreover, the European Commission stated that 'building and maintaining robust alliances and partnerships with third countries is fundamental to the prevention and deterrence of cyber-attacks'.[198] Equally important seems to be the role of cooperation in the Shanghai Cooperation Organisation Agreement on the Cooperation in the Field of International Information Security obliging the parties to cooperate

---

[193] Nigerian Communications Commission, 'Guidelines for the Provision of Internet Service' (2007) art 6
[194] Cybercrimes (Prohibition, Prevention, etc) Act 2015 (Nigeria) art 21(2)
[195] *Nigerian Communications Commission* (n 193)
[196] Russian Federation, 'Convention on International Information Security' (draft, 22 September 2011) art 6 (2) <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666> accessed 7 January 2018
[197] ibid
[198] European Commission, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (13 September 2017) JOIN(2017) 450 final 18

in diligent protection of the critical cyber infrastructure of the parties to the Agreement.[199] States have also individually recognised the importance of the international cooperation as part of their strategic commitment to cyber security.[200] Relevant international legal scholarship has also argued in favour of cooperation being an essential element of diligent prevention and termination of the unlawful transboundary cyber operations.[201]

As to the level of cooperation States are expected to exhibit, Jensen claims that 'no specific standard for the level of cooperation is clearly agreed upon'.[202] While it may be true that no explicit agreements exist, conceptualisation of the due diligence found in other analogous international legal regimes provide guidance. For example, the Draft Articles on Prevention of Transboundary Harm, indicates that a cooperative State, diligent in its efforts to prevent an event holding the potential to negatively affect other States, would at least 'exchange in a timely manner all available information concerning the'[203] looming event. Applying this reasoning to cyberspace, sharing all the available information related to the known and potentially unlawful cyber operation in a timely manner is the least a diligent State can do to prevent or terminate a cyber operation. Particularly so because of the speed at which cyber operations occur.

The benefits of cooperation related to the maximisation of the potential to meet the prevention and termination duties are varied. It, for example, establishes a channel of inter-State communication, utilisation of which would be crucial in the attempt to satisfy the international standard of discharging the due diligence obligation of termination – providing a warning to

---

[199] Agreement Between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (unofficial translation, 16 June 2009) art 3 <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf> accessed 7 January 2018. Parties to the agreement are Kazakhstan, China, Kyrgyz Republic, Russian Federation, Tajikistan and Uzbekistan.

[200] *See eg* Kingdom of Saudi Arabia, 'Developing National Information Security Strategy for the Kingdom of Saudi Arabia' (2013) 65; United States of America, 'Cybersecurity Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure' (2009) 21

[201] Eg *Pirker* (n 73) 207; Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents' (2015) 48 Cornell Intl L J 481, 499

[202] *Jensen* (n 136) 298

[203] *ILC* (n 34) art 12

the targeted State(s). In addition to this, the indirect benefit of the cooperation comes in a form of 'threat information, attack scenarios and best practices in response, mitigations'[204] as well as the technology transfer,[205] which would allow a State to develop the other elements of performance capacity more easily.

3.2. Discharging due diligence obligations to prevent and to terminate

Of course, not only do States have the duty to develop capacity but also to utilise it in order to prevent or terminate the unlawful inter-State cyber operation, when the situation demands. For example, prevention efforts involve enforcing the national legislation to arrest the plotters, engaging a CERT to remedy the network infrastructure vulnerabilities and prevent their exploitation for the purpose of conducting an internationally wrongful cyber operation, engaging ISPs to pre-emptively isolate or disable the network connection of the source of the potential cyber operation, and taking advantage of the intelligence and capabilities of the international partners.

The requirement to diligently control the cyber infrastructure located in a domestic jurisdiction in order to comply with the due diligence obligation of prevention may indeed raise concerns over the abuse of the said obligation. Specifically, it is perhaps not unimaginable that a State could abuse the law and use it as a rationale for excessive control of the cyber infrastructure under its domestic jurisdiction. In the worst of the cases, a State could very well substitute national security concerns with the obligation of diligent prevention, using the principle and the stemming obligation as a justification to violate human rights of the people under its jurisdiction. A requirement to monitor cyber infrastructure on a specific territory could potentially be used as a rationale to violate, for example, human right to privacy or freedom of expression.[206]

---

[204] *ITU BDT Focal Point for Question 3/2* (n 139)
[205] *UN Convention on the Law of the Sea* (n 119) arts 266–278
[206] International Covenant on Civil and Political Rights (UNGA Res 2200A (XXI), 16 December 1966) [ICCPR] arts 17 & 19

While this is a reasonable concern, it is by no means an argument proposed by this thesis. Due diligence provides no universal right to derogation from the obligations part of the international human rights law and the interpretation of the international obligations stemming from the due diligence principle should be performed in good faith.

Nevertheless, there are exceptional circumstances in which a State may be permitted to temporary disregard its human rights law obligations in order to comply with the due diligence obligation of prevention. Generally, such derogations are conditioned by the state of necessity. In certain cases, primary obligations include provisions stipulating the necessity; freedom of expression, for example, may be subject to restrictions when national security is threatened.[207]

In cases where primary obligation offers no qualifications of necessity, one can resort to a more general guidance provided by the ILC's codification of the customary international law on State responsibility, stipulating that derogation is permitted in case of necessity or when a violation of the obligation 'is the only way for the State to safeguard an essential interest against a grave and imminent peril.'[208] This construction of the necessity is elaborated in the following paragraphs.

First, *the only way* means that the State seeking to violate human rights to fulfil its due diligence duties must first consider other means of compliance 'even if they may be more costly or less convenient'.[209] It must therefore first consider means of monitoring its territory in a way that is respectful of the human rights of its population. Being an obligation of conduct, due diligence obligation of prevention does not prescribe what specific measures should be taken by States. Whether a violation of human rights and freedoms was indispensable to comply with the obligation of prevention, will depend on specific circumstances and is question that is of more technical than legal nature.

---

[207] ibid art 19
[208] UNGA Res 56/83 'Responsibility of States for Internationally Wrongful Acts' (12 December 2001) UN Doc A/RES/56/83 (ARSIWA) art 25(1)(a)
[209] *ILC* (n 77) art 25 cmt 15

The fact that peril must be, *inter alia*, *imminent*, is not in contradiction of the due diligence obligation of prevention as it does not signal urgency or an immediate action. Imminence of peril can be assessed well ahead of materialisation of that peril, or in the context of this thesis, of injurious cyber operation. 'A "peril" appearing in the long term might be held to be "imminent" as soon as it is established, at the relevant point in time, that the realisation of that peril, however far off it might be, is not thereby any less certain and inevitable',[210] argued the ICJ.

Equally, the fact that peril about to ensue is of sufficient *gravity* to invoke necessity as a lawful ground for derogation depends on the reasonably expected consequences of the cyber operations resulting from the non-diligent behaviour; '[U]ncertainty about the future does not necessarily disqualify a State from invoking necessity, if the peril is clearly established on the basis of the evidence reasonably available at the time.'[211]

Similarly, what is essential interest 'depends on all the circumstances and cannot be prejudged'[212] by any theoretical stipulation. What should be noted, however, is that it is not only its own essential interest that the State can protect when choosing to disregard the international obligation rationalised by necessity. It can be also rights of other States; when considering the essential interest, States should consider 'interests of the entire community of States'[213] and not only its interests. In seeking compliance with the due diligence obligation of prevention, the necessity to temporary disregard human rights to privacy and freedom of expression can be invoked on the basis of a concern over an imminent grave peril threatening the essential interest of another State.

In the context of the international human rights law, 'it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of

---

[210] *Case Concerning Gabčíkovo-Nagymaros Project* (n 33) para 54
[211] *ILC* (n 77) cmt 16
[212] ibid cmt 15
[213] Roman Boed, 'State of Necessity as a Justification for Internationally Wrongful Conduct' (2000) 3(1) Yale Human Rights and Development J 1, 41

"necessity"'[214] as a legitimate reason to violate human rights in the name of compliance with the due diligence obligations of prevention. As a guidance, however, a violation of human rights in the name of mutual protection of international rights of other States, measures 'imposed in this sphere must be proportionate to the legitimate aim pursued',[215] argued the European Court of Human Rights in the Handyside v the United Kingdom case. This reasoning of the court is in line with State practice and other judgements of the aforementioned Court.[216]

After it has been established that a malicious inter-State cyber operation is indeed utilising an infrastructure under the jurisdiction of a particular State and that prevention efforts have failed, that particular State should **notify** the affected State(s) of the (potentially) damaging cyber operation, allowing the targets to immunise themselves or minimise the consequences. Notification constitutes a minimum international standard in the context of the obligation of prevention and the underlying principle of due diligence. An excerpt from the Corfu Channel substantiates this claim. After the automatic anchored mines damaged British warships, Albania incurred international responsibility for its omission 'to notify the existence of the said mines [and] failed to warn His Majesty's ships of the danger of the said mines',[217] a duty based on the customary due diligence obligation.[218] The requirement has been reiterated by the ILC in the context of the prevention of environmental transboundary harm; 'the State of origin shall notify without delay the States likely to be affected and shall transmit to them the available technical and other relevant information'.[219] The obligation of notification is well established in the international regimes regulating the State response in environmental emergencies[220] and

---

[214] *Handyside v the United Kingdom*, no. 5493/72 (7 December 1976) ECHR para 48
[215] ibid para 49
[216] Stephen J. Schulhofe, 'An international right to privacy? Be careful what you wish for' (2016) 14(1) Intl J of Constitutional L 238
[217] *Corfu Channel case* (n 7) 10
[218] ibid 22
[219] ILC, 'International liability for injurious consequences arising out of acts not prohibited by international law' (1996) II(1) Ybk of the ILC 36
[220] *See eg* ILC, 'The law of the non-navigational uses of international watercourses' (1994) II(2) Ybk of the ILC 129 art 28

has been applied to the domain of cyberspace by various scholars.[221] Several particularities of the requirement of notification ought to be noted. Should a cyber operation hold a potential to damage more than one State or there is an explicit danger of the uncontrollable propagation of the malicious code beyond the borders of one nation, the State of origin is to issue a general warning to all States.[222] It should be issued immediately, preferably prior to the termination efforts being taken. Principally, the warning and the subsequent communication is to be conducted in good faith; *inter alia* timely and in accordance with the State capacity.[223]

And when the cyber operation finally does occur, the State of origin must again utilise the previously developed capacities and attempt to diligently **terminate** the operation. While the elaboration of several technical measures to achieve this is beyond the scope of the present text, States should once again utilise the previously developed capacity and, for example, isolate or cut the connection between the servers used in the operation; in the event of a DDoS attack, filter the redundant data packets, break off the connection of zombie machines and review the user privileges;[224] or, in the event of espionage where phishing is usually the preferred method of penetrating the computer network system, prevent the perpetrators from using the dedicated Internet domain. If termination is not feasible, the State of origin must, in accordance with the due diligence principle, use all the previously developed capacity **to contain and mitigate** the incident and thus minimise its consequences.

---

[221] See eg *Brunnée & Meshel* (n 58); *Bannelier* (n 57) 37; *Gross* (n 201) 501–502; Scott J Shackelford, Scott Russell & Andreas Kuehn, 'Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector' (2016) 17(1) Chicago J of Intl L 1, 7–8; Christopher E Lentz, 'A State's Duty to Prevent and Respond to Cyberterrorist Acts' (2010) 10(2) Chicago J of Intl L 799, 806

[222] *Corfu Channel case* (n 7) (Dissenting opinion by Judge Badawi Pasha) 60

[223] 'States concerned shall exchange in a timely manner all information relevant to preventing or minimising the risk of causing significant transboundary harm' *ILC* (n 34) art 12

[224] GCHQ, 'Guidance 10 Steps: Summary' (16 January 2015) <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary#network-security> accessed 7 January 2018

4. Establishing State responsibility for non-diligent behaviour

State which fails to develop the minimum capacity or discharge it to prevent and terminate a cyber operation depriving the other nations of their legally protected international rights is internationally responsible for the violation of the due diligence obligations. This section explains that invoking State responsibility for the lack of diligence in prevention or termination efforts of the unlawful cyber operation is a more feasible endeavour as compared to invoking responsibility for the operation itself, which, as explained in the preceding chapter, is almost impossible in the given context.

To invoke international responsibility for the violation of due diligence obligations, an injured State must be ready to provide evidence substantiating claims of the jurisdiction of origin, the (constructive or actual) knowledge of the unlawful inter-State cyber operation, and the non-diligent attitude of the authorities in capacity building or discharging the obligations of prevention and termination. In the attempt to prove the alleged violation of due diligence, invoke State responsibility and employ countermeasures, injured States should, if they wish to avoid employing unlawful countermeasures or contributing to the erosion of the rule of law, adopt standards of proof accepted in international law. Only by doing so will they escape inherently subjective judgment and escape escalation of the conflict. For this very reason, the following discussion rests on the standards and acceptable methods of proof documented in the jurisprudence of the ICJ and the ICTY.

4.1. Evidence and proof of origin

Since States can only be responsible for failing to exhibit diligent behaviour in relation to their prevention and termination of operations emanating from their territories or infrastructure under their jurisdiction, the State wishing to employ countermeasures should be able to point a finger at the State of emanation.

As established in the preceding chapter, a standard of proof beyond reasonable doubt is not only overly demanding in the cyber realm but also disproportionate to the seriousness of the allegation[225] – be it the orchestration or toleration of the unlawful cyber operation. Instead, the sufficiently clear and convincing proof is the standard States are to attain when seeking to substantiate allegations of attribution as well as the involvement of a particular infrastructure (located on the specific territorial unit) in the malicious cyber operation. This is supported by the legal scholarship and State *opinio juris*.[226] International jurisprudence reinforces this reasoning; in the adjudication between the US and Iran, the former party presented the ICJ with evidence alleging that the HY-2 missile fired upon the Sea Isle City vessel 'was fired from Iranian-held territory in the Fao area'.[227] The evidence, however, did not amount to 'sufficiently clear'[228] proof and was thus unable to substantiate the conclusion the missile was fired *by* or *from* Iran. The application of the doctrine leads to a single deduction – the allegations that the unlawful cyber operation indeed originated from a particular territory have to be supported by a sufficiently clear and convincing proof.

Undoubtedly, the various methods of establishing the origin of the cyber operation presented in the previous chapter hold the potential to provide such proof. Nevertheless, they remain plagued with unreliability. Once again, socio-political methods are unconvincing and cannot amount to the sufficiently clear and convincing standard, which should be self-imposed by the injured State attempting to invoke State responsibility should it wish to avoid escalation of the conflict. Conversely, while often incapable of pointing at the specific orchestrator or a natural person, computer science does offer a variety of methods with the potential to identify (the location of) the computerised devices utilised in a particular cyber operation. IP traceback remains the main technique in this endeavour[229] although it can sometimes retain an unreliable

---

[225] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 53) para 210
[226] *See* ch 4, section 4.3.2
[227] *Oil Platforms (Islamic Republic of Iran v. United States of America)* [2003] ICJ Rep para 58
[228] ibid 57–58
[229] *See eg* Akamai Technologies, 'Akamai's [state of the Internet] / security: Q2 2016 report' (2016) 28–29 <http://goo.gl/IRp675> accessed 7 January 2018

nature as it is subject to heavy computational load for path reconstruction and likelihood of false positives.[230] This is particularly true in the case of a DDoS attack.[231] Other computer science methods are also available. One of particular interest is the tracking of the Autonomous system number (ASN); it leads researchers to the specific network or ISP and therefore the country of origin,[232] it can be a robust substitute to IP traceback. Both methods previously proved the origin of various inter-State cyber operations, but they failed to establish the identities of specific culprits or the attribution to the State authorities. Based on the IP address, South Korea's Communications Commission found that the 2013 operations targeting various Korean networks originated in China.[233] The same State was found to be the origin of the widespread cyber espionage efforts.[234] In another case, a particular Chinese ASN was identified as a source of espionage against Mongolian governmental systems[235] and other malicious cyber operations.[236]

As indicated in the previous paragraph, evidence pointing to the State of origin, comes in different forms though direct technical proof may hold the highest potential to achieve the sufficiently clear and convincing standard of proof. It may certainly not need to come in a physical form, as required by the ICJ in the Oil Platforms case when trying to determine the origin of the unlawful act.[237] Firstly, physical evidence will probably not be available in the cyber domain. Secondly, and as it has been already established, digital evidence has indeed

---

[230] *See eg* Zhiqiang Gao & N Ansari, 'Tracing cyber attacks from the practical perspective' (2005) 43(5) IEEE Communications Magazine 123, 123

[231] Vamsi Paruchuri et al, 'Authenticated Autonomous System Traceback' (2004) Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)

[232] ibid

[233] 'China IP address link to South Korea cyber-attack' *BBC* (21 March 2013) <http://www.bbc.com/news/world-asia-21873017> accessed 7 January 2018

[234] Mandiant, 'APT1 – Exposing One of China's Cyber Espionage Units' (2013) 7 <http://goo.gl/H3IkzR> accessed 7 January 2018

[235] The ThreatConnect Research Team, 'Khaan Quest: Chinese Cyber Espionage Targeting Mongolia' (*ThreatConnect*, 7 October 2013) <https://www.threatconnect.com/khaan-quest-chinese-cyber-espionage-targeting-mongolia/> accessed 7 January 2018

[236] The ThreatConnect Research Team, 'Divide and Conquer: Unmasking China's 'Quarian' Campaigns Through Community' (*ThreatConnect*, 11 November 2013) <https://www.threatconnect.com/blog/divide-and-conquer/> accessed 7 January 2018

[237] *Oil Platforms* (n 227) para 58

been a permitted form of evidence in international adjudication.[238] Lastly, the Court in the Oil Platforms case seems to have used the aforementioned restrictive terminology in order to distinguish and indicate the insufficient and unreliable character of the witness statement.[239]

4.2. Evidence and proof of knowledge

As previously established, the injured party in the conflict should be able to establish the allegedly negligent State was or should have been aware of the unlawful cyber operation. This can be achieved through the establishment of actual or constructive knowledge.

The doctrinal standard of proof in the case of proving knowledge is less clear – the evidence may be circumstantial but should amount to 'sufficient'[240] proof or 'lead to a single conclusion'[241] or 'leave no room for reasonable doubt',[242] the ICJ argued somewhat puzzlingly in the case of Corfu channel. Once again and for the well-documented reasons, this thesis argues in favour of the standard lower than beyond reasonable doubt.

The ICJ took a more liberal position in the Tehran hostages case, where the evidence had amounted to proof which would satisfy the Court that the submissions were well founded.[243] Two things had been established to the 'satisfaction of the Court'[244] – historically, vigilance in monitoring the security situation around the US Embassy in Tehran and success in preventing and terminating similar attacks on the said diplomatic premises[245] pointed at the fact that Iran should have known of the risk of the raid in question; direct evidence in a form of the records of repeated official calls for help[246] as well as public statements of endorsement by Ayatollah

---

[238] *Prosecutor v Naser Orić* (Trial judgment) [2006] ICTY IT-03-68-T (30 June 2006) para 31
[239] *Oil Platforms* (n 227) para 58
[240] *Corfu Channel case* (n 7) 16
[241] ibid 18
[242] ibid
[243] *United States Diplomatic and Consular Staff in Tehran* (n 36) para 11 & 13
[244] ibid para 63
[245] ibid para 64–65
[246] 'During the three hours or more of the assault, repeated calls for help were made from the Embassy to the Iranian Foreign Ministry.' ibid para 18

Khomeini and the Foreign Minister of Iran[247] proved the State had actual knowledge of the aforementioned events in violation to the international diplomatic law.

Much like the Iranian authorities should have known of the imminent danger of the attack, the Serbian regime should have known of the danger of the genocide in Srebrenica being committed. While requiring a proof of high certainty for the attribution,[248] the employed standard of proof substantiating the knowledge was however most lenient. The Genocide case judgment recognised the fact that there was no evidence pointing that Milosevic or the Serbian authorities knew of the perpetrators' decision to conduct the massacre in Srebrenica.[249] Nevertheless, the Court argued actual knowledge (or certainty) is not the precondition for the international responsibility to arise; 'it is enough that the State was aware, or should normally have been aware, of the serious danger'[250] of the genocide.

In fact, it would appear that the ICJ employed the permissive standard of balance of probabilities – in the attempt to prove the fact that the Serbian regime was indeed aware of the prospects of genocide, the Court took into consideration two statements; General Clark stated before the ICTY that a conversation with Milosevic 'indicated that [the latter] had foreknowledge of'[251] the potential genocide while the recollection[252] of the then EU envoy to Yugoslavia Carl Bildt, urging Milosevic to allow access to United Nations High Commissioner for Refugees and International Committee of the Red Cross to Srebrenica, 'clearly [suggested]'[253] that an awareness of the serious danger of genocide existed. Considering this conclusion, in spite of the fact that Milosevic contradicted[254] the statement of General Clark, it is safe to deduce that the ICJ evaluated the proof on the basis of balance of probabilities; the

---

[247] ibid para 68–73
[248] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 53) para 210
[249] ibid
[250] ibid para 436
[251] ibid para 437
[252] UNGA 'Report of the Secretary-General Pursuant to General Assembly Resolution 53/35 – The Fall of Srebrenica' (15 November 1999) UN Doc A/54/549
[253] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 53) para 436
[254] ibid para 437

evidence amounted to a proof providing that it is 'more likely than not'[255] that the Serbian authorities knew of the imminence of the Genocide.

This thesis has already argued in favour of the standard demanding a sufficiently clear and convincing standard of proof and it continues to do so. The reasons for this have been well-documented in the preceding chapter – to avoid the escalation of the conflict, balance of probabilities is not an appropriate standard of proof while the standard beyond reasonable doubt is too demanding considering the alleged unlawful act.

The fact that Russia was aware of the (imminent) DDoS attack on Estonia cannot be confirmed with a sufficiently clear and convincing proof. Doubtful factuality of the self-proclaimed responsibility of State Duma Deputy assistant Goloskokov,[256] recorded no less than two years after the incident,[257] does not amount to the standard of the clear and convincing proof. Similar can be claimed of the vague statements by the State Duma Deputy Markov, who (also two years after the fact) acknowledged the attack was conducted by his assistant.[258] Although certainly indicative of the possibility that the Russian authorities knew of the malicious operation in March 2007, this statement does not constitute a sufficiently clear and convincing proof.

But should have it known of the operation or the danger of it? The circumstantial evidence, in the form of public knowledge consequential to the 'extensive coverage in the world press'[259] indeed points to the fact that Russian authorities should have been aware of the undergoing cyber operation. When evidence is out of reach or located in the foreign territory, circumstantial evidence (of public knowledge) may be used to substantiate the allegations of the constructive

---

[255] *R v Swaysland* [1987] BTLC 299, 308. See similar assertions made by Denning in *Miller v Minister of Pensions* [1947] 2 AII ER 374
[256] *Tikk, Kaska & Vihul* (n 191) 24
[257] Charles Clover, 'Kremlin-backed group behind Estonia cyber blitz' *Financial Times* (11 March 2009) <ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?ft_site=falcon&desktop=true> accessed 5 May 2017
[258] Robert Coalson, 'Behind the Estonia Cyberattacks' *Radio Free Europe/Radio Liberty* (6 March 2009) <http://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html> accessed 5 May 2017
[259] *United States Diplomatic and Consular Staff in Tehran* (n 36)

knowledge, as previously indicated by the ICJ Tehran Hostages[260] and the Corfu channel judgments. Since evidence pertinent to a cyber operation may be scattered around the world, located on different servers in several territories, this is of special interest in the present investigation.

An affirmative answer providing a clear and convincing proof also follows the test employed in the Corfu channel case. The Federal Security Service of the Russian Federation Information Security Center is normally vigilant in monitoring Russian Internet networks 'using hardware and software installed at Russian [ISPs], Internet access points, and Internet exchanges'[261] just like Albania has historically kept a close eye on the Corfu naval passage. This must be particularly true for the State networks, from which the 2007 DDoS partially originated. Same holds true for any modern State, such as members of the Five Eyes[262] alliance. Said Russian cyber capacities are also indicative of the possibility for the authorities to spot the network anomalies pointing at the outgoing 2007 DDoS attack which 'involved large botnets with Russian based command and control nodes';[263] to construct a sufficiently clear and convincing proof, the affirmation of this theoretical possibility should be corroborated by the assessment of IT experts. Similarly, technical evidence of the Chinese extensive monitoring activities[264] of their networks and the enabling infrastructure provides a sufficiently clear and convincing proof of ordinary vigilance. Should the States whose networks were penetrated by the infamous

---

[260] ibid para 11–13

[261] TAIA, 'Russian Federal Security Service (FSB) Internet Operations Against Ukraine' (TAIA Global Report, 2015) 4–5 <https://goo.gl/PMDY58> accessed 1 April 2016. See also Vitaly Petlevoï, 'Russian authorities step up cybersecurity' *Russia Beyond* (27 January 2013) <http://rbth.com/politics/2013/01/26/russian_authorities_step_up_cybersecurity_22229.html> accessed 8 January 2017

[262] Carly Nyst & Anna Crowe, 'Unmasking the Five Eyes' global surveillance practices' in Alan Finlay (ed), *Global Information Society Watch 2014* (Global Information Society Watch 2014) <http://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices> accessed 11 January 2018

[263] Bryan Harris, Eli Konikoff & Phillip Petersen, 'Breaking the DDoS Attack Chain' (CMU-ISR-MITS-2, Institute for Software Research, Carnegie Mellon University 2013) 2

[264] For an overview of Chinese cyber monitoring activities *see eg* Mark Stokes, Jenny Lin & LC Russell Hsiao, 'The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure' (The Project 2049 Institute, 11 November 2011) <https://goo.gl/LuWhZN> accessed 1 April 2016; Peter Mattis, 'The Analytic Challenge of Understanding Chinese Intelligence Services' (2012) 56(3) Studies in Intelligence 47

ATP1 group be able to clearly demonstrate that Chinese capabilities were indeed sufficient for the theoretical detection of such an outgoing cyber operation, a sufficiently clear and convincing proof may be established.

4.3. Evidence and proof of the lack of diligence

Finally, the injured State needs to be able to prove that the allegedly perpetrating State failed to observe the due diligence principle in its attempt to prevent or terminate the unlawful cyber operation against another State. As established beforehand, this imposes a duty of diligent development of performance capacity as well as the utilisation of it or termination of the cyber operation.

In its endeavour to establish State responsibility, the injured party should be able to prove the alleged perpetrator failed to attain the minimum international standard pertaining to the due diligence obligations. Namely, it should be in possession of a clear and convincing proof demonstrating the fact that the allegedly perpetrating State failed to enact, implement and enforce the appropriate legislation, failed to establish CERT and draft a comprehensive national cybersecurity strategy, share information regarding the incident or warn of the cyber threat.

Russia has indeed enacted the appropriate cybersecurity legislation, established national CERT and drafted several strategic documents forming a national cybersecurity strategy.[265] Be that as it may, there is no public information indicating that the Russian authorities warned Estonia of the DDoS attack or that they offered help in mitigation. Instead, implicit endorsements were voiced – 'something bad had to be done to these fascists'[266] said State Duma Deputy Markov. What is more, in the time of the attack, Russian authorities and CERT

[265] *ITU* (n 142)
[266] *Coalson* (n 258)

proved to be reluctant to offer any kind of assistance although they were asked for one, argued Estonian diplomats.[267] Thus, Russia has failed to observe the due diligence standard.

In an effort to prove the negligent behaviour of the State, an injured party can rely on public information. Numerous repositories of international organisations keep track of the status of national cybersecurity strategies,[268] some of them rely on the data supplied by the States themselves.[269] Similar can be said about the status of the national cybersecurity legislation[270] and existence of national CERTs.[271]

5. Conclusion

This chapter has demonstrated the utility of the due diligence doctrine in response to the questionable feasibility of the attribution and, subsequently, establishment of State responsibility for the unlawful inter-State cyber operations, exposed in the preceding chapter.

I have elaborated the content and the flexible standard of due diligence in international law and provided evidence in support of the applicability of the doctrine in cyberspace; there is no denial that States have the due diligence obligations to prevent and terminate the internationally wrongful cyber operations emanating from their territories.

This includes not only discharging the obligations but also the development of the capacity performance. In brief, the chapter argues that States are under the obligation to do all in their power to, firstly, develop the capacity of performance and, secondly, utilise this capacity to prevent or terminate an unlawful cyber operation performed by any actor under their

---

[267] Gregg Keizer, 'Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable' *Computer World* (9 December 2010) <http://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html> accessed 8 January 2018

[268] *See eg* CCD COE, 'Cyber Security Strategy Documents' <https://ccdcoe.org/strategies-policies.html> accessed 8 January 2018

[269] *See eg* International Telecommunication Union, 'National Strategies Repository' <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx> accessed 8 January 2018

[270] See eg *United Nations Office on Drugs and Crime* (n 149)

[271] *See eg* Carnegie Mellon University, 'List of National CSIRTs' <https://www.cert.org/incident-management/national-csirts/national-csirts.cfm> accessed 8 January 2018

jurisdiction. This involves at least the development and enforcement of sufficient contemporary cybersecurity legislation, establishment of CERTs, adoption of the national cybersecurity strategy and cooperative information exchange when a malicious event materialises. An inclusive participation capacity building is optional but certainly an indication of diligence.

In the final section of the chapter I examined the principle of due diligence in the context of State responsibility and concluded that the injured parties wishing to employ countermeasures must be able to clearly and convincingly prove, first, the territorial or jurisdictional origin of the cyber operation, second, that the State of emanation knew or ought to have known of the illicit use of the infrastructure under its jurisdiction and, finally, that the allegedly responsible State was non-diligent in its prevention or termination efforts.

Since all of the aforementioned tasks are attainable – something that cannot be claimed for the tasks required for the invocation of State responsibility on the grounds of agency – I proceed to elucidate how the injured State is to employ countermeasures, enforce the current and future performance of the law and thus restore the power and security.

Chapter 6

Countermeasures, the non-diligent State and inducing compliance with international law in cyberspace

1. Introduction

Not only does international law prohibit the commission of cyber operations in violation of the rights of other States, it also dictates the diligent prevention and termination of such operations emanating from one's territorial jurisdiction. From a factual perspective, a State responsible for the former is also responsible for the latter.

This is not the case from the legal perspective; a combination of technological limitations and stringent legal standards of attribution prevent the injured State from invoking legal responsibility for the wrongful cyber operation and inducing compliance by way of countermeasures. It can, however, invoke legal responsibility for the violation of the due diligence obligations of prevention and termination.

Generally, a failure to exhibit due diligence in prevention and termination efforts will result in international responsibility for the omission of diligence but not necessarily for the act resulting from this omission.[1] Consequently, and in accordance with the law of the State responsibility, the non-diligent State is under obligation to cease the unlawful act, and thus do its utmost to terminate the cyber operation injurious to the legal rights of the other State. In accordance with the international law of State responsibility, it must also provide guarantees or assurances of non-repetition, namely of its future diligent efforts in prevention and termination of unlawful cyber operations stemming from their territory. Thirdly, the responsible State is under the

[1] Barbara Frey, 'Prevention of human rights violations committed with small arms and light weapons' (25 June 2003) UN Doc E/CN.4/Sub.2/2003/29, 42

obligation to provide reparations for the injury caused to the State deprived of its international rights by the absence of due diligence and the resulting events.

In light of the persisting positive cost benefit calculous of the non-compliance, it is highly unlikely the responsible State will indeed comply with the aforementioned legal obligations. This has been already established in the third chapter. The injured State is therefore entitled to employ countermeasures, by doing so to effectuate the obligation of reparations and so alter the cost benefit calculation of the non-complying party, rendering the current and potential future violation irrational.

This chapter explains who can take countermeasures against whom, and when and how to effectively and lawfully induce compliance with the due diligence obligations. It also elaborates that the quantitatively proportional countermeasures effectuating reparations arising from the responsibility for the omission of a diligent conduct indeed change the calculation of the State *in fact* responsible for the cyber operation and thus deter it from violating international law with cyber means in the future.

2. Who can take countermeasures against whom?

2.1. Who can take countermeasures?

Under international law, only States have the legal capacity to employ countermeasures. This does not mean that every State has the right to give effect to this capacity; generally speaking, it is a State affected by the breach of international obligations that can take countermeasures, although in exceptional circumstances,[2] countermeasures may also be employed by a non-injured State.

Only States can take countermeasures against the foreign powers 'for the State is like a screen between [non-State actors] and the international legal order.'[3] According to the ICJ's

[2] For example, in case of violation of the *erga omnes* international obligations.
[3] Elizabeth Zoller, *Peacetime Unilateral Remedies* (Transnational Publishers 1984) 103–104

argumentation advanced in the Barcelona Traction case, whether the claims under the law of State responsibility 'are made on behalf of a [non-State actor] or on behalf of the State itself, they are always the claims of the State'.[4]

Nevertheless, the reality is that non-State actors play a prominent role in cyberspace and it is not uncommon for a non-State actor, initially targeted by the unlawful cyber operation for which the State is responsible for, to react and hack back.[5] The cyber operation aimed at Google in 2009 is one example of a State pointing its cyber arsenal at a non-State actor. Even though the search giant had taken it upon itself to coerce the Chinese government cyber operatives to cease the operations against its computer network infrastructure located on American territory,[6] such measures of actors not associated with the concept of international legal personality are not countermeasures as part of the international law of State responsibility.

Principally, countermeasures may only be employed by an injured State. This is well-established by the State practice, doctrine and jurisprudence[7] and clearly expressed in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA).[8] In the words of the ILC in a commentary to the ARSIWA, countermeasures are 'a feature of a decentralised system by which injured States may seek to vindicate their rights and to restore the legal relationship with the responsible State which has been ruptured by the internationally wrongful act'.[9]

---

[4] *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain)* [1964] ICJ Rep 46–47

[5] According to the relevant literature, the term *hack back* denotes a reactive cyber operation of a non-State actor countering a disruptive cyber act for which a State is responsible for. *See eg* Jan Messerschmidt, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' (2013) 52(1) Columbia J of Transnational L 275; Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Rule 4 para 2

[6] David E Sanger & John Markoff, 'After Google's Stand on China, U.S. Treads Lightly' *New York Times* (14 January 2010) <http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology> accessed 13 August 2019

[7] Omer Yousif Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Clarendon Press 1988) 47

[8] UNGA Res 56/83 'Responsibility of States for Internationally Wrongful Acts' (12 December 2001) UN Doc A/RES/56/83 (ARSIWA) arts 42, 49(1), 52(1)

[9] ILC, 'Materials on the Responsibility of States for Internationally Wrongful Acts' (UN Legislative Series, 2012) UN Doc ST/LEG/SER B/25, 304 para 1

On the surface, the concept of an injured State is rather straightforward – '[a] State whose individual right has been denied or impaired by the internationally wrongful act or which has otherwise been particularly affected by that act'[10] is considered to be the injured State. In the context of this thesis, States deprived of their rights to diligent protection are therefore considered to be injured and legally empowered to employ countermeasures.

However, due to the fact that the occurrence of events in contravention to the international rights of a State is 'the sine qua non condition for the existence of the breach of the obligation [of prevention and termination]',[11] countermeasures against the non-diligent State can only be employed by a State injured by the wrongful cyber operation resulting from the breach of due diligence obligations. In other words, a State is considered to be injured by the denial of its rights to diligent protection only when it has also sustained an injury from the resulting unlawful act.

To identify the State injured by the resulting wrongful cyber operation one needs to, firstly, establish which legal obligations a cyber operation violated and, secondly, to whom the legal obligations are owed. The specific unlawful character of the Shamoon, 2007 DDoS and RedOctober operations have already been elaborated in the first chapter of the thesis. What remains is to determine which State's rights were violated in the course of the cyber incidents.

States may be deprived of their rights by a cyber operation directly or indirectly. An example of a directly injured State is the DDoS operation in 2007 which targeted, *inter alia*, the governmental computer systems of Estonia[12] constituting an unlawful intervention aimed against its political independence. Since the primary targets in this case were actual organs

---

[10] ibid 272 para 2

[11] Jean Salmon, 'Duration of the Breach' *in* James Crawford, Alain Pellet & Simon Olleson, *The Law of International Responsibility* (OUP 2010) 390

[12] Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations* (CCD COE 2010) 21. *See also* ch 1

of the State, it was Estonia that was an injured State, and thus legally empowered to take countermeasures against the State responsible for the violation.

A similar conclusion can be drawn in relation to the RedOctober cyber operation that was in violation of the provisions of the international diplomatic law, which designates the sending of States' diplomatic communication and archives, irrespective of their location, to be inviolable.[13] Every State whose diplomatic archives were compromised during the RedOctober operation is considered an injured State and therefore entitled to take countermeasures against the internationally responsible party.

A malicious cyber operation can also injure a State indirectly. In fact, the reality is that rational States in pursuit of a quick inflation of their relative power will often direct their offensive cyber capacity against a non-State actor. Considering that various private entities are vital to the power and security of a modern State, it is rather unsurprising that they may be attractive targets of the unlawful power maximisation misdeeds of the rational States. Even when State organs are not directly targeted, the cyber operation may culminate in denial of the international rights of a State. Disrupting the operation of a critical national infrastructure[14] owned and operated by a non-State actor, may serve as an example.

To illustrate, I turn again to the 2007 DDoS operation against Estonia, which targeted not only the web services of the State but also important financial institutions, which, by legal standards, do not fit the concept of a State but of a non-State actor. Nonetheless, as established in the first chapter, the aim of the operation was coercive interference with a matter

---

[13] Vienna Convention on Diplomatic Relations (18 April 1961) 500 UNTS 95 art 24; *see also* ILC, 'Second report on the status of the diplomatic courier and the diplomatic bag not accompanied by diplomatic courier, by Mr. Alexander Yankov, Special Rapporteur' (1981) II(1) Ybk of the ILC UN Doc A/CN.4/347 and Corr.1 & 2 and Add.1 & 2, 164

[14] Critical infrastructure in the UK, for example, includes the following sectors: Chemicals, Civil Nuclear Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Centre for the Protection of National Infrastructure, 'Critical National Infrastructure' <https://www.cpni.gov.uk/critical-national-infrastructure-0> accessed 13 August 2019

in exclusive domain of Estonia. Estonia is thus entitled to take countermeasures against the State internationally responsible for the violation of the principle of non-intervention.

Yet another example of an indirect injury to a State by a cyber operation primarily targeting a non-State actor can be identified in the doings of the Shamoon malware. Despite the fact that the target of the malicious cyber operation was not the State itself, its internationally wrongful character lies in the fact that it constituted unauthorised access to the Saudi cyber infrastructure, which amounted to a violation of its sovereignty.[15] Saudi Arabia, whose international sovereign rights were violated during said cyber operation, is therefore considered to be the injured State.

An unlawful cyber operation may result in more than one injured State. In such case, 'each injured State may separately invoke the responsibility of the State which has committed the internationally wrongful act'[16] and take countermeasures to restore the material and legal relationships between the States, therefore rendering the violation irrational and thus inducing compliance. Due to automated propagation techniques and the low cost of scalability, the potential of such an event in cyberspace is significant.

As a matter of fact, a single cyber operation employing the RedOctober malware breached the inviolability of the diplomatic correspondence and archives of no less than 43 States.[17] Each State, which experienced the violation of its right to confidentiality of diplomatic documentation is considered to be an injured State and legally entitled to take countermeasures against the party internationally responsible for the unlawful deed.

Yet another and a more recent example of a single cyber operation infringing on the international rights of a multitude of States is the havoc wreaked by the WannaCry malware.

---

[15] *See* ch 1; *Schmitt* (n 5) 21: 'the Shamoon virus that required repair or replacement of thousands of Saudi Arabia's oil company Saudi Aramco's hard drives in 2012 qualified as a violation of that State's sovereignty.'
[16] *ARSIWA* (n 8) art 46
[17] Global Research & Analysis Team, '"Red October" Diplomatic Cyber Attacks Investigation' (Kaspersky Lab, 14 January 2013) <securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/> accessed 13 August 2019

The cyber operation, which affected the network systems of 150[18] States, including the British National Health Service,[19] Iranian hospitals,[20] systems of the Russian Interior Ministry[21] and the Indian law enforcement entities,[22] constituted a violation of the principle of sovereignty and thus injured the legal rights of several States.[23] As it stems from the law of State responsibility, each of them can invoke State responsibility and consider taking countermeasures against the responsible State.

Opinio juris indicates that solidarity with allies is a legitimate foundation for lawful countermeasures taken by States whose legal rights were not affected by the unlawful cyber operation. Most recently, the President of Estonia argued

> States which are not directly injured may apply countermeasures to support the State directly affected by the malicious cyber operation. […] The threats to the security of States increasingly involve unlawful cyber operations. It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace.[24]

In the context of anarchical international relations, this is a reasonable proposition of an egoistic State interested in its individual security and self-preservation rather than an objective appeal to promote the rule of law and general compliance with international law. Due to doubts in its own capacity to alter the rational choice calculation of the States diminishing the national

---

[18] Michael Schmitt & Sean Fahey, 'WannaCry and the International Law of Cyberspace' (22 December 2017)
[19] UK National Audit Office, 'Investigation: WannaCry cyber attack and the NHS' HC 414 Session 2017–2019 (27 October 2017) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf> accessed 13 August 2019
[20] '"WannaCry" Cyberattack Targets Iran Hospitals' *Financial Tribune* (14 May 2017) <https://financialtribune.com/articles/sci-tech/64402/wannacry-cyberattack-targets-iran-hospitals> accessed 13 August 2019
[21] Andrew E Kramer, 'Russia, This Time the Victim of a Cyberattack, Voices Outrage' *New York Times* (14 May 2017) https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html> accessed 13 August 2019
[22] 'WannaLaugh: Faced with WannaCry attack, AP cops unplug systems and save data' *New Indian Express* (13 May 2017) <http://www.newindianexpress.com/states/andhra-pradesh/2017/may/13/wannalaugh-faced-with-wannacry-attack-ap-cops-unplug-systems-and-save-data-1604416.html> accessed 13 August 2019
[23] *Schmitt & Fahey* (n 18)
[24] Kersti Kaljulaid, 'President of the Republic at the opening of CyCon 2019' (Office of the President of Estonia, 29 May 2019) <president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019> accessed 13 August 2019

security of Estonia by way of cyber operations, the President sought to establish legal foundation for countermeasures taken by a concert of allied States, which are presumably more likely to successfully restore the power balance disturbed by a wrongdoing cyber power.

Limited State practice in support of the legality of collective countermeasures does exist.[25] An example of third-party countermeasures in the context of this thesis are the ones taken by several States other than the US after Iran refused to prevent and terminate the internationally wrongful detention of US diplomats in Tehran. After the vetoed UN SC resolution[26] calling for sanctions against Iran, the EEC, Japan and the UK[27] took matters into their own hands.[28] The UK, for instance, decided to proceed with countermeasures against Iran for three distinct reasons – to peacefully compel Iran to comply with international law and thus discourage the US from escalating the conflict by military means,[29] to act in solidarity with their ally,[30] and most importantly, to protect the status of the *erga omnes* obligations of international diplomatic law. Referring to the international community at large, British foreign minister Douglas Hurd argued in the House of Commons, '[t]his is not just a quarrel between the US and Iran in which the rest of us are essentially spectators. What has happened in Tehran has been […] an affront to a part of international law in which all our interests are involved'.[31]

However, from a legal standpoint this non-discriminatory approach to who can take countermeasures against the internationally responsible State is problematic; the aforementioned State practice is embryonic and the existing customary law of State

---

[25] Several examples listed in *ILC* (n 9) art 54 cmt 3; ILC, 'Fourth report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur' (1992) ILC Ybk II(1) UN Doc A/CN.4/444 and Add.1–3, para 38. *See also* Jochen A Frowein, 'Obligations *erga omnes'* in *Max Planck Encyclopedia of Public International Law* (December 2008) paras 12 & 13

[26] UNSC Verbatim Record (11 & 13 January 1980) UN Doc S/PV.2191 para 149

[27] Iran (Trading Sanctions) Order 1980 (29 May 1980) 737 Statutory Instruments 2585; Export of Goods (Control) (Iran Sanctions) Order 1980 (29 May 1980) 735 Statutory Instruments 2579

[28] Russian representative at the UN General Assembly meeting complained: 'This is a clear lack of respect for the Charter of the United Nations and *an attempt to take the law into one's own hands*, and it should be resolutely condemned by all Member States.' [emphasis added] *UNSC Verbatim Record* (n 26) para 168

[29] L. R. Fletcher arguing the British reaction will have a 'restraining influence upon the military proclivities of our major ally in the Western Alliance.' HC Deb 12 May 1980 vol 984 c959

[30] '[To sustain] the good health of the Alliance on which our national security depends to a large extent.' ibid c963

[31] ibid c913

responsibility as codified by the ARSIWA Article 49 does not permit countermeasures by a State, the international legal rights of which were not injured by a cyber operation. States, such as France, have also spoken against the legality of the countermeasures taken by the States not legally injured by the internationally wrongful cyber operation.[32]

What States other than the directly injured ones can do is invoke responsibility and take *lawful* measures, such as retorsion, when the violated rights in question are owed either to a group of States which it is a member of or of the legal obligation owed to the international community as a whole.[33] States can therefore invoke responsibility 'not in its individual capacity by reason of having suffered injury'[34] but in the interest of preservation of the rule of international law. Accordingly, if a cyber operation was to violate obligations of *erga omnes status*, that is, the obligations owed 'towards the international community as a whole',[35] any of the members of the international community may be considered to have a legal interest in the survival of the specific rule and empowered to take invoke State responsibility.[36] 'Acts of aggression, and of genocide, [violations of] the principles and rules concerning the basic rights of the human person, including protection from slavery and racial discrimination'[37] as well as the right of self-determination[38] are all considered to be *erga omnes* obligations.

Since the 2007 DDoS operation against Estonia violated its sovereignty but did not constitute a breach of *erga omnes* obligations, under the existing international law, Estonia is the only State allowed to invoke State responsibility and take countermeasures. In the same vain, it should not be claimed that any State with legal interest could invoke State responsibility of the internationally responsible party for the RedOctober cyber operation in violation of the provision of the diplomatic law. While the protection of diplomatic personnel may constitute

---

[32] Michael Schmitt, 'France's Statement on International Law and Cyber: An Assessment' (*Just Security*, 16 September 2019)
[33] *ARSIWA* (n 8) art 48
[34] *ILC* (n 9) art 48 cmt 1
[35] *Barcelona Traction, Light and Power Company, Limited* (n 4) 32 para 33
[36] *ARSIWA* (n 8) art 48 (1b)
[37] *Barcelona Traction, Light and Power Company, Limited* (n 4) 32 para 34
[38] *Case Concerning East Timor (Portugal v Australia)* [1995] ICJ Rep para 29

the *erga omnes* obligation,[39] this is certainly not true for the inviolability of premises and the derivative[40] obligations of the inviolability of diplomatic correspondence and archives; the ILC was explicit that 'the obligation of the receiving State […] to protect the premises of a mission *is owed to the sending State*'.[41]

Further elaboration of the extended legal right to invoke State responsibility is not attempted below; invocation of State responsibility itself and adopting lawful measures not proportional with the unlawful inter-State cyber operation does not sufficiently alter the cost benefit calculation of the perpetrating State and is therefore not enough to induce compliance with the international law.

2.2. Targets of countermeasures

Countermeasures, being a compliance inducing mechanism, are only to be aimed at the State considered to be responsible for the internationally wrongful conduct. The ICJ was clear on this matter – countermeasures 'must be taken in response to a previous international wrongful act of another State and must be directed against that State'[42] and the customary nature of the rule was reinforced by the ILC arguing 'countermeasures may not be directed against States other than the responsible State'.[43] Contemporary *opinio juris* indicates the same understanding of the law of countermeasures in the context of cyber operations.[44]

As explained in the preceding pair of chapters, a State is deemed responsible for the violation of international law by cyber means when the violation has been legally attributed to that State. Due to the technical limitations and stringent legal standards of attribution, a State injured by

---

[39] ILC, 'Fourth report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur' (1992) ILC Ybk II(1) UN Doc A/CN.4/444 and Add.1–3, para 38; Maurizio Ragazzi, *The Concept of International Obligations Erga omnes* (Clarendon Press 1997) 192

[40] Eileen Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (OUP 2016) 156

[41] *ILC* (n 9) art 43 cmt 6 [emphasis added]

[42] *Case Concerning Gabčíkovo-Nagymaros Project (Hungary v Slovakia)* [1997] ICJ Rep 83

[43] *ILC* (n 9) art 49 cmt 4

[44] Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) <gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 13 August 2019

an unlawful cyber operation is unlikely to be able to invoke responsibility and take countermeasures against the State which is *in fact* responsible for the cyber operation. However, if a State has commissioned the unlawful cyber operation, it has also failed to take diligent steps to prevent or terminate the said wrongful operation. As indicated by the previous chapter, the injured State may indeed be able to establish State responsibility for a failure to meet the standards pertaining to the due diligence obligations of prevention and termination and by doing so remove the power and security benefits of the non-diligent and *de facto* orchestrating or sponsoring State by way of countermeasures.

To establish which State bears the responsibility of failing to act diligently, the State whose rights to diligent protection have been violated by the cyber operation must be able to convincingly prove the territorial jurisdiction of emanation, the accused State's knowledge of the (imminent) unlawful cyber operation and its non-diligent attitude towards termination or prevention.

To illustrate, the 2007 DDoS operation against Estonia cannot be attributed to the Russian Federation[45] because the nexus of agency or control between the natural persons involved in the operation and the State cannot be legally established. Even if socio-political methods of attribution indicated that Russia was *in fact* responsible for the unlawful DDoS operation, it is not to be considered legally responsible for the said cyber operation. However, what can be established is that Russian authorities should have known of the DDoS in violation of the Estonian international rights, that the operation emanated from Russian territory and that Russia had failed to exhibit diligence in the prevention and termination of the cyber operation.

Firstly, the presence of constructive knowledge of the Russian authorities has been already indicated in chapter five; due to the ordinary vigilance over their cyberspace and the widespread media reports, Russia should have been aware of the outgoing DDoS.[46]

---

[45] *See* ch 4
[46] *See* ch 5

Secondly, Russia has exhibited diligence by developing the capacity to prevent and terminate,[47] but public information does not indicate it has taken any steps to discharge the pair of due diligence obligations. In fighting off the perpetrators and the crippling data traffic, Estonia received assistance from the European community of the Computer Security Incident Response Teams,[48] from NATO, Finland and US but not Russia.[49] Besides, President Putin has shown reluctance to prevent or terminate the Russian non-State actors from conducting cyber operations against other nations; '[artists] may act on behalf of their country, they wake up in a good mood and paint things. Same with hackers, they woke up today, read something about the state-to-state relations. […] If they are patriotic, they contribute in a way they think is right, to fight against those who say bad things about Russia'[50] Putin opined several years after the 2007 DDoS operation.

Thirdly, technical information substantiates the assessments that the said cyber operation indeed emanated from the territory of Russia. Generally speaking, several particularities of the cyber operation point to its territorial origin; the language of the malware, its metadata, fonts and the keyboard layout used by the authors can all reveal the origin of the operation. Though it has been said that, for example, the language indicators found in malware 'often point to the attacker's country of origin',[51] the territorial origin of the malicious computer code, however it is established, does not amount to convincing proof for the legitimate target of countermeasures. Much like how the ICJ did not proclaim international responsibility on the State whose territory was used to manufacture or assemble the mines which sank the British navy ships in the Corfu straight, the State where the malware is written or compiled cannot be

---

[47] International Telecommunication Union, 'Cyberwellness Profile Russian Federation' (22 January 2015) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Russia.pdf> accessed 13 August 2019

[48] 'TF-CSIRT to Estonia's Rescue' (*TERENA News*, 10 May 2007) <https://www.terena.org/news/fullstory.php?news_id=2103> accessed 13 August 2019

[49] *Tikk, Kaska & Vlhul* (n 12) 24

[50] Euan McKirdy & Mary Ilyushina, 'Putin: "Patriotic" Russian hackers may have targeted US election' *CNN* (2 June 2017) <https://edition.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html> accessed 13 August 2019

[51] FireEye, 'Digital Bread Crumbs: Seven Clues To Identifying Who's Behind Advanced Cyber Attacks' (26 June 2013) 3 <fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-digital-bread-crumbs.pdf> accessed 13 August 2019

considered to be the originating territory of the cyber operation and cannot be held responsible for the violation of the due diligence obligations. The exploits used in the WannaCry operation, for example, were the work of the US National Security Agency,[52] though later used by North Korea in the operation targeting various governmental computer systems.

Even though the authors of the malicious code and the actual cyber operation may very well be the same actors, what the injured State should establish is under which territorial jurisdiction were the perpetrators acting from, which territory were the main command and control servers situated on, which State was the end destination of the stolen data, and which territory was used to manipulate the functioning or the components of the malware or similar. The preceding chapter has shown this can be done via IP traceback or, more reliably, ASN analysis, though other forms of evidence may serve as a sufficiently clear proof of the State of origin.

The fact that the 2007 DDoS was organised on Russian-speaking forums[53] does not say much of the territorial origin and certainly does not amount to the legal standard of proof, which should be observed to avoid false conclusions and consequentially unlawful countermeasures. Sufficiently clear and convincing proof that the 2007 DDoS emanated from Russia is however available. According to a simple whois query, the web-dozor.ru and 2ch.ru forums both provided the perpetrators with the list of Estonian targets and instructions on how to conduct the operation[54] and were thus deemed to have been central organisational points for the operation as they are not only registered in Russia but also hosted by the Russian ISPs, on computer servers under the Russian territorial jurisdiction.[55] Coupled with the fact that Estonia identified 'specific IP addresses and references to web forum users, who were

---

[52] Brad Smith, 'The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack' (*Microsoft*, 14 May 2017) <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack> accessed 13 August 2019

[53] *Tikk, Kaska & Vlhul* (n 12) 23

[54] ibid 23 fn 81

[55] 'Whois Record for 2ch.ru' <http://whois.domaintools.com/2ch.ru> accessed 19 May 2016; 'Whois Record for Web-Dozor.ru' <http://whois.domaintools.com/web-dozor.ru> accessed 19 May 2016

likely located on the Russian territory'[56] it is safe to say that the 2007 DDoS indeed emanated from Russian territory and that the allegation may be substantiated by a sufficiently clear or convincing proof.

Note also that there may be several territories and thus several States that serve as the point of emanation. In fact, in an effort to obscure the origin, many cyber operations rely on a significant number of transit points or servers located in different territories.[57] These transit States are also considered to be territorial jurisdictions of emanation, putting them under the obligations of due diligence. Much like the State of origin, the non-diligent State of transit is internationally responsible for its failure to take reasonable steps to prevent and terminate the cyber operation in contravention of the international rights of the targeted State.

A number of legal scholars advanced the idea that due diligence obligations imposed on the States of the cyber operation emanating from their jurisdictions includes not only the States of origin but also the States of transit through which the injurious operation is routed.[58] Indeed, expanding responsibility to the transit States serves the purpose of reinforcing the law and aids the aim of it – to promote peace among nations by minimising the occurrence of unlawful maximisations of power. Also, akin to the argument in favour of the international minimum standard of due diligence obligations of prevention and termination, holding the intermediaries responsible for non-diligent behaviour discourages the creation of areas of lawlessness and thus further promotes a decentralised international system of mutual reassurance of peaceful cohabitation among nations.[59]

---

[56] *Tikk, Kaska,& Vlhul* (n 12) 27

[57] TrendMicro, 'Utilising Island Hopping in Targeted Attacks' (25 September 2014) <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks> accessed 13 August 2019

[58] Scott Shackelford, Scott Russell & Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17(1) Chicago J of Intl L fn 100; Michael N Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale L J Forum <http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace> accessed 13 August 2019; *Schmitt* (n 5) 34

[59] *See* ch 5

Although this may be true, further investigation of the responsibility of the transit States falls outside of scope of this thesis for three interconnected reasons. Firstly, this thesis is set to seek legal mechanisms that induce compliance with international law from States that are *in fact* responsible for the materialisation of the unlawful cyber operation and thus reap significant benefits or increase of power by disregarding the law. Except in the case of cooperation between States sharing a common interest in decreasing the power and security of a common adversary,[60] the transit State will not benefit from the unlawful cyber operation. Russia, one of the transit States in case of RedOctober,[61] has not benefited from the cyber operation, for instance. On the contrary, reports indicate that the perpetrators stole the diplomatic documents of the Russian embassy in the US,[62] thus denying its rights to inviolability of the diplomatic correspondence and archives. This also suggests that Russia had no knowledge of the RedOctober operation; if it did, it would undoubtedly do its utmost to diligently prevent or terminate the operation in contravention of its legal rights.

Secondly, because the malicious traffic is often dispersed and hidden in legitimate data flows, the transit State is unlikely to possess actual or even constructive knowledge of the cyber operation, which would be needed in order to place it under the due diligence obligations to prevent and terminate. This is particularly true in the context of DDoS operations. Not only did most of the 178[63] transit States not benefit from the cyber operation and the consequential decline of Estonia's power and security, they are also unlikely to have had any knowledge of the enabling role the infrastructure under its jurisdiction played in the 2007 operation. Unless informed by Estonia, they could not have possessed any actual knowledge. If the operation

---

[60] Stuxnet is currently the only (known) cyber operation considered to be conducted by two States in concert. Ellen Nakashima & Joby Warrick, 'Stuxnet was work of U.S. and Israeli experts, officials say' *Washington Post* (2 June 2012) <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c7a1c56dd3e1> accessed 13 August 2019

[61] 'To control the network of infected machines, the attackers created […] several server hosting locations in different countries (mainly Germany and Russia).' *Global Research & Analysis Team* (n 17)

[62] Benjamin Bidder, Matthias Schepp & Hilmar Schmundt, 'Virus Hunters Try to Catch Diplomatic Time Bomb' *Spiegel* (25 January 2013) <https://goo.gl/fC67zf> accessed 13 August 2019

[63] Daniel Bilar, 'On nth Order Attacks' *in* Christian Czosseck, Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 271

peaked at 90 Mb/s[64] and 178 transit States were involved, the average traffic contribution of one State was 0.51Mb/s, which is low enough to be easily mistaken for a legitimate outgoing traffic. And because the strength of a DDoS operation lies in the great number of participants individually contributing rather innocent amounts of data traffic, States of transit cannot possess the capacity to spot the malicious activity, which is a necessary requirement for establishing constructive knowledge. A similar argument can be made for other cyber operations. ProjectSauron, a State-orchestrated cyber operation targeting government and military systems of several States, relied on legitimate email service to exfiltrate the stolen information.[65] It is absolutely unreasonable to claim that the transit States hosting the relevant cyber infrastructure required for a normal operation of the specific email service knew or even should have known of the cyber operation and thus be placed under the due diligence obligations of prevention and termination.

The last example exposes a third issue with the potential invocation of State responsibility of the non-diligent transit States. Territories of the transit States may indeed be an enabling factor in a cyber operation but can seldom be considered to have actually been 'used contrary to the rights of other States',[66] and thus be under the due diligence obligations of prevention and termination. Because cyber operations often consist of different separate modules and utilise several routing infrastructures or transit States, their malicious and unlawful nature may only materialise when used in conjunction with each other. Email servers, which carry the data acquired by a cyber operation in violation of State sovereignty, cannot be considered to have been used contrary to the international rights of other States if the individual action has no unlawful character. Also, one State whose infrastructure is involved in the DDoS operation and has provided only incremental amount of traffic unable to cause disruption on itself, cannot

---

[64] ibid

[65] Global Research and Analysis Team, 'The ProjectSauron APT' (Version 1.02, Kaspersky Lab, 9 August 2016) <https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf> accessed 13 August 2019

[66] *Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania)* (Merits) [9 April 1949] ICJ Rep 18

be rightfully considered to have violated the rights of the other States; especially considering that legitimate and illegitimate traffic (in reasonable quantities) are indistinguishable in the case of DDoS operations.

Due to the nature of cyber operations, only territorial jurisdictions of transit infrastructure may be known. A technical analysis of the RedOctober operation, for instance, indicates that the perpetrators utilised several servers and relied heavily on the commercial network infrastructure under the jurisdictions of Germany and Russia. The State of origin or the prime beneficiary of the reduction in power and security of the injured States, however, cannot be determined through this measure.[67] Injured States are therefore unlikely to be able to point at the State of emanation with sufficiently clear or convincing proof, which is a legally prescribed standard of proof in relation to the question of emanation.[68] Even though the invocation of State responsibility for the failure to make diligent efforts to prevent and terminate a cyber operation is indeed more likely than the invocation of the responsibility for the cyber operation itself, technology remains a limitation for the inducement of compliance by countermeasures based on the former. This holds true also for the Shamoon operation, which exemplifies the limits of the application of the due diligence principle in the quest to induce compliance by way of countermeasures. There is no public information pointing at the fact that the operation originated in Iran, nor is there any information exposing the transit States. Nevertheless, if Saudi Arabia was to take countermeasures against Iran, it should be able to prove with sufficient clarity that Shamoon was deployed from the territory of Iran, that Iran indeed knew or should have known of the operation and that it had not taken diligent efforts to prevent and terminate the operation.

In spite of the fact that countermeasures are to target only the internationally responsible non-diligent State, strict containment of their effects is not always possible. Considering that the proliferation of (simple forms of) computer malware is notoriously indiscriminate, this is

---

[67] *Global Research & Analysis Team* (n 17)
[68] *See* ch 5

particularly true in case of countermeasures by cyber means. The doctrine of countermeasures indicates that such measures are not strictly prohibited. The Portugal/Germany Arbitral Tribunal's award, deliberating on the reprisals taken by Germany, recognised the fact that consequences may indeed be felt by the innocent State; as long as the reprisals are directed against the responsible State, their 'indirect and unintentional consequence which, in practice, the injured State will always endeavour to avoid or to limit as far as possible',[69] do not render them unlawful. Infringement on the international rights of Portugal by German reprisals, however, was not incidental. Even though it was intended to inflict an indirect deprivation on Great Britain, reprisals targeted Portugal, which were used as a means to an end. Because the latter violated no legal rights of Germany, reprisals were pronounced unlawful.[70] Inspired by the aforementioned decision of the Arbitral Tribunal's award, the ILC's Special Rapporteur Ago distinguished between the unlawful 'cases in which the action implementing the reprisals against the State guilty of prior breaches is an action immediately and deliberately directed against the innocent third State [and, on the other hand, the lawful] cases in which, conversely, the action is aimed directly only at the State against which the reprisals are being taken and it is only in the context of this action that the rights of a third State are also infringed.'[71]

Three conclusions in regard to the effects of countermeasures in the cyber context can be drawn from the paragraph above. It transpires that unintended consequences of countermeasures on innocent States are to be avoided or limited as far as possible. The borderless nature of cyberspace and the traditional conception of the indiscriminate propagation of a computer malware suggest caution when countermeasures are conducted by a reactive cyber operation. Pretending for a moment that they were reactive cyber

---

[69] *The Cysne Arbitration (Portugal v Germany)* [1930] II UNRIAA (Sales No. 1949.V.1) 1011, 1056–1057

[70] 'As Portugal had not violated, in relation to Germany, any rule of international law, acts of reprisals directed against her were contrary to international law.' *Portugal v. Germany (The Cysne)* 5 ILR 487, 491

[71] ILC, 'Eighth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur. The internationally wrongful act of the State, source of international responsibility (continued)' (1979) II(1) Ybk of the ILC UN Doc A/CN.4/SERA/1979/Add.l (Part 1), 46 para 97

countermeasures, ProjectSauron and WannaCry serve as an illustration of the two opposites of the spectrum – on the one hand, a tailored and targeted cyber operation and, on the other hand, an indiscriminate cyber operation with unlimited consequences on the third States. ProjectSauron, a State-orchestrated cyber operation, is a tailored operation, targeting only specific governmental network infrastructures of several States. While cyber operations with similar functionality usually result in a widespread infection, 'ProjectSauron seems to [have been] dedicated to just a few countries, focused on collecting high value intelligence by compromising almost all key entities it could possibly reach within the target area. […] Almost all of ProjectSauron's core implants are unique, have different file names and sizes, and are individually built for each target.'[72] Even if the effects of ProjectSauron would have spilled over to the innocent States, the orchestrator clearly tried to avoid this. Conversely, WannaCry infected more than 230,000 systems in 150 countries[73] and has rightly been characterised by the British[74] and American[75] authorities as indiscriminate. In brief, if these two operations were legitimised as cyber countermeasures furnished by a previous lack of diligence in preventing and terminating a wrongful cyber deed, the ProjectSauron would be within the limits of the law, while the same cannot be claimed for WannaCry.

What is more, cyber countermeasures must not use the infrastructure of an innocent State as a means to an end. In the era of cloud computing governed by remote storage solutions,[76] a situation where countermeasures target the infrastructure of a non-State actor in one State in order to inflict compliance-inducing deprivation onto another State is not hard to envision. Indeed, disrupting the infrastructure under the jurisdiction of an innocent State, potentially the

---

[72] *Global Research and Analysis Team* (n 65) 6

[73] ENISA, 'WannaCry Ransomware Outburst' (15 May 2017) <https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst> accessed 13 August 2019

[74] Lord Ahmad, 'Foreign Office Minister condemns North Korean actor for WannaCry attacks' (Press Release (19 December 2017) <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks> accessed 13 August 2019

[75] Thomas P Bossert, 'It's Official: North Korea Is Behind WannaCry' *Wall Street Journal* (18 December 2017) <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537> accessed 13 August 2019

[76] UK Ministry of Justice, for example, is using Amazon data storage cloud services since November 2016 but Amazon's European servers were only found in Frankfurt and Dublin prior to December 2016.

weakest link on which the functionality of the internationally responsible State depends, may be a convenient method of reactive cyber measures against the non-diligent wrongdoer. Such countermeasures, however, would not constitute a lawful reaction of the initially injured State.

Lastly, this does not mean the non-State actors cannot be targeted by countermeasures. Much like how an injury may be inflicted on a State indirectly, countermeasures may live up to their instrumentality in an indirect manner. As long as the State is the object of the countermeasures, '[t]he targets of a countermeasure need not be State organs or State cyber infrastructure'.[77] It is important that these non-State actors are under the jurisdiction of the State targeted by the countermeasures, otherwise the State taking countermeasures may be responsible for using the third State as an intermediary, which is, as explained in the preceding paragraph, not permissible.

3. Procedural and temporal considerations

3.1. Ex-ante procedural conditions of resorting to countermeasures

Before the injured State is permitted to employ countermeasures to induce compliance with the obligations arising from the international responsibility, certain procedural conditions must be met. If the instrumentality of countermeasures – inducing compliance[78] – is to be achieved, the non-punitive character of the response must be explicitly communicated to the wrongdoing State. This condition is of imperative importance in distinguishing the instrumental countermeasures meant to reinforce the law from the usually practiced reactive violation of the law, which indeed provides restoration of power but also brings about the deterioration of the rule of law.[79]

[77] *Schmitt* (n 5) 112
[78] *See* ch 3
[79] *See* ch 2

To communicate the instrumentality, the State about to employ countermeasures should, *inter alia*, call the responsible State to comply with the primary obligation and explicitly notify the perpetrator of its intentions to take countermeasures.[80] To live up to the instrumentality, countermeasures must also be limited to temporary non-performance and must be discontinued, if possible, as soon as compliance is achieved.

International customary law outlines the conditions relating to the resorting of countermeasures, designed to not only announce the instrumentality of the imminent countermeasures but also to assure that less invasive methods of reconciliation are used before flexing any muscles. Acknowledging that taking countermeasures involves the risk of 'causing an escalation which will lead to a worsening of the conflict',[81] the underlying purpose of these preconditions is to avoid the fruition of such a situation, to induce compliance without any reactive deprivations and to restore the power and security relationship as it existed before the breach.

Regardless of when the injured State invokes the international responsibility and decides to proceed with countermeasures, it must invite the non-diligent State to compliance and inform of its intention to take them. These are well-established ex-ante procedural conditions of resorting to countermeasures. In assessing the lawfulness of Czechoslovakia against Hungary in the Gabčíkovo-Nagymaros Project case, the ICJ maintained 'the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it'.[82] This stance was endorsed and codified by the ILC in the ARSIWA. Prominent scholars such as Zoller[83] and Elagab[84] also argued in favour of the legal

---

[80] *ARSIWA* (n 8) art 52(1b)
[81] *Air Service Agreement of 27 March 1946 between the United States of America and France* [1978] XVIII UNRIAA para 91
[82] *Case Concerning Gabčíkovo-Nagymaros Project* (n 42) 56, para 84
[83] *Zoller* (n 3) 119
[84] *Elagab* (n 7) 64–79; Omer Yousif Elagab, 'The Place of Non-Forcible Counter-Measures in Contemporary International Law' *in* Guy S Goodwin-Gill & Stefan Talmon (eds), *The Reality of International Law: Essays in Honour of Ian Brownlie* (Clarendon Press 1999) 129–132

requirement of a demand for compliance with the obligations of cessation and reparation prior to the employment of countermeasures.

In theory, a call to compliance and a threat of countermeasures may be sufficient to procure the desired effect and in fact convince the responsible State to take diligent steps to terminate a continuous cyber operation emanating from its territory or to prevent a future one as well as to provide reparations for the violation. Elagab offers an example of a dispute between the US and Yugoslavia in 1948 where a mere threat of countermeasures induced compliance. After the latter shot down a pair of American aircrafts and detained crew and passengers, the US protested and threatened with countermeasures if the Yugoslav government did not cease the unlawful conduct and did not provide reparations in 48 hours. A threat was sufficient to induce compliance as both of the secondary obligations consequential to its international responsibility were met by Yugoslavia.[85]

However, when it comes to cyber operations, protests and invitations to compliance are unlikely to restore the legal relationship or power and security balance between the States. As I have explained in the second chapter of this thesis, practice indicates States are unlikely to admit having anything to do with malicious cyber operations, let alone to take steps toward compliance with international law; protests diminishing the reputation of the responsible State are insufficient to change the rational calculation of the wrongdoing State.[86]

Even though it is unlikely to procure the desired effect, an invitation to compliance and notification of intent to take countermeasures are nevertheless important steps in avoiding the escalation of a conflict, particularly so in the context of cyber operations. Since evidence pointing to the originating jurisdiction of a cyber operation might be unreliable, the injured State should put its claims to the test by inviting the allegedly responsible State to comply with its obligations and give them the opportunity to explain their behaviour.

---

[85] *Elagab* (n 7) 69–70
[86] *See* ch 2

This is well-established State practice, be it in relation to unlawful cyber operations or other violations of international law. For example, after what seems to have been a series of unauthorised intrusions in the American network infrastructure, officially classified as an interference with the 2016 US presidential elections,[87] US President Obama reached out to his Russian counterpart; according to the former, Russia was urged 'to cut it out [or] there were going to be serious consequence'.[88]

The rejection of responsibility or a lack of any satisfactory response to the allegation and call to compliance triggers the right to resort to countermeasures. To illustrate, in the dispute between France and the US, which was finally resolved by the Air Services arbitration, the latter took countermeasures only after a warning of upcoming countermeasures had been conveyed to France. The reply of the US to the Memorial Submitted by the Government of the French Republic explained that 'the US specifically warned, by diplomatic note, that countermeasures would be taken if France did not end the violation'.[89] Because the demands remained unsatisfied even after a 30 day period and because France indicated no intention to comply with the specific international obligations in the future, the US resorted to countermeasures. In a similar vein, the British government recently decided to proceed with freezing Russian assets only after the demands to explain the allegations of the Russian conduct in violation of the British legal rights had been met with 'sarcasm, contempt and defiance […, demonstrating] a complete disdain for the gravity'[90] of the violations.

The ex-ante preconditions to countermeasures outlined are however not absolute. The regime of countermeasures recognises the priority of inducing compliance over the fear of escalation

---

[87] President of the United States, 'Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment' (*The White House*, 29 September 2016)
[88] William M Arkin, Ken Dilanian & Cynthia McFadden, 'What Obama Said to Putin on the Red Phone About the Election Hack' *NBC News* (19 December 2016) <https://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116> accessed 13 August 2019
[89] 'Law of Treaties and Other International Agreements' *in* US Department of State, *Digest of United States Practice in International Law* (Office of the Legal Adviser 1978) 655, 773
[90] Theresa May, 'PM Commons Statement on Salisbury incident response: 14 March 2018' (Oral statement to Parliament,14 March 2018) <https://www.gov.uk/government/speeches/pm-commons-statement-on-salisbury-incident-response-14-march-2018> accessed 13 August 2019

of the conflict. In what is classified as an urgent countermeasure, injured States are permitted to proceed with taking countermeasures when there is a real possibility the responsible State will be able to immunise itself from the effects of countermeasures and thus escape the equalising impacts countermeasures would have on the power and security relationship between the parties in the conflict. In my view, this fear of immunisation is exaggerated and the States injured by a cyber operation consequential to the absence of diligent attempts of prevention and termination should avoid them as much as possible.

The fear of immunisation from the effects of countermeasures as a rationalisation for urgent countermeasures is provided by the ILC as well as the Tallinn Manual 2.0 in the specific context of wrongful cyber operations. Clearly inspired by the ILC's warning of the 'modern conditions of communications',[91] the Tallinn Manual 2.0 substantiated the argument in favour of urgent countermeasures based on the fact that '[n]otifying the responsible State of its intent to [respond by blocking all electronic access to the responsible State's bank accounts] would afford that State an opportunity to transfer assets out of the country, thereby effectively depriving the injured State of the option of taking that countermeasure'.[92]

The key erroneous assumption in both is that the injured States need to specify the kind of countermeasures to be taken if the call to compliance with the secondary obligations of cessation and reparations are not met in due course. State practice does not support this.[93] To build up on the examples given above – US President Obama did not specify what *serious consequences* in reaction to the Russian interference with the electoral process are to be expected if the unlawful intrusions to the American computer network infrastructure persist.[94] Nor did British Prime Minister May enumerate on the 'full range of measures',[95] when declaring

---

[91] *ILC* (n 9) 330
[92] *Schmitt* (n 5) 120
[93] *Elagab* (n 7) 71
[94] *Arkin, Dilanian & McFadden* (n 88)
[95] James Masters, 'Theresa May's full statement on Russian spy's poisoning' *CNN* (13 March 2018) <https://edition.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html> accessed 13 August 2019

the intent to take countermeasures against Russia in 2018 for the alleged poisoning of British citizens on British soil.

Because the law of State responsibility does not prescribe reciprocity but proportionality[96] and because it does not dictate the methodology of countermeasures, the injured State is permitted to deprive the responsible State of almost any international right[97] even if countermeasures are preceded by a call to compliance and notification of intent. The fact that the responsible State is unaware where countermeasures will manifest, effective immunisation is virtually impossible.

Given these points, urgent countermeasures have no real advantage. In fact, urgent countermeasures in the context of this thesis pose a significant risk of being unlawful and of sparking the escalation of a conflict. Firstly, evidence pointing at the origin of the cyber operation is frequently characterised by a degree of uncertainty and taking countermeasures against a State which has not breached the obligation of due diligence is unlawful. Secondly, while the diligent development of capacity to prevent and terminate is largely a matter of public knowledge,[98] whether the State of emanation has or has not fulfilled the obligations may not always be apparent. Avoiding urgent countermeasures, and thus calling on the allegedly responsible State to comply with the due diligence obligations and informing it of the intent to take countermeasures, will allow the allegedly responsible State to potentially demonstrate that it indeed has done its utmost to prevent and terminate the unlawful cyber operation. At the same time, refraining from taking urgent countermeasures will protect the injured State from inflicting an unlawful reactive deprivation, which could lead to escalation.

---

[96] *See* ch 3 for distinction between *reciprocal* and *proportional* countermeasures.
[97] Limits exist. Countermeasures are not to be forceful and shall not affect the fundamental human rights, rights stemming from the international humanitarian law, peremptory norms and self-contained regime of international diplomatic law. See *ILC* (n 9) art 50 and commentary
[98] *See* ch 5

3.2. Temporary character of countermeasures

To be instrumental, countermeasures are only to be applied at the time of the non-compliance with the international obligations. In other words, when the breach occurs and the responsible State refuses to comply with the due diligence obligations of prevention and termination, with the obligation to guarantee non-repetition or with the obligation of reparation, the injured State may proceed with inducing compliance by way of countermeasures. Most recently, the principle has been pronounced by the ICJ in 2011 during its deliberation of countermeasures taken by Greece against the Republic of North Macedonia. The court found that the countermeasure employed to procure cessation of North Macedonia's wrongful act was in itself wrongful because the initial wrongful conduct ceased long before the countermeasure was taken.[99] This means that instrumental countermeasures are limited to a temporal suspension of the international obligations,[100] which is why they ought to be 'suspended without undue delay'[101] once the responsible State has complied with the obligations arising from its international responsibility.

In order to determine the timeframe during which the injured State is permitted to employ countermeasures, establishing the beginning and the end of the non-compliance with the obligations stemming from failure to take diligent steps to prevent and terminate the unlawful cyber operation is imperative.

Provided that the State is or should have been aware of the imminent or the ongoing cyber operation emanating from its territory, a breach of due diligence obligations occurs if the unlawful cyber operation in fact materialises. Consequentially, the State incurring responsibility for the very breach is therefore under the so-called secondary obligations from the moment the unlawful cyber operation occurs. To establish the window of opportunity for

---

[99] *Application of The Interim Accord of 13 September 1995 (Greece v Former Yugoslav Republic of Macedonia)* [2011] ICJ Rep paras 120, 121, 164, 165, 170

[100] *Naulilaa Arbitration (Portugal v Germany)* [1928] II UNRIAA (Sales No. 1949.V.1) 1012, 1026

[101] *ARSIWA* (n 8) art 52(3)

countermeasures, the temporal characteristics of the trinity of obligations should be elaborated.

First, the responsible State is under the obligation to cease a non-diligent conduct, which means to take diligent steps towards prevention and termination of a cyber operation. Since it is not legally responsible for the resulting unlawful cyber operation, it is also not under the obligation to cease the latter; 'cessation of the continuing breach is solely owed by the state or the organisation responsible for it *under the rules of attribution of conduct*'.[102]

As explained in the third chapter, obligations of cessation or compliance with the primary obligations in the present only apply when the non-compliance has a continuous character. Since the unlawful event which diligence was supposed to prevent already materialised, the responsible State cannot be under the obligation to take diligent steps towards prevention. In other words, the violation of the due diligence obligation of prevention is an instantaneous wrongful act. This means that the employment of countermeasures to induce compliance with the due diligence obligation of prevention cannot be instrumental, which is the defining attribute of a lawful reaction under the international law of countermeasures.

A violation of the due diligence obligation of termination, on the other hand, may extend in time. For as long as the unlawful cyber operation in question is ongoing, the State of origin ought to cease with the non-diligent behaviour or, in other words, to do everything in its power to terminate it. If the State of origin takes no steps towards compliance with the due diligence obligations or cessation of the non-performance, the injured State may induce compliance by way of countermeasures during the entire period of this non-performance.

If, however, the cyber operation has completed, the responsible State is not under the obligation of cessation as there is nothing to prevent or terminate anymore. Once again,

---

[102] Pierre d'Argent, 'Reparation, Cessation, Assurances and Guarantees of Non-Repetition' *in* André Nollkaemper & Ilias Plakokefalos (eds), *Principles of Shared Responsibility in International Law – An Appraisal of the State of the Art* (CUP 2014) 216 [emphasis added]

countermeasures intended to induce compliance with the unlawful conduct concluded in the past are not instrumental and therefore not a lawful reaction.

This is not to say that in the event of the completed cyber operation, the non-diligent State has escaped the responsibility and that the State which is *in fact* responsible for the resulting unlawful cyber operation got away with the benefit of an increase in its national power and a rational reason to resort to illegitimate power maximisation also in the future.

The obligations assuring future compliance are indeed still outstanding. If countermeasures inducing cessation are intended to procure current compliance with the primary due diligence obligations, the secondary obligations of non-repetition and reparation, on the other hand, aim to induce diligent behaviour in the future. Both can and should be demanded and induced by way of countermeasures even once the unlawful conduct has concluded.

Obligation to provide guarantees of assurances of non-repetition, seeks to do so by relying on the promises of compliance given by the wrongdoing State. To provide guarantees of non-repetition, the responsible State, is to indicate willingness to be diligent in the future, to do its utmost to prevent and terminate a cyber operation emanating from its territory. Guarantees and assurance of non-repetition can only be demanded in the face of a significant risk of repetition[103] and may take the form of a commitment to technical, organisational and legal capacity-building measures, which will allow it to discharge the obligations of prevention and termination in the future.

Unfortunately, promises of non-repetition do not provide much of an assurance that the breach of obligations will in fact not occur again.[104] What is a more effective method of assuring future compliance is the third secondary obligation, the obligation of reparation, which aims to ensure compliance by increasing the costs of non-compliance, thus to change the rational calculous and deter impending violations. Even though the obligation of reparation arises as soon as the

---

[103] *See* ch 3
[104] ibid

unlawful cyber operation materialises and hence the breach of due diligence obligations occurs, reparation should not be demanded nor should they be enforced by way of countermeasures until the resulting cyber operation is concluded and the scope of injury can be assessed in its entirety.

Because the responsible State is legally obliged to provide reparations and guarantees of non-repetition for as long as these two obligations have not been met, it is worth noting that the right to invoke State responsibility and employ countermeasures does not stretch in time indefinitely. While '[n]one of the attempts to establish any precise or finite time limit for international claims in general has achieved acceptance,'[105] steps towards employment of countermeasures should be taken without an unreasonable delay.[106] When it comes to inducing compliance through international judiciary, it is 'for the Court to determine in the light of the circumstances of each case whether the passage of time renders an application inadmissible'[107] and thus decide whether the process of including compliance with international law has been attempted within the boundaries of reasonableness. Accordingly, in the context of inducing compliance by measures of self-help, quantification of a reasonable delay and therefore determining the availability of redress by countermeasures is to be determined by the injured State based on specific circumstances of the breach and the responsibility.

Generally speaking, the sooner the injured State takes steps towards employing countermeasures, the better.[108] Not only is this true in the interest to uphold the legitimacy of the law, as argued in the third chapter, but also in the context of the obligation of cessation. In the case of an ongoing unlawful cyber operation occasioned by the lack of due diligence, early countermeasures may indeed induce compliance with the obligation of diligent termination and thus possibly prevent further damage caused by the operation of a continuing character.

---

[105] *ARSIWA* (n 8) art 45
[106] *ILC* (n 9) art 45 cmt 6
[107] *Certain Phosphate Lands in Nauru (Nauru v. Australia) - Preliminary objections* [1992] ICJ Rep para 32
[108] *See* ch 3

In the event of a completed cyber operation, on the other hand, swift countermeasures aimed at procuring the guarantees of non-repetition or securing reparation may deter the responsible State from repeating the unlawful maximisation of the power and security, a situation that is indeed likely to materialise if not met with proportional costs in the form of countermeasures.[109] Resorting to countermeasures as soon as the breach occurs may however not always be in the interest of an injured State. The so-called limit to application of due diligence originating in the inability of an injured State to clearly and convincingly establish the State of emanation could be eliminated as the time passes. Rapid advancements in technology may, for example, enable Saudi Arabia to convincingly establish the State of origin of Shamoon in the years following the conclusion of the operation.

What does all this mean in practice? We now know the first wave of the DDoS cyber operation in violation of the sovereign rights of Estonia hit its network infrastructure on the 27th of April 2007.[110] It originated from the territory of Russia, which should have been aware of it and (as far as the public information goes) did nothing to diligently attempt to prevent or terminate the operation and thus incurred the international responsibility for its violation of due diligence obligations. On that very date, the breach occurred and by operation of law, Russia was under the secondary obligations of present and future compliance – to cease with the non-diligent behaviour, to guarantee non-repetition in the future and to provide reparations. By the 11th of May, the time the operation concluded, Estonia did not attempt to induce diligent termination by way of countermeasures even though it had every right to do so; if it did, however, the countermeasures inducing cessation should be suspended on the 11th of May as the object of termination has ceased to exist.

Even after the breach of the due diligence obligations of prevention and termination have long concluded, Estonia may still be legally empowered to enforce non-repetition and reparation.

---

[109] *See* ch 2

[110] Beatrix Toth, 'Estonia under cyber attack' (*Hun-CERT*, 2007) 1 <https://goo.gl/Zy9r8o> accessed 13 August 2019

Estonia could very well take countermeasures against Russia even 11 years after the cyber operation occasioned by the Russian lack of diligent prevention and termination efforts crippled its computer network systems. Provided that it is able to provide a justification for the delay of several years, that is.

Since there is a significant risk of repetition indicated by the permissive attitude of Russian authorities in relation to the so-called patriotic cyber artists[111] and the fact that its relationship with Estonia has not seen significant improvements in the last 11 years,[112] the latter may rightfully demand non-repetition. However, because future compliance with the primary obligations based on guarantees and assurances of non-repetition depends on the unreliable promise of rational egoists, the effectuation of reparation is imperative; the restoration of the earlier power relationship through reparation alters the rational choice calculation of the responsible State and therefore ensures compliance with the law in the future.[113] Countermeasures effectuating reparation may be employed for as long as the obligation is due. Since there is no indication of the Russian attempt to re-establish the power relationship by, for example, providing satisfaction in form of an apology or compensation for the economic damage caused by the DDoS botnets targeting Estonia's financial systems, Estonia is still permitted to take countermeasures to restore the power relationship, thus changing the rational choice calculation of Russia and inducing compliance with the obligations of due diligence in the future.

---

[111] *McKirdy & Ilyushina* (n 50)

[112] '[For Russia], cyber operations are a cheap and easily used means of advancing the regime's interests. It is a weapon used to silence the opposition within the country as well as to influence international organisations and foreign countries.' Estonian Foreign Intelligence Service, 'International Security and Estonia 2018' (2018) 52 <https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf> accessed 11 August 2019

[113] *See* ch 3

4. Lawful and effective countermeasures are proportional

To be lawful under the international law of State responsibility as well as effective in inducing compliance with the obligations of due diligence, countermeasures must be proportional with the initial wrongdoing and the material injury caused by it.

To exhibit qualitative proportionality with the initial breach of the international obligations, countermeasures must approximate legal equivalence with the initial wrongdoing; in the context of responsibility for the non-diligent behaviour, deprivation of international rights by way of countermeasures must not be grossly disproportionate to the violation of the due diligence obligations of prevention and termination. To particularise a qualitatively proportional countermeasure in reaction to a violation of due diligence obligations is not needed here; aside from restrictions enshrined in the ARSIWA article 50,[114] States can choose to take whatever proportional measures they deem potentially effective in procuring compliance. Suffice to say that a violation of due diligence obligations to prevent and terminate the internationally wrongful acts does not need to be countered by a non-diligent behaviour or a measure absolutely equivalent to the initial breach what would constitute a reciprocal countermeasure.

Proportional deprivation of peace and security by reciprocal and reactive non-compliance with international obligations may be a sufficient cost to induce temporary cessation but not necessarily an adequate one to match the benefits of the initial violation and to alter the rational choice of the non-diligent States *in fact* conducting or sponsoring the cyber operation.[115] Countermeasures which are not proportional with the consequences of the unlawful cyber operation cannot be an effective compliance inducing mechanism in the case where a State legally responsible for the non-diligent prevention and termination was also *in fact* responsible for the unlawful cyber operation itself and thus reaped the benefits in a form of the inflation of its relative power. Countermeasures taking into account only the qualitative proportionality

---

[114] *ARSIWA* (n 8) art 50
[115] *See* ch 3

may also jeopardise the purpose of the law of State responsibility and diminish its potential to supress the (re)occurrence of inter-State cyber operations in contravention with the international legal rights.

As per the rational choice theory, countermeasures are only effective in reducing the benefits reaped by the State responsible *in fact* for the unlawful cyber operation and in imposing compliance with its international obligations when they are proportional also in quantitative terms[116] or when effects of countermeasures on the responsible State's power exhibit an approximate equivalency with the injurious consequences of the non-diligent behaviour of the responsible State.

According to the international law of State responsibility, the material consequences 'caused by the internationally wrongful act of a State'[117] are embodied by the reparation owed. It is therefore submitted that countermeasures must be in quantitative proportional relationship with the due reparation. In spite of the fact that the non-diligent State cannot be considered to be legally responsible for the resulting cyber operation, it is to provide reparations for all the injurious consequences of the resulting unlawful cyber operation based on the principle of causation.

The State wishing to employ effective countermeasures must establish a sufficient causal nexus[118] between the lack of due diligence in prevention or termination efforts and the injurious consequences of the resulting cyber operation – material injury, being the loss of power and thus a reduced level of security. The principle of causation derives from tort law but has been applied to public international law by the scholarship[119] as well by the international

---

[116] *See* ch 3
[117] *ARSIWA* (n 8) art 31
[118] *Biwater Gauff (Tanzania) Ltd. v. United Republic of Tanzania* (Award) ICSID Case No. ARB/05/22, para 738. See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep para 462: 'with a sufficient degree of certainty'
[119] Tal Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility* (Bloomsbury Publishing 2006); Ilias Plakokefalos, 'Causation in the Law of State Responsibility and the Problem of Overdetermination' (2015) 26(2) EJIL

jurisprudence. In the Corfu Channel case, the United Kingdom requested that the Court declare Albania as internationally responsible not only for the omission of the due diligence obligation but also for the reparation of material injuries inflicted by the resulting incidents in the Corfu straight.[120] The ICJ obliged and found Albania responsible for *inter alia* 'the damage and loss of human life which resulted from them, and that there is a duty upon Albania to pay compensation to the United Kingdom'.[121] A similar reasoning is observed in the Tehran Hostages case, where the ICJ ruled that 'Iran is under an obligation to make reparation to the Government of the United States of America for the injury caused to the latter by the events of 4 November 1979 and what followed from these events',[122] events being the lack of diligence in prevention of the occupation of American diplomatic and consular premises in Iran. What the Court did not provide is an explanation of how exactly the material injuries incurred by the United Kingdom and the United States were caused by the acts resulting from the omission of the due diligence obligations.

To establish when the responsible non-diligent State is under the obligation of reparation for the material injuries of the resulting unlawful cyber operation, I proceed to explaining the applicable principles of the law of tort; accordingly, to indicate a factual and a legal causation between a non-diligent behaviour and the injury of a resulting unlawful cyber operation, the State wishing to take countermeasures ought to confirm that the lack of diligence was *a* cause and *the* cause[123] of the injury from resulting unlawful cyber operation.

The inquiry of causation is therefore twofold – first, the unlawful omission has to amount to 'a substantial factor in producing'[124] the material injury or in fact **cause** or **occasion** the said injurious act. To say that the conduct was a cause of the subsequent injury it must be

---

[120] *Corfu Channel case* (n 66) 10
[121] ibid 23
[122] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* [1980] ICJ Rep para 95(5)
[123] Richard W Wright, 'Causation, Responsibility, Risk, Probability, Naked Statistics, and Proof: Pruning the Bramble Bush by Clarifying the Concepts' (1988) 73 Iowa L Rev 1001, 1012
[124] Jane Stapleton, 'Legal Cause: Cause-in-Fact and the Scope of Liability for Consequences' (2001) 54 Vanderbilt L Rev 941, 973

'necessary to produce the event *and* [constitute] an abnormal intervention in the existing or expected state of affairs'.[125] To establish whether the conduct was indeed necessary to produce an injurious event in violation of the rights of another State, tort dictates the application of the *but for* test. What is a standard test of causality in tort law and 'of particular interest for international law because it has also been used by international courts and tribunals',[126] the so called *but for* test considers the omission to be the cause of the injurious unlawful act if the act would not have occurred but for that omission. In other words, the *but for* test 'tells us whether the relevant, legally proscribed conduct was a necessary condition for the outcome in question'.[127] Omission of due diligence may indeed be a necessary condition for the injurious event to materialise in another State; in the Corfu channel case, it is more likely than not that the explosions would not have occurred had Albania notified the British navy of the existence of the minefield and the dangers it posed to its warships. Additionally, to be considered a cause, the omission must also constitute an abnormal intervention in the regular state of affairs. It is said that an omission is to be 'treated as an [abnormal] intervention […] and so as a cause whenever a positive act is expected or required but the [State] does not perform it. Thus, the change brought about is a change not in the existing but in the expected state of affairs.'[128] In the context of the law of State responsibility and the omission of the diligent prevention and termination, any conduct below the legally acceptable standard of due diligence would constitute an abnormal intervention and thus a cause of the resulting act and its material injury. For example, in the case of the incident at the US embassy in Tehran, Iran did send the Revolutionary Guards to the scene to protect the diplomatic premises but the Guards' inaction once there meant that Iran did not do enough

[125] *Becker* (n 119) 294
[126] *Plakokefalos* (n 119) 477
[127] Peter Cane, *Responsibility in Law and Morality* (Hart Publishing 2002) 120
[128] Tony Honoré, *Responsibility and Fault* (Hart Publishing 1999) 12

to comply with the due diligence as expected and prescribed by the international diplomatic law.[129]

Accordingly, failing to satisfy the expected standard of diligent prevention or termination of legally injurious cyber operation would constitute an abnormal intervention but to argue the omission was indeed a necessary condition for the resulting cyber operation remains challenging. While diligent efforts of prevention and termination are indeed more likely than not to prevent or terminate a cyber operation and thus prevent or minimise the consequential material injury or loss of power resources, it is by no means a guarantee that the injury and loss of power resources will not occur. In other words, even territories of the most diligent nations can be used for malicious cyber operations, injurious to other nations.[130] In fact, success is not a requirement of the law; being obligations of conduct, diligent prevention and termination do not require States to succeed and guarantee the absence of injurious cyber acts. Besides, cyberspace offers immense flexibility and creative State agents or non-State actors wishing to diminish the power and security of another State will always be able to launch a cyber operation even under the conditions of a diligent State. In brief, though it is not impossible, it would be hard to establish 'with a sufficient degree of certainty'[131] that the violation and the consequential injury would not have occurred but for the omission of diligent prevention or termination efforts by the State and thus the omission was in fact the cause for the resultant cyber operation.

What is more plausible to be successfully established is that the omission of a diligent prevention in fact occasioned the cyber operation and the consequential injury. Thus, a non-

---

[129] *United States Diplomatic and Consular Staff in Tehran* (n 122) 13

[130] US is such an example. Although diligent in prevention and termination capacity building, most malicious (although not necessarily also inter-State) cyber operations nowadays come from the US. *See* International Telecommunication Union, 'ITU Global Cybersecurity Index (GCI) 2018' (2018) 62 <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>; Jordan Robertson, 'A Decoy Computer Was Set Up Online. See Which Countries Attacked It the Most' *Bloomberg* (24 September 2014) <bloomberg.com/news/2014-09-23/a-decoy-computer-was-set-up-online-see-which-countries-attacked-it-the-most.html> both accessed 11 August 2019

[131] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 118) para 462

diligent State may be under the obligation of reparation proportional with the material injury of the resulting wrongful cyber operation if its failure to meet the due diligence standards in fact occasions the resulting cyber act in question. In other words, a factual causal relationship between the omission and the injury of the resulting act materialises when the first creates or fails to remove the opportunity for the occurrence of an act in violation of the rights of the other State.[132] That a breach of duty to prevent indeed occasions the malicious cyber operations and that this allows for countermeasures commensurate with the material injury of the resulting cyber operations on the grounds of causal nexus between the omission and cyber operation has been recognised by several States. Applying the causality principle to international law, a document jointly produced by 16 States and NATO, argues that if a State fails to live up to the standard of diligent prevention, 'it should be held responsible for international cyber attacks against another State because its omission *helped create a safe haven* for attackers to attack other States.'[133]

After a cause in fact has been established, the second stage in the injured State's causal inquiry must determine whether the non-diligent behaviour was also a cause in law; it must determine whether the omission of due diligence was *the* cause of the injury of the resulting cyber operation.

The ILC has been careful not to take a clear position on the universally applicable methodology and omitted the prescription of attributes pertaining to the nexus between the unlawful conduct and the injury. Drafters of the ARSIWA 'had considered a number of suggestions for qualifying that causal link, but, [concluded] that, since the requirements of a causal link were not

[132] H L A Hart & Tony Honoré, *Causation in the Law* (OUP 1985) 6

[133] 'Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.3: Concept Framework' (MNE7) (Version 3.0, 3 October 2012) 8 [on file with the author] 8. Mind that the authors of the document did not intend to limit the term *cyber attack* to the forceful cyber operations.

necessarily the same in relation to every breach of an international obligation, it would not be prudent or even accurate to use a qualifier.'[134]

Nevertheless, the commentary of the aforementioned Articles does point in the direction of the applicable principles of the law of tort. Common law[135] and the international arbitration awards have adopted the test of directness based on foreseeability. An injury, which 'is too indirect and remote [cannot] become the basis, in law, for an award of indemnity'[136] argued the arbitrators in the Trail Smelter case.

Whether the injuries of the resulting cyber operation are too remote or not depends on the assessment of the foreseeability[137] of the injury. For example, the arbitrators in the Naulilaa case did not hold Germany responsible for reparations of the indirect damage resulting from 'an unforeseen sequence of exceptional circumstances'.[138] The fact that injury from a resulting unlawful cyber operation is indeed foreseeable can be distilled from the purpose of the due diligence obligation, which is established for the very reason of preventing the occurrence and consequences of unlawful transboundary cyber operations, imposing a shared responsibility for the functional international law and nurturing international peace and security. What is more, as established in the preceding paragraphs of this thesis, the obligation of diligent prevention and termination in cyberspace has been explicitly voiced by various States, further supporting the argument that they are indeed aware of the foreseeability of the cyber operations in violation of the legal rights of other States in the event of non-diligence.

The fact that internationally wrongful and injurious cyber operations stemming from a particular territorial jurisdiction are indeed foreseeable is also supported by the factual arguments. This is particularly true for the States which have historically been the source of cyber operations

---

[134] ILC, 'State responsibility (concluded) Draft articles proposed by the Drafting Committee on second reading' (2000) I Ybk of the ILC UN Doc A/CN.4/SER.A/2000, 388 para 17
[135] Michael A Jones, *Textbook on Torts* (Blackstone Press 1998) 266–267
[136] *Trail smelter case (United States v Canada)* [1938 and 1941] III UNRIAA 1905, 1931 para 5
[137] *Jones* (n 135) 267
[138] *Naulilaa Arbitration* (n 100) 1031

in contravention to the international rights of other States. Accordingly, the internationally wrongful cyber operations originating in China, Russia and Iran, territories which accounted for more than a third of all sources of malicious inter-State cyber operations in the past decade,[139] can rightfully be considered as foreseeable consequences of their potential lack of non-diligent attitudes in regards to prevention and termination efforts.

Upon successfully establishing a causal relationship between the (injury of the) resulting cyber act and the omission of the diligent behaviour, the non-diligent State is under the obligation to provide reparations not only for the lack of diligence but also for all the injurious consequences of the resulting cyber act. In the context of the rational choice theory outlined in the second chapter, the non-diligent State is under the obligation to repair all the loss of power and security incurred by the State injured by the unlawful cyber operation.

This leads to the conclusion that the non-diligent State of origin can be subjected to countermeasures proportional to the consequences of the resulting cyber operation, which are a reduction of relative power of the targeted State and a relative increase of power of the State which is *in fact* but not also *in law* responsible for the unlawful power-maximising cyber operation. The utility of countermeasures proportional to the resulting cyber operation therefore stretches beyond inducing compliance with the due diligence obligations. It assures that the States responsible *in fact* but not also *in law*[140] for the internationally wrongful cyber operation, are indeed subjected to costs, the extent of which will match the power benefits born by the unlawful cyber operation and therefore render the selfish illegitimate power maximisation irrational.

All things considered, Estonian countermeasures inducing Russian compliance with the reparation and consequentially future compliance with the due diligence obligations of prevention and termination should be proportional with the initial violation and its effects.

---

[139] Council on Foreign Relations, 'Cyber Operations Tracker data' <https://www.cfr.org/interactive/cyber-operations/export-incidents?_format=csv> accessed 11 August 2019

[140] *See* ch 4

Whatever form the reactive breach of international obligations of Estonia, the important part is that their effects are quantitatively proportional with the effects of the non-diligent behaviour. But because Russian failure to take diligent measures of prevention and termination has occasioned a foreseeable internationally wrongful cyber operation, the State is also under the obligation of reparation for the effects of the denial of Estonian sovereign rights consequential to the non-diligent behaviour.

As already established, these effects materialised in a decrease of the economic and political power of Estonia[141] which the injured State may collect by way of quantitatively proportional countermeasures. By doing so, Estonia will proportionally reduce the power benefits gained by Russia, which is *in fact* responsible for the DDoS and thus render future non-compliance irrational.

5. Conclusion

This chapter elaborates which States can take countermeasures, which States can be targeted by countermeasures and when can they be taken. Additionally, it discusses the potential of proportional countermeasures against the non-diligent State to deter States *in fact* responsible for unlawful cyber operations from resorting to such wrongful maximisation of power in the future.

To this end, the chapter argues that countermeasures can only be taken by States directly or indirectly injured by the unlawful cyber operation, by States on behalf of the non-State actors under its jurisdiction whose international rights were infringed upon by the cyber operation in question and by third States with a vested interest in the preservation of the *erga omnes* oblations breached by the cyber operation.

The chapter also discusses which States can be targeted by countermeasures. Though there may be several States of emanation under the due diligence obligations of prevention and

[141] *See* ch 1

termination, this chapter only considers countermeasures against the State of origin. This is not only because the transit State is less likely to have actual or constructive knowledge of the operation but also because the infrastructure under the jurisdiction of a transit States may contribute only a portion of the cyber operation which may not be unlawful in itself. What is more, the context of the thesis is regarding States which are *in fact* responsible for the cyber operation and reap the benefits of it, which is not the case with the States of transit.

When countermeasures are conducted via cyber means, a spill-over of their consequences is likely; the chapter argues that such consequences are permissible as long as the primary target of instrumental countermeasures was the responsible state. In particular, the spill-over effect is not contentious when the State taking countermeasures has done its best to avoid them and has not used the infrastructure of other States as a means to an end.

Thirdly, the chapter elaborates the time frame of lawful countermeasures, argued against taking urgent countermeasures and discussed the ex-ante procedural obligations of the State taking countermeasures.

Lastly, the chapter discusses the lawfulness and effectiveness of countermeasures from the perspective of their proportionality. It argued that quantitatively proportional countermeasures will render the cost benefit calculation of the non-diligent behaviour as well as of the unlawful cyber operation irrational, and thus promote future compliance in general.

Chapter 7

Conclusion and the way ahead

This concluding chapter summarises the arguments made in this thesis and critically evaluates whether it has achieved the objectives set at the very beginning.

The first chapter of this thesis argued that cyber operations depriving States of their international legal rights, of their power and security, are frequent and on the rise for they are a power maximisation tool of selfish States in anarchical international relations.

States injured by these malicious cyber operations respond by increasing their institutional capacity to conduct and defend from such operations and by investing in new technologies enabling them to do so. States also seek a solution to the proliferation of cyber operations in developing and promoting the voluntary non-binding norms guiding international conduct in cyberspace. Be that as it may, the introductory chapter indicates that these solutions do not have any tangible effect on the quantity of malicious inter-State cyber operations.

For this reason, this thesis proceeded to investigate the ability of international law to supress the occurrence of malicious inter-State cyber operations and consequently increase peace and security.

Traditionally, international law provides peace and security by limiting the selfish maximisation of power of States in the anarchical world constellation. Nevertheless, international law can only perform this function when States comply with their international obligations. The investigation of this thesis is therefore centred on the compliance-inducing mechanisms of international law and its ability to reduce the present-day degree of non-compliance and thus provide nations with peace and security in the cyber era.

Since the prospect of a cyber-specific treaty legal regime is currently meagre, the thesis investigated the compliance-inducing powers of the established international law. It scrutinised the primary obligations of developing *lex specialis*, primary obligations of dynamically

interpreted and applicable rules of the established international law, as well as the secondary rules arising from the international legal responsibility of the States. Although it is acknowledged that international law itself cannot be a panacea for all cyber ills, nor is absolute compliance a realistic prospect, it is nonetheless hoped that the outcomes of the thesis will prove useful to injured States and encourage them to make use of the legal compliance inducing mechanisms and thus secure peace and strengthen security.

In addition to exposing the scale of the aforementioned problem and charting the investigation of a solution, the introductory chapter presented the methodological boundaries. Accordingly, it explained the limited scope of the research, which only considers unlawful inter-State cyber operations below the threshold of the use of force. What is more, the focus on inter-State cyber operations, the ones which target a State and are conducted or sponsored by a State, is dictated by their complexity and scale, making them the biggest threats to peace and security. The research avoided cyber operations amounting to the use of force due to a clear prevalence of operations short of causing physical damage and injury to human beings. The limited scope is further rationalised by the fact that much has been already written on the topic of the law of use of force in cyberspace. Three cyber operations – 2007 DDoS, Shamoon and RedOctober – were extensively analysed throughout the thesis. The first chapter concluded by proving they fit into the methodological framework and provides the reader with the relevant information surrounding the cyber incidents further analysed throughout this thesis.

In order to uncover a solution to non-compliance with the international law in cyber space, one has to understand the deeper issue at hand. This is the objective of **the second chapter** of the thesis, which lays down the theoretical foundation. In brief, the chapter establishes the main motivation of States in an anarchical world and asserts that States resort to unlawful cyber operations simply because non-compliance pays off.

Under the circumstances of anarchy in international relations, where no central power (enforcing entity) may be identified, States are drawn to seek security manifesting in absence internal or external threats to their survival. They do so, firstly, by maximising their power. In

particular, States seek to maximise their power resources, be it economic, military or diplomatic, generating security through either power projection or by being a deterrence.

Security is also attained by means of peace. In the pursuit of peace or absence of whatever commotion to sovereign life, States establish and uphold international law, embodying the restrictions on maximisation of power and promise of peace. As argued in the preceding chapter, the objective of international law has not altered with the introduction of the cyber operations into the international life and States still count on international law to provide peace.

Although States generally comply with international law, systemic and technological motives provide a strong temptation to resort to deviance. First, the limitations on power maximisation imposed by the law cannot be seen favourably by States concerned with their security. Second, under the conditions of anarchy trust in reciprocal compliance is fragile and States are further inclined to violate the law. The third reason is provided with the introduction of new technology. New technology, and particularly so the complex and invisible nature of cyber operations, enhances distrust between nations and distrust in reciprocal compliance, which is needed for the law to deliver peace.

Of course, States gravitate towards non-compliance when the benefits are unilateral. Accordingly, States seek a violation that will bring a quick and inexpensive maximisation of power resources, reduce the relative power and security of the adversary all the while keeping the protection of peace provided by the adversary's compliance with international law.

The temptation turns into actual violation when the benefits of non-compliance surpass the costs. Simply, non-compliance is rational when it pays off. States therefore resort to the maximisation of their security by way of unlawful cyber operations because the benefits clearly outweigh the costs associated with such conduct. Therefore, the extent and probability of facing costs play a pivotal role in the decision to comply or not with international law.

The second chapter established that the costs associated with an unlawful cyber operation are unlikely to be imposed, mostly due to limitations of technology. And when costs are

imposed on the non-compliant State, they are limited to reputational or other costs, which are significantly inferior to the substantial benefits reaped by the non-compliant State.

The power and security gains of the non-complying State are, however, a mirage. To make up for the lost power, and consequentially security, the State injured by a cyber operation will – in order to match the scope and speed of the unlawful relative power gains of the adversary – follow suit and seek power via unlawful means. If it proves to be rational, to pay off, they will repeat it. Others will take note and follow their deviant path. This leads to a spiral of conflict and the erosion of the rule of law, causing a reduction of security for every State.

Every State-conducted or -sponsored cyber operation in violation of its international obligations involves the international responsibility of that State. Responsibility is the central element of any binding normative order and corollary to the legal nature of its obligations. This led Crawford to argue that State responsibility is 'a cardinal institution of international law.'[1] **The third chapter** elaborates the role of the international law of State responsibility in inducing compliance of the rational States with their primary obligations under the conditions of anarchy. Being an antithesis to the preceding chapter, the third chapter exposed a lawful and feasible solution, with a notable potential to be effective in inducing the State responsible for an internationally wrongful cyber operation to comply with international law today and tomorrow.

Upon a breach of international obligations, and in accordance with the law of State responsibility, three secondary general obligations are imposed upon the wrongdoing State – the obligations of cessation, of non-repetition and of reparation. These obligations aim to induce compliance by the operation of law.

[1] James R Crawford, 'State Responsibility' in *Max Planck Encyclopedia of Public International Law* (September 2006) para 1 <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093?rskey=R5NNaq&result=1&prd=EPIL> accessed 13 August 2019

The first, the obligation of cessation, is merely a restatement of the primary obligation and reiteration of its obligatory nature. It requires the State responsible for an ongoing violation of international law to comply at will, to restore the levels of peace and security as they existed prior to the breach.

Although the obligation of non-repetition also seeks restoration of peace and security, it aims to assure compliance in the future. It is only relevant when an unlawful cyber operation has concluded and arises only when there is a significant risk of repetition. Due to the fact that unlawful cyber operations are easily repeated, guarantees of non-repetition should be demanded from the responsible States, particularly so from the ones with a prior history of resorting to unlawful cyber operations in their quest for inexpensive and quick power maximisation.

Assuring compliance in the future is the objective of the third secondary obligation, the obligation of reparation. Three forms of reparation are recognised by international law – restitution, compensation and satisfaction.

Restitution, the preferred method of reparation, requires the State in the wrong to re-establish the material situation that existed before the breach, or to re-establish the power balance between the nations. When restitution is not possible, which is often the case in cyber space, the responsible State is obliged to provide compensation, satisfaction or both. When damage is materially assessable – when a cyber operation causes the loss of economic power – the appropriate method of reparation is compensation, taking the form of repayment for the decrease in economic power with interests. Satisfaction, on the other hand, comes in the form of an apology or similar symbolic deed, amounting to a detriment to the international reputation of the responsible State.

Each of the forms of reparation are plagued with issues in the context of unlawful cyber operations. The specific nature of cyberspace inhibits the ability of restitution to actually restore the power relationship between the parties prior to the conflict; compensation is only

successful in inflating the costs of the wrongdoer when the unlawful cyber operation inflicts a relative decrease in economic power of the targeted State; and, restitution or the self-inflicted reduction of international standing of a responsible State, as already mentioned, is not sufficient to alter the cost benefit analysis of the selfish States and to render non-compliance irrational. As a matter of fact, all secondary obligations assume the wrongdoing State's admission of responsibility for the unlawful cyber operation, which has not been publicly recorded to date.

For the above reasons, the injured State seeking to induce compliance of the wrongdoing State should direct its attention towards various mechanisms offered by the international law (of State responsibility). The third chapter first considers the possibilities of international adjudication and multilateral sanctions which both indeed inflict undesired deprivation of power on the State responsible for a breach of its international obligations and thus counterbalance the benefits of non-compliance. However, political considerations of the heterogeneous international community and the expected unwillingness of the wrongdoing State to agree to the jurisdiction of the ICJ, for example, hinders the effectiveness of these two mechanisms in bringing the wrongdoing State to comply with its obligations.

The State, deprived of its legal rights by an unlawful cyber operation, should therefore resort to lawful measures of self-help. As shown in the chapter three, retorsion, a form of unfriendly actions not in contravention to the international obligations of the injured State, cannot be considered an effective compliance inducing mechanism. Similar to reparation by way of satisfaction, public protest, being the most prevalent form of retorsion, only affects the international reputation of the wrongdoer and is not effective in inducing the rational State to comply with its international obligations. At least not in the context of unlawful cyber operations.

For this reason, the third chapter took a closer look at the self-help mechanism of countermeasures, which not only deliver a proportional deprivation of power and therefore restore the prior power relationship but also do not depend on consent from the responsible

party or the international community to do so. To be lawful and effective in inducing compliance with international law, countermeasures must be qualitatively and quantitatively proportional with the initial wrongdoing. While lessons from the jurisprudence indicate the former is of supreme importance when assessing their lawfulness, the quantitative proportionality is the one which guarantees countermeasures will inflate the costs of the wrongdoing State to the point of restoration of power and security relationship, thus effectively rendering the non-compliance irrational. If employed regularly, countermeasures will also assume the role of a deterrent and discourage the rational States from resorting to unlawful cyber operations in the future.

Before proportional countermeasures are employed, the injured State must legally attribute the unlawful cyber operation to a State. **The fourth chapter** exposed the reasons behind the inability of the injured State to do so.

Attribution, the core of the international law of State responsibility, requires the injured party of the inter-State cyber conflict to identify the authors of the unlawful conduct as well as establish their association with a particular perpetrating State.

In its first task – assigning authorship to a particular natural person – the State wishing to employ countermeasures must identify the computer or network of origin which leads to the natural person utilising it in order to launch a cyber operation against a foreign nation. Indeed, this may be a tedious task, plagued with unreliability of the conclusions stemming from the nature of the Internet protocols, but not an impossible one. What will, in all likelihood, be impossible is to successfully identify the natural person using said equipment for the perpetration of the internationally wrongful cyber operation as this would involve the use of forensic methods, which are rather ineffective when not deployed locally.

The second issue with establishing attribution is related to establishing a nexus between the cyber perpetrators and a State. Once the natural person responsible for a cyber operation is identified, the State wishing to invoke State responsibility and employ countermeasures must

be able to establish an association of the author with a particular State. In accordance with the international law of State responsibility, the unlawful act is attributed to the State when conducted by a *de facto* or *de jure* State organ. Specifically, attribution to the State is established if the unlawful act was found to have been perpetrated by an actor which is designated as organ of the State by the relevant domestic legislation or when the actor is found to be operationally assimilated with or dependently acting on behalf of a State. Other forms of relationship between the perpetrators and the State permit attribution; when the authors of an unlawful cyber operation operate under the instructions, directions or effective control of a State, that act is legally attributed to that State. Actors allegedly orchestrating the Shamoon and 2007 DDoS attacks and the lack of information connecting them to a State exemplify the issues injured parties have when trying to establish attribution to a State, even when the actors behind the operation are known. Specifically, it cannot be legally established that Nashi, the author of the 2007 DDoS, is a *de facto* or *de jure* organ of the State, or that it acted under the directions, instructions or effective control of Russia. Similarly, the orchestrating organisation of the Shamoon operation cannot be connected to Iran, which is allegedly *in fact* responsible for the operation.

The biggest issue with attribution is that the burden of proof lies on the injured State, which needs to be ready to provide sufficiently clear and convincing, direct evidence before State responsibility is invoked and countermeasures are employed. Specifically, the fourth chapter argued for a self-imposed high standard of proof, in order to, *inter alia*, prevent escalation following the employment of countermeasures. Since the focus of this thesis is the responsibility of States, I argued that the third standard of sufficiently clear and convincing proof would be appropriate in establishing the attribution of a cyber operation to a State. The standard is supported by not only the international jurisprudence related to the State responsibility but also by several expressions of *opinio juris* specifically addressing the issue of standard of proof in the context of inter-State cyber operations.

Another potential issue with the evidence required for attributing the cyber operation to a State is related to the legally permitted types of evidence. Direct evidence is likely to be unavailable to the injured State due to the aforementioned technical difficulties. Circumstantial evidence, on the other hand, is only acceptable in situations when no rebuttal is provided by the accused State or to prove the knowledge of the State of a cyber operation. Indeed, circumstantial evidence and deduction prove with sufficient certainty that Russia knew of the 2007 cyber operation, for example. But since Russia rejected the responsibility, the cyber operation in question cannot be attributed to it by means of circumstantial evidence.

Forms of evidence, ordinarily referred to by politicians when making claims about the attribution of cyber operations to a particular State, also prove problematic from the standpoint of international law. Although legitimate, digital forms of evidence can be easily falsified and should thus be corroborated with other evidence. Similar can be claimed about newspapers, which standing on their own, according to jurisprudence related to State responsibility, cannot be sufficient to establish attribution.

Since States have previously relied on evidence provided by the private actors when making claims of attribution of cyber operations, the fourth chapter analysed the suitability of such forms of evidence in the process of legal attribution. Although jurisprudence indicates that evidence provided by private actors may be used for the purpose of attribution, caution must be exercised. Private actors rely on a combination of technical and socio-political methods of attribution and their claims have no political or legal repercussions if a State is wrongly accused. States invoking international responsibly on the basis of such claims, on the other hand, risk employing unlawful countermeasures if evidence provided by a non-State entity is not verified and turns out to be simply wrong.

Due to the issues with attribution and the consequential inability to employ countermeasures and thus increase the cost of the rational perpetrating State, the party injured by the unlawful cyber operation should rethink the unlawful character of the cyber operation. This is the subject matter elaborated in **the fifth chapter** of the thesis.

To this end, the chapter investigated the well-established legal principle of due diligence and the corresponding international obligations, requiring States to do their utmost to prevent and terminate acts stemming from their territories which are in contravention with the international rights of other States.

The investigation of due diligence is rationalised by the premise that every State sponsoring or conducting an unlawful cyber operation is also in violation of the due diligence obligations of prevention and termination. Both the due diligence principle, as well as the resulting obligations, are recognised by the international customary law and international jurisprudence. Most importantly, due diligence and the obligations of prevention and termination are recognised by many States in the context of cyber operations.

International legal doctrine indicates that due diligence requires proactive posture even before the occurrence of a cyber operation that deprives the other States of their international rights. Accordingly, due diligence requires States to develop the capacity to prevent and terminate an unlawful act and to discharge the said capacity when circumstances demand so.

A State is considered to have violated due diligence obligations only when it has failed to act diligently in its prevention and termination efforts of an unlawful cyber operation of which it knew or should have known. Even when the actual knowledge of the emanating unlawful cyber operation is absent, States are considered to be in violation of their international due diligence obligations when they possess constructive knowledge. The existence of the latter is determined on the basis of the test devised by the ICJ in the Corfu Channel Case and adopted by this thesis. Accordingly, the State should have known of the emanating unlawful cyber operation if it is established that it ordinarily monitors cyber infrastructure on its territory and that it has the theoretical capacity to spot the operation in question.

Due diligence obligations are obligations of conduct and not of result, which means the pertaining legal standards are flexible. These obligations dictate the employment of best efforts to achieve prevention and termination but impose no obligation to actually prevent and

terminate the unlawful act. Although the due diligence standard depends on the capacity of the State and the circumstances of the unlawful act, States should conform to the international minimum standards at all times.

The fifth chapter further detailed the due diligence obligations in cyberspace and indicates the possible international minimum standards related to the due diligence obligations of prevention and termination in cyberspace. Specifically, it outlined the areas which a diligent State could address if it genuinely wished to develop and to discharge the capacity to prevent and terminate a cyber operation emanating from its territory. It also presented the international minimum standard of due diligence obligations of prevention and termination, which requires States to have a national cybersecurity strategy, enact and enforce national cybersecurity legislation enabling it to diligently prevent and terminate, establish a national CERT as well as engage in international cooperation on matters related to cybersecurity. In addition to these minimum legal standards related to capacity development, States must also at least warn the targeted State of an incoming the unlawful cyber operation.

The benefit of invoking the State responsibility for the omission of diligence in termination and prevention efforts related to the emanating unlawful cyber operation (as opposed to the State responsibility for the conduct of the said cyber operation) lies in the fact that the former can in fact be proven despite of limitations of technology. Firstly, although proof of territorial origin of the cyber operation must still be sufficiently convincing and the relevant evidence may still be plagued by unreliability, evidence of the territorial origin of a cyber operation is more likely to be available to the injured State than evidence pointing at the natural person conducting the cyber operation and its connection with the State for the purpose of invoking State responsibility. Secondly, sufficiently clear proof of the knowledge of the emanating unlawful cyber operation may be established by way of circumstantial evidence. This is important since circumstantial evidence has, historically speaking, not been permitted in establishing the attribution of the unlawful act itself. Thirdly, proving the lack of due diligence should also be an achievable task for the injured State; the cybersecurity capacity enabling a State to prevent

and terminate the operation is a matter of public information while the questions of whether the injured State was warned or whether its termination efforts were aided by the State of emanation, can easily be answered by the former.

The sixth chapter applied and tested the theory developed in the previous chapters. It explained who under international law is entitled to induce compliance by way of countermeasures and against whom countermeasures can be taken.

Specifically, the chapter argues that countermeasures precluded from wrongfulness under the law of State responsibility may only be taken by the State whose international rights were directly or indirectly violated by another State's failure to diligently prevent or terminate a cyber operation. In the event of a multitude of injured States, each of them is entitled to take countermeasures against the internationally responsible State.

While countermeasures may only be aimed at the latter, the instrumentality of the reactive and lawful deprivation of the responsible party of its legal rights can be achieved indirectly by targeting the non-State actors under its jurisdiction. Be that as it may, countermeasures must not utilise the infrastructure of the third, innocent State and by doing so deprive it of its international legal rights in order to achieve compliance of the responsible State.

Considering the legal nature of due diligence obligations, injured States can only take countermeasures against the non-diligent State which knew or should have known of the internationally wrongful cyber operation. Additionally, it can only take countermeasures against the State whose territory has been successfully established as the origin of the cyber operation occasioned by the omission of diligent prevention and termination.

To investigate the theoretical arguments made in the preceding chapters and substantiate the utility of invoking the responsibility of a State for its failure to diligently prevent and terminate instead of responsibility for the unlawful conduct of cyber operations, I further examined the 2007 DDoS operation against Estonia. Accordingly, I provided evidence proving that the aforementioned cyber operation originated from cyber infrastructure under the territorial

jurisdiction of the Russian Federation. I also explain why Russia should have known of the internationally wrongful cyber operation and why it failed to comply with its due diligence obligation of termination. All things considered, Estonia could have taken countermeasures against Russia, because the latter failed to exhibit due diligence in prevention or termination efforts related to the 2007 cyber operation. The operation, of which Russia should have known, emanated from the cyber infrastructure located on the territory under its territorial jurisdiction.

The chapter also elaborated procedural conditions and temporal considerations related to countermeasures for the lack of diligence in prevention and termination efforts in the context of unlawful inter-State cyber operations below the use of force. Specifically, the instrumentality and the non-punitive character of countermeasures must be communicated with the targeted State to avoid escalation and erosion of the normative order. States injured by a cyber operation occasioned by non-diligent behaviour must therefore invite the responsible State to comply with its international obligations and, in the case of continuing violation, communicate the intention to take countermeasures before these are taken. Although the latter condition can be rightfully omitted in the case of taking urgent countermeasures, the chapter made a clear case against them.

Intended to secure compliance of the internationally responsible State, countermeasures are to be employed only during the period of its non-compliance with the secondary obligations stemming from the international law of State responsibility and should be promptly discontinued as soon as compliance and thus power level is restored. Specifically, the injured State can induce the obligation of cessation by way of countermeasures once the unlawful cyber operation which the responsible State was required to terminate or prevent occurs. These countermeasures should be dismissed as soon as the cyber operation concludes.

Countermeasures intended to induce compliance with the obligations of non-repetition and reparation, however, can be taken for as long as the promises of non-repetition and reparation in full are outstanding. Note that this does not mean that the injured State is allowed to wait

indefinitely before taking countermeasures, which should generally be taken without undue delay.

In its third section, the chapter explained how can countermeasures induce compliance not only with the obligations of due diligence but also with the obligations breached by the cyber operation occasioned by the lack of diligence. Accordingly, irrespective of their form, countermeasures must be quantitatively proportional with the material injury consequential to the cyber operation occasioned by the non-diligent behaviour.

The aim of the present thesis was to investigate the theoretical capacity of the established international legal mechanisms to supress the present-day degree of non-compliance with the international law in cyberspace. All things considered, I have shown that countermeasures based on the State responsibility for the non-diligent prevention and termination of the cyber operation can be used by the injured States to lawfully inflate the costs of the State *in fact* responsible for the unlawful cyber operation, thus removing the main reason fuelling the rational choice of non-compliance. The elaborated compliance inducing methodology based on the legal responsibility for the non-diligent behaviour in cyber space indeed gives the injured States the ability to not only restore individual peace and security but also to reinforce the rule of law in cyberspace, consequentially contributing to an increase in peace and security for all States.

Invoking State responsibility for the non-diligent behaviour in cyberspace and, on the basis of that, taking countermeasures against the States *in fact* responsible for the cyber operations is important particularly in the context of hurdles preventing a successful attribution in accordance with the established standards part of the international law of State responsibility.

Whether the presented solution is indeed satisfactory and has a potential to realistically minimise the proliferation of the internationally wrongful cyber operations can be answered affirmatively only in part. Relying on the responsibility for the violation of the obligations of due

diligence is not the panacea for all temptations of inexpensive and rapid State power inflations offered by cyber operations.

Perpetual technological advancement of malicious cyber operations will undoubtedly continue to allow States to seek illegitimate but quick and inexpensive maximisation of their relative power resources. As indicated in this thesis, the principle of due diligence and the corresponding obligations of prevention and termination can alleviate this issue and allow the States to induce compliance of the selfish power maximisers but will certainly not completely remove the temptation of unilateral non-compliance.

Technology is also a limitation to the application of the solution proposed by this thesis. As explained in chapter six, I have focused only on States of origin and not the States of transit. And although I have claimed that establishing and proving the origin of a cyber operation is a more feasible task than attributing a cyber operation to a particular State, technology remains a limitation. Examples were given where the State of origin is unknown. Other examples were provided where neither the State of origin nor the State of transit were known.

By investigating the issue of compliance with international law in the context of cyber operations below the use of force, I have addressed the literature gap. This is not to say that the doctoral thesis, proposing a solution to the proliferation of unlawful inter-State cyber operations below the use of force, will in fact have any positive effect on international peace and security. To achieve this, the proposed compliance-inducing legal mechanisms must be utilised. Only when the power-hungry, rational States comply with their obligations also in cyberspace, international law will perform its function to provide peace and security.

Primarily, the presented legal mechanisms should be utilised by the States deprived of their international legal rights by the cyber operation. I am of a firm conviction that international law can still perform its function in the cyber era – that is to provide peace and security – as long as States do not lose faith in its ability to deliver. In the anarchical world and in the absence

of a central enforcement entity, it is up to the (injured) States to stand up to the wrongdoers, employ measures of self-help and induce compliance with international law.

The first step towards this should be an explicit recognition of the due diligence obligations in cyber space, reaffirming their status in the international law applicable in the digital domain. This should be followed by countermeasures, which will proportionally reduce the relative power gains of the wrongdoing State and thus compel it to cease with the wrongdoing cyber operation and to refrain from conducting or sponsoring one in the future. It will also send a clear message to the rest of the international community that unlawful power maximisation by way of cyber operations is not a rational choice in their pursuit of security. As noted in the initial chapter of the thesis, I hope States will find utility in this thesis. I wish the injured States would take notice of the law and feel empowered to act.

Caution is however advised as international law applicable to cyber operations is still under development. As indicated, primary rules, such as sovereignty, are still questioned by some States, for example. Also, despite a clear indication of the existence of the due diligence obligations of prevention and termination in cyberspace, some States remain fearful of the requirements such obligations may impose on them. And because an international minimum standard of diligence depends on the state of technology and its price or availability, it certainly will change as time goes on.

Due to the politicised efforts to establish a new cyber specific treaty, the aforementioned development of the law will most certainly be achieved through State practice and *opinio juris*. This does not mean that States are the only drivers of normative progress, as some would like us to believe. Scholarship is an important force behind the normative development of the international rules applicable to cyberspace. The topics legal scholars should thus further investigate include the questions of sovereignty in cyberspace, the content and standards of due diligence in cyberspace, the obligations of transit States, and the issues of causation, particularly the qualification of the remoteness of the material injury and similar.

Table of primary sources

(Inter)national cases

Affaire Du Lac Lanoux [1957] XII UNRIAA

Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo) (Merits) [2010] ICJ Rep

Air Service Agreement of 27 March 1946 between the United States of America and France [1978] XVIII UNRIAA

Al-Skeini v UK [2011] ECtHR 55721/07

Alabama case (United States of America v Great Britain) (decision of 14 September 1872) *in* J B Moore, *History and Digest of the International Arbitrations to which the United States has been a Party* (vol I, GPO 1898)

Alabama Claims of the United States of America Against Great Britain [1871] XXIX UNRIAA

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment) [2007] ICJ Rep

Application of the Interim Accord of 13 September 1995 (The Former Yugoslav Republic of Macedonia v Greece) [2011] ICJ Rep

Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) [1964] ICJ Rep

Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) (separate opinion of Judge Bustamante) [1964] ICJ Rep

Biwater Gauff (Tanzania) Ltd. v. United Republic of Tanzania (Award) ICSID Case No. ARB/05/22

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) [2005] ICJ Rep

Case Concerning East Timor (Portugal v Australia) [1995] ICJ Rep

Case Concerning Gabčíkovo-Nagymaros Project (Hungary v Slovakia) [1997] ICJ Rep

Case of Velásquez-Rodríguez v Honduras (Reparations and Costs) [1989] (Judgment of 21 July 1989) Inter-American Court of Human Rights

Certain Phosphate Lands in Nauru (Nauru v. Australia) - Preliminary objections [1992] ICJ Rep

Charles S. Stephens and Bowman Stephens (U.S.A.) v United Mexican States [1927] IV UNRIAA

Chorzów Factory Case (Germany v Poland) (Merits) [1928] PCIJ Rep Ser A, No 17

Claim of the Salvador Commercial Company ("El Triunfo Company") [1902] X UNRIAA

Combuslion Engineering, Inc., et al and The Islamic Republic of Iran, et al [1991] (Partial Award No 506-308-2) 26 Iran-US CTR

Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania) (Merits) [9 April 1949] ICJ Rep

Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania) (Individual Opinion of Judge Alvarez) [9 April 1949] ICJ Rep

D. Earnshaw and Others (Great Britain) v United States [1925] VI UNRIAA

Danfoss A/S and Sauer–Danfoss ApS v Skatteministeriet [2011] CJEU Rep 2011 I-09963

Federal Republic of Germany et al vs. United States et al, 526 U.S. 111

Flexi-Van Leasing, Inc. v Islamic Republic of Iran [1982] Iran-US CTR

Gabčíkovo-Nagymaros Project (Hunngary/Slovakia) [1997] ICJ Rep

Handyside v the United Kingdom, no. 5493/72 (7 December 1976) ECHR

Hyatt International Corporation v The Government of the Islamic Republic of Iran [1985] 9 Iran-US CTR

In re Eastern Transportation Co. (The T.J. Hooper), 60 F.2d 737 (2d Cir. 1932) Judge Learned Hand

Island of Palmas Arbitration (Netherlands v US) [1928] II UNRIAA

Kenneth P. Yeager v The Islamic Republic of Iran [1987] 17 Iran-US CTR

L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States [1926] IV UNRIAA

LaGrand (Germany v United States of America) (Merits) [2001] ICJ Rep

Libyan American Oil Company (LIAMCO) v Government of the Libyan Arab Republic [1982] 62 ILR

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep

Miller v Minister of Pensions [1947] 2 AII ER

Mixed Claims Commission (United States and Germany) (Opinion in the Lusitania Cases) [1923] VII UNRIAA (No. 1956.V.5)

Monetary Gold Removed from Rome in 1943 (Italy v France, United Kingdom of Great Britain and Northern Ireland and United States of America) (Judgment) [1954] ICJ Rep

Naulilaa Arbitration (Portugal v Germany) [1928] II UNRIAA (Sales No. 1949.V.1)

Noble Ventures, Inc. v Romania, Case No ARB/01/11 (award) ICSID (12 October 2005)

North Sea Continental Shelf Cases (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) (Judgment of 20 February 1969) [1969] ICJ Rep

Oil Platforms (Islamic Republic of Iran v United States of America) (Separate Opinion of Judge Higgins) [2003] ICJ Rep

Oil Platforms (Islamic Republic of Iran v. United States of America) [2003] ICJ Rep

Plattform “Ärzte für das Leben”’ v Austria App No 10126/82 (ECHR 21 June 1988)

Portugal v. Germany (The Cysne) 5 ILR

Prisoners of War–Eritrea’s Claim 17 (Ethiopia v Eritrea) [2003] (Partial Award), XXVI UNRIAA

Prosecutor v Bagosora (Trial Judgment and Appeals Judgment) [1998] ICTR-98-41-T

Prosecutor v Duško Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995)

Prosecutor v Karemera et al (Decision on Prosecutor's Motion for Admission of Certain Exhibits into Evidence) [2008] ICTR-98-44-T (25 January 2008)

Prosecutor v Naser Orić (Trial judgment) [2006] ICTY IT-03-68-T (30 June 2006)

Pulp Mills on the River Uruguay (Argentina v Uruguay) [2010] ICJ Rep

R v B [2003] 2 Cr. App. R. 13 Lord Woolf CJ

R v Swaysland [1987] BTLC

Rainbow Warrior (New Zealand v France) [1990] XX UNRIAA

Ribitsch v Austria App No 18896/91 (ECHR 4 December 1995)

Schering Corporation and The Islamic Republic of Iran [1984] 5 Iran-US CTR

Spanish Zone of Morocco (Great Britain v Spain) [1924] II UNRIAA

The Cysne Arbitration (Portugal v Germany) [1930] II UNRIAA (Sales No. 1949.V.1)

The MOX Plant Case (Ireland v United Kingdom) (Separate Opinion of Judge Mensah) [2001] ITLOS

Trail smelter case (United States v Canada) [1938 and 1941] III UNRIAA

United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) [1980] ICJ Rep

US v Ahmad Fathi et al, No 1:16-cr-00048 (South D New York 21 January 2016) <https://www.justice.gov/opa/file/834996/download> accessed 1 July 2019

US v Wang Dong et al (Indictment, No. 14–118 W.D. Pa., 1 May 2014) <https://goo.gl/RHm0Fh> accessed 1 April 2016

Vienna Convention on Consular Relations (Paraguay v United States of America) (Request for the Indication of Provisional Measures, Order of 9 April 1998) [1998] ICJ Rep

William E. Chapman (U.S.A.) v United Mexican States [1930] IV UNRIAA

Treaties and other international agreements

Agreement Between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (unofficial translation, 16 June 2009) <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf> accessed 7 January 2018

Charter of the United Nations (San Francisco, 26 June 1945)

Convention on Cybercrime (23 November 2001, entered into force 1 July 2014) ETS 185

Convention on the Law of the Non-Navigational Uses of International Watercourses (New York, 21 May 1997)

Declaration of the UN Conference on Environment and Development (Rio de Janeiro, 14 June 1992) UN Doc A/CONF.48/14

Framework Convention on Climate Change (Rio de Janeiro, 9 May 1992, 31 ILM 851)

International Covenant on Civil and Political Rights (UNGA Res 2200A (XXI), 16 December 1966)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (Geneva, 8 June 1977)

United Nations Convention on the Law of the Sea (Montego Bay, 10 December 1982)

Vienna Convention for the Protection of the Ozone Layer (Vienna, 22 March 1985)

Vienna Convention on Diplomatic Relations (18 April 1961) 500 UNTS 95

Vienna Convention on the Law of Treaties (Vienna, 23 May 1969) 1155 UNTS

Resolutions, opinions and other documents of international organisations

— 'Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.3: Concept Framework' (Version 3.0, 3 October 2012) [on file with the author]

Advisory Opinion No. 4 (advisory opinion) [1923] PCIJ Rep Series B <http://www.icj-cij.org/pcij/serie_B/B_04/Decrets_de_nationalite_promulgues_en_Tunisie_et_au_Maroc_Avis_consultatif_1.pdf> accessed 1 May 2019

Council of Europe, 'International and multi-stakeholder co-operation on cross-border Internet' (Directorate General of Human Rights and Legal Affairs, 2010)

Council of Europe, Opinion on "Whether Draft Federal constitutional Law No. 462741-6 on amending the Federal constitutional Law of the Russian Federation on the procedure of admission to the Russian Federation and creation of a new subject within the Russian Federation is compatible with international law" endorsed by the Venice Commission at its 98th Plenary Session' (CDL-AD(2014)004-e, Venice, 21-22 March 2014) <http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2014)004-e> accessed 1 July 2019

Council of the European Union, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption' (Brussels, 7 June 2017) 9916/17 <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> accessed 17 May 2019

Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (Advisory opinion) [1999] ICJ Rep

European Commission, ‘Client and Supplier Countries of the EU28 in Merchandise Trade’ (Trade-G-2, 21 September 2018) <trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf> accessed 24 February 2019

European Commission, ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’ (13 September 2017) JOIN(2017) 450 final

European Commission, Communication from the Commission on the precautionary principle (COM/2000/0001 final, 2 February 2000)

European External Action Service, ‘EU sanctions against Russia over Ukraine crisis’ (European Union Newsroom, 10 March 2016) <https://europa.eu/newsroom/highlights/special-coverage/eu-sanctions-against-russia-over-ukraine-crisis_en> accessed 1 July 2019

European Parliament, ‘Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU’ (2017) EPRS/STOA/SER/16/214N

ILC, ‘Addendum - Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur the internationally wrongful act of the State, source of international responsibility (part 1)’ (1980) II(I) Ybk of the ILC UN Doc A/CN.4/318/Add.5–7

ILC, ‘Document A/9010/Rev.1: Report of the International Law Commission on the work of its twenty-fifth session (7 May- 13 July 1973)’ (1973) II Ybk of the ILC UN Doc A/CN.4/SER.A/1973/Add.l

ILC, ‘Draft Articles on State Responsibility with Commentaries Thereto’ (adopted by the ILC on the first reading, January 1997) UN Doc 97-02583

ILC, ‘Draft articles on Succession of States in respect of State Property, Archives and Debts with commentaries’ (1981) II(II) Ybk of the ILC

ILC, ‘Draft articles on the law of the non-navigational uses of international watercourses and commentaries thereto and resolution on transboundary confined groundwater’ Ybk of the ILC (1994) II(2)

ILC, ‘Draft articles on the law of treaties’ (1966) II Ybk of the ILC UN Doc A/CN.4/SER. A/1966/Add. 1

ILC, ‘Draft Articles on the Protection of Persons in the Event of Disasters, with commentaries’ (2016) II(2) Ybk of the ILC, UN Doc A/71/10

ILC, ‘Draft articles on the responsibility of international organisations, with commentaries 2011’ (2011) II(2) Ybk of the ILC UN Doc A/CN.4/SER.A/2011/Add.1 (Part 2)

ILC, ‘Eighth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur. The internationally wrongful act of the State, source of international responsibility (continued)’ (1979) II(1) Ybk of the ILC UN Doc A/CN.4/SERA/1979/Add.l (Part 1)

ILC, ‘First report on State responsibility, by Mr. James Crawford, Special Rapporteur’ UN Doc A/CN.4/490 and Add. 1–7

ILC, ‘Fourth report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur’ (1992) ILC Ybk II(1) UN Doc A/CN.4/444 and Add.1–3

ILC, ‘Fourth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility (continued)’ (1972) II Ybk of the ILC UN Doc A/CN.4/SER.A/1972/Add.1

ILC, ‘International Liability for Injurious Consequences Arising out of Acts not Prohibited by International Law (Prevention of Transboundary Harm from Hazardous Activities)’ (2001) II (Part Two) Ybk of the ILC, UN Doc A/CN.4/SER.A/2001/Add.1 (Part 2)

ILC, ‘International liability for injurious consequences arising out of acts not prohibited by international law’ (1996) II(1) Ybk of the ILC UN Doc A/CN.4/SER.A/1996/Add.1 (Part 1)

ILC, ‘Materials on the Responsibility of States for Internationally Wrongful Acts’ (UN Legislative Series, 2012) UN Doc ST/LEG/SER B/25

ILC, ‘Report of the Commission to the General Assembly on the work of its forty-sixth session’ (1994) 2(II) Ybk of the ILC 103 citing Restatement of the Law, Third, Foreign Relations Law of the United States, vol. 2 (St. Paul, Minn., American Law Institute Publishers 1987)

ILC, ‘Report of the International Law Commission on the work of its fifty-second session (1 May–9 June and 10 July–18 August 2000)’ (2000) II(2) Ybk of the ILC UN Doc A/CN.4/SER.A/2000/Add.1 (Part 2)/Rev.1

ILC, ‘Report of the International Law Commission on the work of its forty-seventh session (2 May-21 July 1995)’ (1995) II(2) UN Doc A/CN.4/SER.A/1995/Add.l (Part 2)

ILC, ‘Report of the International Law Commission: Sixty-fifth session’ (6 May–7 June and 8 July–9 August 2013) UN Doc A/68/10

ILC, ‘Report on International Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur’ (1956) II Ybk of the ILC UN Doc A/CN.4/96

ILC, ‘Second Report on International Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur’ (1957) II Ybk of the ILC, UN Doc A/CN.4/106

ILC, ‘Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur’ (1989) II(1) Ybk of the ILC UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1

ILC, ‘Second report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The origin of international responsibility’ (1970) II Ybk of the ILC, UN Doc A/CN.4/SER.A/1970/Add.1

ILC, ‘Second report on the status of the diplomatic courier and the diplomatic bag not accompanied by diplomatic courier, by Mr. Alexander Yankov, Special Rapporteur’ (1981) II(1) Ybk of the ILC UN Doc A/CN.4/347 and Corr.1 & 2 and Add.1 & 2

ILC, ‘Sixth report on the content, forms and degrees of international responsibility (part two of the draft articles) and "Implementation" (mise en oeuvre) of international responsibility and the settlement of disputes (part three of the draft articles), by Willem Riphagen, Special Rapporteur’ (1985) II(1) Ybk of the ILC UN Doc A/CN.4/389 and Corr.1 & Corr.2

ILC, ‘State responsibility (concluded) Draft articles proposed by the Drafting Committee on second reading’ (2000) I Ybk of the ILC UN Doc A/CN.4/SER.A/2000

ILC, ‘Summary record of the 2899th meeting’ (10 August 2006) UN Doc A/CN.4/SR.2899

ILC, ‘The law of the non-navigational uses of international watercourses’ (1994) II(2) Ybk of the ILC UN Doc A/CN.4/SER.A/1994/Add.l (Part2)

ILC, ‘Third report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility’ (1971) II(1) Ybk of the ILC UN Doc A/CN.4/SER.A/1971/Ad(U (Part 1)

International Telecommunication Union Telecommunication Development Bureau Focal Point for Question 3/2, ‘Global Cybersecurity Index – Reference Model’ (Second Meeting of ITU D Study Group 2, Document 2/164 E, 22 July 2015)

International Telecommunication Union, ‘Cyberwellness Profile Russian Federation’ (22 January 2015) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Russia.pdf> accessed 13 August 2019

International Telecommunication Union, ‘Final Acts of the Plenipotentiary Conference (Guadalajara, 2010)’ (2011)

International Telecommunication Union, ‘Global Cybersecurity Index & Cyberwellness Profiles’ (2015)

International Telecommunication Union, ‘ITU Global Cybersecurity Index (GCI) 2018’ (2018) <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf> accessed 11 August 2019

International Telecommunication Union, ‘National CIRTs world-wide’ <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf> accessed 7 January 2018

International Telecommunication Union, ‘National Strategies Repository’ <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx> accessed 7 January 2018

International Telecommunication Union, ‘Resolution 45 (Rev. Dubai, 2014) – Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam’ (The World Telecommunication Development Conference 2014)

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Advisory Opinion) 34 [2011] ITLOS Rep

Statute of the International Atomic Energy Agency (New York, 23 October 1956)

Statute of the International Court of Justice (San Francisco, 24 October 1945)

UN GAOR 1st Committee (71st Session) ‘Thematic discussion on specific subjects and introduction and consideration of draft resolutions and decisions submitted under all disarmament and related international security agenda items’ (24 October 2016) 15 UN Doc A/C.1/71/PV.19

UN Human Rights Commision, ‘Womah Mukong v Cameroon’ (Communication No 458/1991, 1994) UN Doc CCPR/C/51/D/458/1991

UN Human Rights Office of the High Commissioner, ‘The Corporate Responsibility to Respect Human Rights: An Interpretive Guide’ (HR/PUB/12/02, 2012) <https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf>

UN, ‘The Secretary-General's remarks at opening of 72nd session of the General Assembly’ (New York, 12 September 2017) <un.org/sg/en/content/sg/statement/2017-09-12/secretary-generals-remarks-opening-72nd-session-general-assembly> accessed 12 August 2019

UNGA ‘Developments in the field of information and telecommunications in the context of international security’ (9 September 2013) UN Doc A/68/156/Add.1

UNGA ‘Developments in the field of information and telecommunications in the context of international security’ (19 July 2016) UN Doc A/71/172

UNGA ‘Developments in the field of information and telecommunications in the context of international security’ (11 August 2017) UN Doc A/72/315

UNGA ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) UN Doc A/68/98

UNGA ‘Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General’ (14 September 2011) UN Doc A/66/359

UNGA ‘Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General’ (13 January 2015) UN Doc A/69/723

UNGA ‘Potential Security Impacts of Cyberspace Misuse Considered in First Committee, as Speakers Warn of Arms Race, Emergence of New Theatre of Warfare’ (30 October 2015) UN Doc GA/DIS/3537 <https://www.un.org/press/en/2015/gadis3537.doc.htm> accessed 4 June 2019

UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (22 July 2015) UN Doc A/70/174

UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) UN Doc A/68/98

UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (30 July 2010) UN Doc A/65/201

UNGA ‘Report of the Secretary-General Pursuant to General Assembly Resolution 53/35 – The Fall of Srebrenica’ (15 November 1999) UN Doc A/54/549

UNGA ‘Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-operation among States’ (16 November 1964) 19th Sess, UN Doc A/5746

UNGA Res 1514 (XV) (14 December 1960) UN Doc A/RES/1514

UNGA Res 2222 (XXI) (19 December 1966)

UNGA Res 25/2625 (24 October 1970) UN Doc A/RES/25/2625

UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/2625(XXV)

UNGA Res 55/63 (22 January 2001) UN Doc A/RES/55/63

UNGA Res 56/83 ‘Responsibility of States for Internationally Wrongful Acts’ (12 December 2001) UN Doc A/RES/56/83

UNGA Res 69/283 (23 June 2015) UN Doc A/RES/69/283

UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237

UNGA Res 799 (7 December 1953) UN Doc A/RES/799(VIII)

United Nations Conference on International Organisation, ‘Commission 1, general provisions’ (San Francisco, 1945)

United Nations Office for Disaster Risk Reduction, ‘2009 UNISDR Terminology on Disaster Risk Reduction’ (May 2009)

United Nations Office on Drugs and Crime, ‘Cybercrime Repository – Database of Legislation’ (UNODC) <https://www.unodc.org/cld/v3/cybrepo/legdb/search.html?lng=en> accessed 7 January 2018

UNSC Verbatim Record (11 & 13 January 1980) UN Doc S/PV.2191

Domestic legislations and other regulatory instruments

31A C.J.S. Evidence para 8 (1964)

Advance Fee Fraud and other Fraud Related Offences Act 2006 (Nigeria)

Constitution of the Republic of the Serb People of Bosnia and Herzegovina (28 February 1992)

Cybercrime Act 2007 (Sudan)

Cybercrime and Computer Related Crimes Act 2007 (Botswana)

Cybercrimes (Prohibition, Prevention, etc) Act 2015 (Nigeria)

Export of Goods (Control) (Iran Sanctions) Order 1980 (29 May 1980) 735 Statutory Instruments

Guam Crimes and Corrections, Chapter 48 Notification of Breaches of Personal Information (United States)

HR 3776 Cyber Diplomacy Act of 2017, 115th Congress (2nd Sess 2018) SEC.3

HR 5222 Iran Cyber Sanctions Act of 2016, 114th US Congress (2nd Sess 2016) <https://www.congress.gov/114/bills/hr5222/BILLS-114hr5222ih.pdf> accessed 1 July 2019

Hungary, 'Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary' (21 March 2013)

Iran (Trading Sanctions) Order 1980 (29 May 1980) 737 Statutory Instruments

President Barack Obama, 'Executive Order 13570 -- Prohibiting Certain Transactions with Respect to North Korea' (18 April 2011) <https://obamawhitehouse.archives.gov/the-press-office/2011/04/18/executive-order-13570-prohibiting-certain-transactions-respect-north-kor> accessed 1 July 2019

Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (South Africa)

S 2202 Economic Cooperation Act of 1948, 80th US Congress (2nd Sess, 69, 3 April 1948) <legisworks.org/congress/80/publaw-472.pdf> accessed 24 February 2019

US Department of the Treasury, 'Cyber-related Sanctions: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Executive Order 13694), as amended' (29 December 2016) <https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber> accessed 29 July 2019

US Presidential Executive Order 13010 (15 July 1996) 'Critical Infrastructure Protection'

Various national documents and positions

— Papers Relating to the Treaty of Washington (US GPO 1872)

<http://www.spiegel.de/media/media-35687.pdf> accessed 1 July 2019

Australia, ‘Australia’s International Cyber Engagement Strategy’ (Annex A: Australia's position on how international law applies to state conduct in cyberspace, 4 October 2017)

Australia, ‘Cyber Security Strategy’ (2009)

Bundesamt für Sicherheit in der Informationstechnik, ‘Die Lage der IT-Sicherheit in Deutschland 2014’ (November 2014) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf;jsessionid=686D15F6B6BFAD9B90DE29C65EE3937F.2_cid341?__blob=publicationFile&v=2> accessed 13 August 2019

Centre for the Protection of National Infrastructure, ‘Critical National Infrastructure’ <https://www.cpni.gov.uk/critical-national-infrastructure-0> accessed 13 August 2019

Colombia, ‘Policy Guidelines on Cybersecurity and Cyberdefense’ (draft, 4 July 2011)

Comitato Parlamentare Per La Sicurezza Della Repubblica, ‘Relazione Sulle Possibili Implicazioni E Minacce Per La Sicurezza Nazionale Derivanti Dall’utilizzo Dello Spazio Cibernetico’ (2010)

Daniel R Coats, ‘Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community’ (Office of the Director of National Intelligence, US Senate Select Committee on Intelligence, 13 February 2018) 5 <dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf> accessed 12 August 2019

Estonian Foreign Intelligence Service, ‘International Security and Estonia 2018’ (2018) <https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf> accessed 11 August 2019

European Union Committee, ‘Protecting Europe Against Large-Scale Cyberattacks’ HL (Paper 68, 2009–10)

FBI National Press Office, ‘Update on Sony Investigation’ (Federal Bureau of Investigation, 19 December 2014) <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> accessed 1 April 2016

FBI, ‘Update on Sony Investigation’ (17 December 2014) <http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> accessed 11 June 2019

Finland, ‘Finland´s Cyber Security Strategy’ (24 January 2013)

GCHQ, ‘Guidance 10 Steps: Summary’ (16 January 2015) <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary#network-security> accessed 7 January 2018

Government of Finland, ‘Finland’s Cyber Security Strategy - Background Dossier’ (Government Resolution 24 January 2013) 33 <http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/48-finlandas-cyber-security-strategy-background-dossier> accessed 4 June 2019

Government of Japan, ‘Cybersecurity Strategy’ (4 September 2015)

Government of Netherlands, ‘Government response to the AIV/CAVV report on cyber warfare’ (26 April 2012) <http://cms.webbeat.net/ContentSuite/upload/cav/doc/advies_22_reg_reactie_EN.pdf> accessed 1 April 2016

Harold H Koh, ‘International Law in Cyberspace’ (US Department of State, 18 September 2012) <2009-2017.state.gov/s/l/releases/remarks/197924.htm> accessed 26 January 2019

HC Deb 12 May 1980 vol 984

HM Government, National Cyber Security Strategy 2016-2021 (1 November 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> accessed 1 July 2019

Intelligence and Security Committee of Parliament, Annual Report 2016–2017 (HC 655, 20 December 2017) <https://goo.gl/nvaqd4> accessed 29 June 2019

Internet Service Providers Association of Ireland, ‘Code of Practice and Ethics’ (2013) .5 <http://www.ispai.ie/wp-content/uploads/2013/09/Code-of-Practice-and-Ethics.pdf> accessed 7 January 2018

Jeremy Wright, ‘Cyber and International Law in the 21st Century’ (23 May 2018) <gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 23 July 2019

Kersti Kaljulaid, ‘President of the Republic at the opening of CyCon 2019’ (Office of the President of Estonia, 29 May 2019) <president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019> accessed 13 August 2019

Kingdom of Saudi Arabia, ‘Developing National Information Security Strategy for the Kingdom of Saudi Arabia’ (2013)

Kingdom of the Netherlands, ‘Developments in the field of information and telecommunications in the context of international security’ (Resolution 69/28, 2015)

Leon E Panetta, ‘Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City’ (US Department of Defence, 11 October 2012) <archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> accessed 29 June 2019

Libicki MC, ‘It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture’ (US House of Representatives, Committee on Armed Services, 1 March 2017) <docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-LibickiM-20170301.pdf> accessed 29 June 2019

Lord Ahmad, ‘Foreign Office Minister condemns North Korean actor for WannaCry attacks’ (Press Release (19 December 2017) <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks> accessed 13 August 2019

Michael S Rogers, ‘Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities’ (US House of Representatives, 16 March 2016) <http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf> accessed 11 December 2018

National Security Agency, SIGINT Development, ‘Chinese Exfiltrate Sensitive Military technology’ (S//REL)

Nigeria, ‘National Cybersecurity Strategy’ (2015)

Nigerian Communications Commission, ‘Guidelines for the Provision of Internet Service’ (2007)

Norway, ‘Cyber Security Strategy for Norway’ (2012)

Office of the Secretary of State for Wales, ‘UK cyber security a top priority for UK Government’ (Press Release, 19 November 2015) <gov.uk/government/news/uk-cyber-security-a-top-priority-for-uk-government> accessed 29 June 2019

President of the United States, ‘Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment’ (The White House, 29 September 2016)

President of the United States, ‘International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World’ (May 2011)

President of the US, ‘National Security Strategy of the United States of America’ (December 2017) <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> accessed 1 July 2019

President of the US, ‘Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment’ (White House, 29 December 2016) <https://bit.ly/2kuHFtU> accessed 1 July 2019

Russian Federation, ‘Convention on International Information Security’ (draft, 22 September 2011) <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666> accessed 7 January 2018

Russian Federation, ‘Information Security Doctrine of the Russian Federation’ (9 September 2000) <itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf> accessed 1 July 2019

Singapore, ‘National Cyber Security Masterplan 2018’ (2013)

Swiss Confederation, ‘National strategy for the protection of Switzerland against cyber risks’ (19 June 2012)

Theresa May, ‘PM Commons Statement on Salisbury incident response: 14 March 2018’ (Oral statement to Parliament,14 March 2018) <https://www.gov.uk/government/speeches/pm-commons-statement-on-salisbury-incident-response-14-march-2018> accessed 13 August 2019

UK National Audit Office, ‘Investigation: WannaCry cyber attack and the NHS’ HC 414 Session 2017–2019 (27 October 2017) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf> accessed 13 August 2019

United States of America, ‘Cybersecurity Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure’ (2009)

US Air Force, ‘Cyberspace Operations: Air Force Doctrine Document 3–12’ (15 July 2010)

US Congress, Information Technology And Cyber Operations: Modernisation And Policy Issues To Support The Future Force, Hearing Before the Subcommittee on Intelligence, Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives, 113 Cong (1 Sess 2013) (Statement of Gen Keith B. Alexander, USA,

Commander, United States Cyber Command) <fas.org/irp/congress/2013_hr/cyber.pdf> accessed 1 July 2019

US Cyber Command, 'Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command' (20 April 2018)

US Department of Defence, 'F-35 Lightning II Program Fact Sheet – Selected Acquisition Report (SAR) 2015 Cost Data' (Joint Strike Fighter, 24 March 2016) <http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf> accessed 1 July 2019

US Department of Defence, 'Home and Defense and Civil Support Joint Operating Concept' (version 2.0, 1 October 2007)

US Department of Defence, 'The Department of Defense Cyber Strategy' (April 2015)

US Department of Homeland Security & FBI, 'GRIZZLY STEPPE – Russian Malicious Cyber Activity' (29 December 2016) <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> accessed 1 July 2019

US Department of Homeland Security, 'ICS-CERT Monthly Monitor' (September 2012) <https://goo.gl/ZzuDNZ> accessed 1 April 2016

US Department of Justice, 'Cyber's Most Wanted' (Federal Bureau of Investigation, 1 May 2014) <https://www.fbi.gov/wanted/cyber/sun-kailiang/@@download.pdf> accessed 31 May 2017

US Department of State, 'The Truman Doctrine and the Marshall Plan' (Office of the Historian) <history.state.gov/departmenthistory/short-history/truman> accessed 24 February 2019

US Department of State, Digest of United States Practice in International Law (Office of the Legal Adviser 1978)

US Department of Treasury, 'North Korea Sanctions Program' (2 November 2016) <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/nkorea.pdf> accessed 1 July 2019

US House of Representatives, 'Statement of Admiral Michael S Rogers, Commander United States Cyber Command Before the House Committee on Armed Services Emerging Threats and Capabilities Subcommittee' (11 April 2018) 12 <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf> accessed 19 May 2019

US National Intelligence Community, ‘FY 2013 Congressional Budget Justification’ (Volume I, National Intelligence Summary, February 2012) <https://fas.org/irp/budget/nip-fy2013.pdf> accessed 1 July 2019

US National Security Agency, ‘Computer Network Operations – Genie’ Spiegel (3 February 2015) <http://www.spiegel.de/media/media-35660.pdf> accessed 1 July 2019

US National Security Agency, ‘Iran – Current Topics, Interaction with GCHQ’ (12 April 2013) <https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/> accessed 1 July 2019

US Secretary of Defense, ‘Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations’ (23 June 2009) <http://goo.gl/TDTRLG> accessed 1 April 2016

US Senate, ‘Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service’ (1 March 2018) <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf> accessed 26 January 2019

US-China Economic and Security Review Commission, ‘2013 Annual Report to Congress’ 13th US Congress (1st Sess, 20 November 2013) 245 <https://www.uscc.gov/Annual_Reports/2013-annual-report-congress> accessed 29 July 2019

US-China Economic and Security Review Commission, ‘2016 Annual Report to Congress’ 14th US Congress (2nd Sess, 16 November 2016) 292–298<https://www.uscc.gov/Annual_Reports/2016-annual-report-congress> accessed 29 July 2019

Table of secondary sources

— ‘2017 Black Hat Attendee Survey’ (BlackHat USA, July 2017) 20 <blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf> accessed 12 August 2019

— ‘Arab Youth Group’ (*Pastebin*, 15 August 2012) <http://pastebin.com/PUHqDQnd> accessed 1 April 2016

— ‘Botnet’ (*Radware*) <http://goo.gl/hcGg3Z> accessed 1 April 2016

— ‘Britain's GCHQ Hacked Belgian Telecoms Firm’ *Der Spiegel* (20 September 2013) <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html> accessed 9 August 2019

— ‘China employs two million microblog monitors state media say’ *BBC* (4 October 2013) <http://goo.gl/zMqIAr> accessed 1 April 2016

— ‘China IP address link to South Korea cyber-attack’ *BBC* (21 March 2013) <http://goo.gl/aL0NP7> all accessed 1 April 2016

— ‘Cyberspace’ in *Oxford Dictionaries* (OUP 2018) <https://en.oxforddictionaries.com/definition/cyberspace> accessed 6 January 2018

— ‘Estonia hit by 'Moscow cyber war' *BBC* (17 May 2017) <http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

— ‘Estonia says cyber-assault may involve the Kremlin’ *New York Times* (Tallinn, 17 May 2007) <http://goo.gl/tSSlxx>

— ‘EU restrictive measures in response to the crisis in Ukraine’ (*Council of the EU*, 20 March 2014) <http://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis> accessed 29 July 2019

— ‘EU sanctions against Russia over Ukraine crisis’ (*European Union Newsroom*) <europa.eu/newsroom/highlights/special-coverage/eu-sanctions-against-russia-over-ukraine-crisis_en> accessed 29 July 2019

— ‘Expert Meeting on Private Military Contractors: Status and State Responsibility for their Actions’ (The University Centre for International Humanitarian Law, Geneva 29–30 August 2005)

— ‘Frequently Asked Questions’ (*Pastebin*) <http://pastebin.com/faq> accessed 1 April 2016

— ‘Iran oil fires raise cyber sabotage fears’ *Press TV Iran* (14 August 2016) <http://www.presstv.ir/DetailFr/2016/08/14/479952/Iran-oil-industry-fires-cyberattack-US-Israel> accessed 1 July 2019

— ‘Israel: Military Shot Down Syrian Spy Drone’ *VOA News* (11 November 2017) <https://www.voanews.com/a/israel-says-its-military-shot-down-syrian-spy-drone/4110874.html> accessed 3 August 2019

— ‘Leon Panetta warns of “cyber Pearl Harbour”’ *BBC* (12 October 2012) <https://www.bbc.com/news/av/technology-19923046/leon-panetta-warns-of-cyber-pearl-harbour> accessed 19 May 2019

— ‘Newsmakers with Senator Joe Lieberman’ (*C-SPAN*, 21 September 2012) <https://www.c-span.org/video/?308327-1/newsmakers-senator-joe-lieberman> accessed 1 July 2019

— ‘President Obama upbraids China over cyber attacks’ *BBC* (13 March 2013) <www.bbc.co.uk/news/world-us-canada-21772596> accessed 29 July 2019

— ‘Russian Federal Security Service (FSB) Internet Operations Against Ukraine’ (TAIA Global Report, 2015) <https://goo.gl/PMDY58> accessed 1 April 2016

— ‘Saudi Aramco digital explosion Six days passed, network still down’ (*Pastebin*, 20 August 2012) <http://pastebin.com/cTJeeTat> accessed 7 January 2019

— ‘Separate cyber team to attack aramco, 12 days network down’ (*Pastebin*, 25 August 2012) <http://pastebin.com/k2HFJ2LY> both accessed 1 April 2016

— ‘sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks Laboratory of Cryptography and System Security’ (CrySyS, Budapest University of Technology and Economics, v1.05 (31 May 2012) <http://www.crysys.hu/skywiper/skywiper.pdf> accessed 28 July 2019

— ‘TF-CSIRT to Estonia’s Rescue’ (*TERENA News*, 10 May 2007) <https://www.terena.org/news/fullstory.php?news_id=2103> accessed 13 August 2019

— ‘The cyber raiders hitting Estonia’ *BBC* (17 May 2007) <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> accessed 1 April 2016

— ‘Untitled’ (*Pastebin*, 15 August 2012) <http://pastebin.com/HqAgaQRj>

— ‘Untitled’ (*Pastebin*, 17 August 2012) <http://pastebin.com/tztnRLQG> accessed 1 April 2016

— '"WannaCry" Cyberattack Targets Iran Hospitals' *Financial Tribune* (14 May 2017) <https://financialtribune.com/articles/sci-tech/64402/wannacry-cyberattack-targets-iran-hospitals> accessed 13 August 2019

— 'WannaLaugh: Faced with WannaCry attack, AP cops unplug systems and save data' *New Indian Express* (13 May 2017) <http://www.newindianexpress.com/states/andhra-pradesh/2017/may/13/wannalaugh-faced-with-wannacry-attack-ap-cops-unplug-systems-and-save-data-1604416.html> accessed 13 August 2019

— 'Whois Record for 2ch.ru' <http://whois.domaintools.com/2ch.ru> accessed 19 May 2016

— 'Whois Record for Web-Dozor.ru' <http://whois.domaintools.com/web-dozor.ru> accessed 19 May 2016

Abi-Saab GM, 'De la sanction en droit international' *in* Jerzy Makarczyk (ed), *Theory of International Law at the Threshold of the 21 Century* (Kluwer 1996)

Agence France-Presse, 'Russia accused of series of international cyber-attacks' *Guardian* (13 May 2016) <https://www.theguardian.com/technology/2016/may/13/russia-accused-international-cyber-attacks-apt-28-sofacy-sandworm> accessed 1 July 2019

Akamai Technologies, 'Akamai's [state of the Internet] / security: Q2 2016 report' (2016) <http://goo.gl/IRp675> accessed 7 January 2018

Al Arabiya, 'Iran denies role in cyberattacks against Gulf oil and gas companies' *Al Arabiya* (14 October 2012) <https://english.alarabiya.net/articles/2012/10/14/243682.html> accessed 1 April 2016

Albano K & Kessem L, 'The Full Shamoon: How the Devastating Malware Was Inserted into Networks' (*IBM*, 15 February 2017) <https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks> accessed 28 July 2019

Albright D, Brannan P & Walrond C, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?' *Institute for Science and International Security Report* (22 December 2010) <http://goo.gl/yM4Wy> accessed 3 August 2018

Albright M, 'Enforcing International Law' (1995) 89 Proceedings of the Annual Meeting (ASIL)

Alexander D, 'Theft of F-35 design data is helping U.S. adversaries –Pentagon' *Reuters* (19 June 2013) <https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619> accessed 1 July 2019

Alshathry S, 'Cyber Attack on Saudi Aramco' (2017) 11(5) Intl J of Management and Information Technology

American Law Institute, *Restatement of the law, second: foreign relations law of the United States* (American Law Institute Publishers 1965)

Andorno R, 'The Precautionary Principle: A New Legal Standard for a Technological Age' (2004) 1(1) J of Intl Biotechnology L

Anzilotti D, *Corso di Diritto Internationale* (vol 1, 3rd edn, Athenaeum 1928) *cited in* F.V. Garcia-Amador, *Recent Codification of the Law of State Responsibility for Injuries to Aliens* (Brill 1974)

Anzilotti D, *Scritti di Diritto Internazionale Pubblico* (CEDAM 1956–7) 243 *cited in* Giorgio Gaja, 'Positivism and Dualism in Dionisio Anzilotti' (1992) 3 EJIL

Anzilotti D, *Cours de droid international* (trans Gidel, Pantheon-Assas/LGDJ 1999)

AP, 'South Korea traces cyber-attacks to Chinese IP address' *Guardian* (21 March 2013) <http://goo.gl/7FUKia>

Arkin WM, Dilanian K & McFadden C, 'What Obama Said to Putin on the Red Phone About the Election Hack' *NBC News* (19 December 2016) <https://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116> accessed 13 August 2019

Arnoux RA, 'Who invented fusion?' (ITER, 12 February 2014) <https://www.iter.org/newsline/-/1836> accessed 9 August 2019

Art R & Jervis R, *International Politics: Enduring Concepts and Contemporary Issues* (Pearson Education 2016)

Ashouri A, Bowers C & Warden C, 'An Overview of the Use of Digital Evidence in International Criminal Courts' (Salzburg Workshop on Cyberinvestigations, October 2013)

Axelrod R, 'More Effective Choice in the Prisoner's Dilemma' (1980) 24(3) J of Conflict Resolution

Axelrod R, *The Evolution of Cooperation* (Basic Books 1984)

Baldwin D, 'Inter-Nation Influence Revisited' (1971) 15(4) J of Conflict Resolution

Baldwin D, 'Power and International Relations' *in* Walter Carlsnaes, Thomas Risse & Beth A Simmons (eds), *Handbook of International Relations* (SAGE 2002)

Bannelier K, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2014) 14 Baltic Ybk of Intl L

Barkham J, 'Information Warfare and International Law on the Use of Force' (2011) 34 (1) New York University J of Intl L and Pol

Barnidge Jr RP, 'The Due Diligence Principle Under International Law' (2006) 8(1) Intl Community L Rev

Barrett M et al, 'Assured Access to the Global Commons Final Report' (NATO 2011)

Becker T, *Terrorism and the State: Rethinking the Rules of State Responsibility* (Bloomsbury Publishing 2006)

Beek C & Samani R, 'The State of Shamoon: Same Actor, Different Lines' (*McAfee*, 25 April 2017) <https://securingtomorrow.mcafee.com/executive-perspectives/state-shamoon-actor-different-lines/> accessed 19 May 2019

Bidder B, Matthias Schepp & Hilmar Schmundt, 'Virus Hunters Try to Catch Diplomatic Time Bomb' *Spiegel* (25 January 2013) <https://goo.gl/fC67zf> accessed 13 August 2019

Bilar D, 'On nth Order Attacks' *in* Christian Czosseck, Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)

Biller J & Schmitt M, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences' *EJIL: Talk!* (24 October 2018) <ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences> accessed 9 August 2019

Bishop Jr WW, 'The Role of International Law in a Peaceful World' *in* Joseph J Norton (ed), *Public International Law and the future World Order* (F.B. Rothman 1987)

Blomeyer-Bartenstein H, 'Due diligence' *in* R Bernhardt (ed), *Encyclopedia of Public International Law* (Elsevier Science Publishers 1987)

Boebert E, 'A Survey of Challenges in Attribution' *in* National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (The National Academies Press 2010)

Boed R, 'State of Necessity as a Justification for Internationally Wrongful Conduct' (2000) 3(1) Yale Human Rights and Development J

Borger J, 'Brazilian president: US surveillance a "breach of international law"' *Guardian* (24 September 2013) <https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> accessed 11 December 2018

Bosco DL, *Five to Rule Them All: The UN Security Council and the Making of the Modern World* (OUP 2009)

Bossert TP, 'It's Official: North Korea Is Behind WannaCry' *Wall Street Journal* (18 December 2017) <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537> accessed 13 August 2019

Braganca M, ‘Hunt for Red October. The new face of cyber espionage’ (2014) 4 SIAK-J (Intl Edition)

Brenner SW, ‘“At Light Speed”: Attribution and Response to Cybercrime/Terrorism/Warfare’ (2007) J of Crim L & Criminology

Brenner SW, *Cyber Threats – The Emerging Fault Lines of the Nation State* (2009 OUP)

Broad WJ, Markoff J & Sanger DE, ‘Israeli Test on Worm Called Crucial in Iran Nuclear Delay’ *New York Times* (15 January 2011) <nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all> accessed 1 July 2019

Broadhurst R et al, ‘Organisations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime’ (2014) 8(1) Intl J of Cyber Criminology

Bronk C & Tikk E: ‘Hack or Attack? Shamoon and the Evolution of Cyber Conflict’ (James A Baker III Institute for Public Policy, Rice University Working Paper, February 2013)

Bronk C & Tikk-Ringas E, ‘The Cyber Attack on Saudi Aramco’ (2013) 55(2) Survival, Global Politics and Strategy

Bronk H, Thorbruegge M & Hakkaja M, ‘CSIRT Setting up Guide in English’ (ENISA, 22 December 2006) <https://www.enisa.europa.eu/publications/csirt-setting-up-guide> accessed 7 January 2018

Brown D, ‘A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict’ (2006) 47 Harvard Intl L J

Brownlie I, *International Law and the Use of Force by States* (OUP 1963)

Brownsword R, ‘An Introduction to Legal Research’ <http://www.scribd.com/doc/14260230/An-Introduction-to-Legal-Research#scribd> accessed 17 August 2018

Brunnée J & Meshel T, ‘Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance’ (2015) 58 GYIL

Buchan R & Inaki N, ‘Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions’ (2019) 51 Cornell Intl L J

Buchan R, ‘Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?’ (2012) 17(2) J of Conflict and Security L

Buchan R, ‘Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm’ (2016) 21(3) J of Conflict & Security L

Buchan R, ‘The International Legal Regulation of State-Sponsored Cyber Espionage’ *in* Anna-Maria Osula & Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE 2016)

Bull H, *The anarchical society: A study of order in world politics* (3rd edn, Palgrave 2002)

Bumgarner J, ‘Decapitating Saudi Aramco with the Sword of Justice’ (*DefenceIQ*, 22 January 2013) <http://goo.gl/2axlJ7> accessed 1 April 2019

Bumiller E & Shanker T, ‘Panetta Warns of Dire Threat of Cyberattack’ *New York Times* (11 October 2012) <nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html> accessed 3 August 2018

Buncombe A, ‘Donald Trump's explosive UN speech: Read it in full’ *The Independent* (19 September 2017) <independent.co.uk/news/world/americas/us-politics/trump-un-speech-read-in-full-transcript-north-korea-general-assembly-a7956041.html> accessed 9 August 2019

Burchill S, *The National Interest in International Relations Theory* (Palgrave Macmillan UK 2005)

Buzan B, ‘Peace, Power, and Security: Contending Concepts in the Study of International Relations’ (1984) 21(2) J of Peace Research

Caltagirone S, Pendergast A & Betz C, ‘The Diamond Model of Intrusion Analysis’ (Center for Cyber Threat Intelligence and Threat Research, Technical Report ADA586960, 5 July 2013)

Cane P, *Responsibility in Law and Morality* (Hart Publishing 2002)

Cannizzaro E, ‘The Role of Proportionality in the Law of International Countermeasures’ (2001) 12(5) EJIL

Carnegie Mellon University, ‘List of National CSIRTs’ <https://www.cert.org/incident-management/national-csirts/national-csirts.cfm> accessed 8 January 2018

Carr J, ‘Who's Responsible for the Saudi Aramco Network Attack?’ (*Digital Dao*, 27 August 2012) <http://goo.gl/gfsvL3> accessed 1 April 2019

Carter A, ‘Remarks on “Sustaining Nuclear Deterrence”’ (*US Department of Defence*, 26 September 2016) <defense.gov/News/Speeches/Speech-View/Article/956630/remarks-on-sustaining-nuclear-deterrence/> accessed 24 February 2019

Casalini F & Di Stefano S, ‘State behaviour in cyberspace: a new challenge for the international community’ (Diplo Foundation, 12 March 2018) <diplomacy.edu/blog/state-

behaviour-cyberspace-new-challenge-international-community> both accessed 29 June 2019

Casey T, 'Threat Agent Library Helps Identify Information Security Risks' (Intel Information Technology White Paper, September 2007) <https://goo.gl/I2d4bN> accessed 1 April 2016

Cassese A, *International Law* (2nd edn, OUP 2005)

Cassese A, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' (2007) 18(4) EJIL

CCD COE, 'Cyber Security Strategy Documents' <https://ccdcoe.org/strategies-policies.html> accessed 8 January 2018

Chan S, 'Cyberattacks Strike Saudi Arabia, Harming Aviation Agency' *New York Times* (1 December 2016) <https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html> accessed 1 July 2019

Chappell B & Memmott M, 'Putin Says Those Aren't Russian Forces in Crimea' *NPR* (4 March 2014) <http://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea> accessed 1 July 2019

Cheng B, *General Principles of Law as Applied by International Courts and Tribunals* (CUP 1994)

Christenson GA, 'Attributing Acts of Omission to the State' 12 (1990) Michigan J of Intl L

Chung IY, *Legal Problems Involved in the Corfu Channel Incident* (Librairie Droz 1959)

Clarke RA & Knake RK, *Cyber War: The Next Threat to National Security and What to do about it* (Ecco 2012)

Clover C, 'Kremlin-backed group behind Estonia cyber blitz' *Financial Times* (11 March 2009) <ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?ft_site=falcon&desktop=true> accessed 5 May 2017

Coalson R, 'Behind the Estonia Cyberattacks' *Radio Free Europe/Radio Liberty* (6 March 2009) <http://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html> accessed 5 May 2017

Cohen D & Narayanaswamy K, 'Survey/Analysis of Levels I, II, and III Attack Attribution Techniques' (Cs3, April 2004)

Commonwealth Telecommunications Organisation, 'Commonwealth Approach for Developing National Cyber Security Strategies' (Revised 2015)

Condorelli L & Kress C, ‘The Rules of Attribution: General Considerations’ *in* James Crawford, Alain Pellet & Simon Olleson (eds), *The law of international responsibility* (OUP 2010)

Corn GP & Taylor R, ‘Sovereignty in the Age of Cyber’ (2017) 111 AJIL Unbound 207)

Council on Foreign Relations, ‘Cyber Operations Tracker data’ <https://www.cfr.org/interactive/cyber-operations/export-incidents?_format=csv> accessed 12 August 2019

Crawford J, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries United Nations* (CUP 2002)

Crawford J, ‘State Responsibility’ in *Max Planck Encyclopaedia of Public International Law* (September 2006) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093?rskey=dfuWu4&result=1&prd=EPIL> accessed 17 January 2019

Crawford J, *Brownlie’s Principles of Public International Law* (8th edn, OUP 2012)

Crawford J, *State Responsibility: The General Part* (CUP 2013)

Czosseck C, Ottis R & Talihärm AM, ‘Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security’ *in* Matthew Warren (ed), *Case Studies in Information Warfare and Security for Researchers, Teachers and Students* (Academic Conferences 2013)

D'Amato A, ‘Is Law Really “Law”?’ (1984) 79(5&6) Northwestern University L Rev

D’Amato A, ‘Is International Law really “Law”?’ (1985) Northwestern University L Rev

D’Argent P, ‘Reparation, Cessation, Assurances and Guarantees of Non-Repetition’ *in* André Nollkaemper & Ilias Plakokefalos (eds), *Principles of Shared Responsibility in International Law – An Appraisal of the State of the Art* (CUP 2014)

Dawidowicz M, *Third-Party Countermeasures in International Law* (CUP 2017)

De Vattel E, *The Law of Nations* (bk II, Joseph Chitty trans., Gaunt 2001)

Dehghan SA, ‘Iranian oil ministry hit by cyber-attack’ *Guardian* (23 April 2012) <https://www.theguardian.com/world/2012/apr/23/iranian-oil-ministry-cyber-attack> accessed 1 July 2019

Delerue F & Géry A, ‘France's Cyberdefense Strategic Review and International Law’ (*Lawfare*, 23 March 2018) <https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law> accessed 9 June 2019

Denza E, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (OUP 2016)

Deutsch KW, *The Analysis of International Relations* (Prentice–Hall 1968)

Deutsche Telekom, 'Security on the Internet: Report on Information and Internet Security' (October 2013)

Dinstein Y, *War, Aggression and Self-defence* (CUP 2001)

Dörr O, 'Obligations of the State of Origin of a Cyber Security Incident' (2015) 58 GYIL

Downing LL, 'The Prisoner's Dilemma Game as a Problem-Solving Phenomenon: An Outcome Maximisation Interpretation' (1975) 6(4) Simulation and Games

Dupuy PM, 'Due Diligence in the International Law of Liability' *in* OECD, *Legal Aspects of Transfrontier Pollution* (OECD 1977)

Dworkin R, 'Easy Cases, Bad Law, and Burdens of Proof' (1972) 25 Vanderbilt L Rev

Efrony D & Shany Y, 'A Rule Book in the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) AJIL

Egan BJ, 'Remarks on International Law and Stability in Cyberspace' (US Department of State, 10 November 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> accessed 9 August 2019

Elagab OY, *The Legality of Non-Forcible Counter-Measures in International Law* (Clarendon Press 1988)

Elagab OY, 'The Place of Non-Forcible Counter-Measures in Contemporary International Law' *in* Guy S Goodwin-Gill & Stefan Talmon (eds), *The Reality of International Law: Essays in Honour of Ian Brownlie* (Clarendon Press 1999)

ENISA, 'National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace' (May 2012)

ENISA, 'Cyber Incident Reporting in the EU – An overview of security articles in EU legislation' (August 2012)

ENISA, 'An evaluation Framework for National Cyber Security Strategies' (November 2014)

ENISA, 'WannaCry Ransomware Outburst' (15 May 2017) <https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst> accessed 13 August 2019

ENISA, ‘Threat Landscape Report 2017’ (January 2018) <enisa.europa.eu/publications/enisa-threat-landscape-report-2017> accessed 26 January 2019

Eriksson B et al, ‘A learning-based approach for IP geolocation’ *in* Arvind Krishnamurthy & Bernhard Plattner (eds), *Passive and Active Measurement* (Springer 2010)

Evron G, ‘Bating Bonets and Online Mobs’ (2008) Winter/Spring, Georgetown J of Intl Affairs

Farkas L & O’Farrell O, *Reversing the Burden of Proof: Practical Dilemmas at the European and National Level* (European Commission 2014)

Fildes J, ‘Stuxnet worm 'targeted high-value Iranian assets' *BBC* (23 September 2010) <bbc.com/news/technology-11388018> accessed 26 January 2019

Finkle J, ‘Exclusive: Insiders suspected in Saudi cyber attack’ *Reuters* (2 September 2012) <http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907> 18 July 2018

Finnemore M & Hollis DB, ‘Constructing Norms for Global Cybersecurity’ (2016) 110 (3) AJIL

Finnemore M, ‘Cybersecurity and the Concept of Norms’ (Carnegie Endowment for International Peace, 30 November 2017) <carnegieendowment.org/files/Finnemore_web_final.pdf> accessed 11 June 2018

FireEye, ‘Digital Bread Crumbs: Seven Clues To Identifying Who’s Behind Advanced Cyber Attacks’ (26 June 2013) <fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-digital-bread-crumbs.pdf> accessed 13 August 2019

FireEye, ‘APT28: A Window into Russia’s Cyber Espionage Operations?’ (2014) 28 <https://goo.gl/BeXhoK> accessed 1 April 2016

FIRST, ‘FIRST Best Practice Guide Library (BPGL)’ <https://www.first.org/resources/guides> accessed 7 January 2018

Fisher R, *Improving compliance with international* law (University Press of Virginia 1981)

Fitzgerald E, ‘Helping States Help Themselves: Rethinking the Doctrine of Countermeasures’ (2016) 16 Macquarie L J

Flynn Goodwin C & Nicholas P, ‘Developing a National Strategy for Cybersecurity – Foundations for Security, Growth, and Innovation’ (Microsoft, October 2013)

Follath E & Stark H, ‘How Israel Destroyed Syria's Al Kibar Nuclear Reactor’ *Der Spiegel* (2 November 2009) <http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html> accessed 1 July 2019

Foster CE, *Science and the Precautionary Principle in International Courts and Tribunals* (CUP 2013)

Franck TM, 'On Proportionality of Countermeasures in International Law' (2008) 102(4) AJIL

Freeland C, 'The Case for Progressive Internationalism' *The Economist – The World in 2018* (December 2017)

French D & Stephens T, 'ILA Study Group on Due Diligence in International Law' (1st Report, 7 March 2014)

Frey B, 'Prevention of human rights violations committed with small arms and light weapons' (25 June 2003) UN Doc E/CN.4/Sub.2/2003/29

Fried JHE, 'How Efficient is International Law?' *in* Karl Deutsch & Stanley Hoffmann (eds), *The Relevance of International Law* (Schenkman Publishing 1968)

Frowein JA, 'Obligations *erga omnes'* in *Max Planck Encyclopedia of Public International Law* (December 2008)

Fuller B, 'Federal Intrusion Detection, Cyber Early Warning and the Federal Response' (SANS Institute InfoSec Reading Room, version 1.4b, 2013) <https://www.sans.org/reading-room/whitepapers/warfare/federal-intrusion-detection-cyber-early-warning-federal-response-1095> accessed 7 January 2018

Gamblin J, 'Mirai-Source-Code' GitHub (15 July 2017) <github.com/jgamblin/Mirai-Source-Code> accessed 21 May 2019

Gao Z & Ansari N, 'Tracing cyber attacks from the practical perspective' (2005) 43(5) IEEE Communications Magazine

Garnett R & Clarke P, 'Cyberterrorism: A New Challenge for International Law' *in* Andrea Bianchi (ed) *Enforcing International Law Norms Against Terrorism* (Hart Publishing 2004)

Gellman B & Nakashima E, 'U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show' *Washington Post* (30 August 2013) <https://wapo.st/2LTGsyD> accessed 1 July 2019

Gervais M, 'Cyber Attacks and the Laws of War' (2012) 1(8) J of L & Cyber Warfare: The New Frontier of Warfare

Giegerich T, 'Retorsion' in *Max Planck Encyclopedia of Public International Law* (March 2011) <opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983?prd=EPIL> accessed 29 July 2019

Global Cyber Security Capacity Centre (University of Oxford), ‘Cybersecurity Capacity Maturity Model for Nations (CMM)’ (revised edition, 31 March 2016)

Global Research & Analysis Team, ‘“Red October” Diplomatic Cyber Attacks Investigation’ (Kaspersky Lab, 14 January 2013) <securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/> accessed 13 August 2019

Global Research & Analysis Team, ‘The “Red October” Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies’ (*Kaspersky Lab*, 14 January 2013) <https://securelist.com/blog/incidents/57647/the-red-october-campaign/> accessed 1 July 2019

Global Research & Analysis Team, ‘“Red October”. Detailed Malware Description 2. Second Stage of Attack’ (Kaspersky, 17 January 2013) <securelist.com/red-october-detailed-malware-description-2-second-stage-of-attack/36842> accessed 12 August 2019

Global Research & Analysis Team, ‘ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms’ (Kaspersky Lab, 8 August 2016) <securelist.com/faq-the-projectsauron-apt/75533/> accessed 26 January 2019

Global Research and Analysis Team, ‘The ProjectSauron APT’ (Version 1.02, Kaspersky Lab, 9 August 2016) <https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf> accessed 13 August 2019

Gold M, ‘Taiwan a “testing ground” for Chinese cyber army’ (*Reuters*, 18 July 2013) <http://goo.gl/tJ7Psp>

Goldsmith J, ‘Against Cyberanarchy’ (1998) 65(4) University of Chicago L Rev

Goldsmith J, ‘Review: Sovereignty, International Relations Theory, and International Law’ (2000) 52 Stanford L Rev

Goldstein J, ‘Estonia's Cyber Attacks: Lessons Learned’ (Wikileaks, 30 August 2011) <http://goo.gl/1IOhn> accessed 11 August 2018

Gowlland-Debbas V, ‘Security Council Enforcement Action and Issues of State Responsibility’ (1994) 43(1) Intl and Comparative L Quarterly

Green JA, ‘Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice’ (2009) 58(1) ICLQ

Greenberg A, ‘Hold North Korea Accountable for WannaCry—And the NSA, too’ (*Wired*, 19 December 2017) <https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/> accessed 1 July 2019

Grohmann K, ‘Games organisers confirm cyber attack, won't reveal source’ (*Reuters*, 11 February 2018) <https://uk.reuters.com/article/us-olympics-2018-cyber/games-organizers-confirm-cyber-attack-wont-reveal-source-idUKKBN1FV036> accessed 1 July 2019

Gross L, ‘States as Organs of International Law and the Problems of Auto-interpretation’ *in* George A Lipsky (ed), *Law and Politics in the World Community* (University of California Press 1953)

Gross O, ‘Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents’ (2015) 48 Cornell Intl L J

Guo C et al, ‘Mining the Web and the Internet for Accurate IP Address Geolocations’ in *2009 Proceedings IEEE INFOCOM* (Institute of Electrical and Electronics Engineers April 2009)

Guzman AT, *How International Law Works: A Rational Choice Theory* (OUP 2010)

Hall WE, *A Treatise on International Law* (2d edn, Clarendon Press 1884)

Hammarskjold D, ‘Liberty and Law in International Life’ *in* Clarence W Jenks, Roberto Ago & Oscar Schachter (eds), *International Law in a Changing World* (LLC 2012)

Harris B, Konikoff E & Petersen P, ‘Breaking the DDoS Attack Chain’ (CMU-ISR-MITS-2, Institute for Software Research, Carnegie Mellon University 2013)

Hart HLA & Honoré T, *Causation in the Law* (OUP 1985)

Hart HLA, *The Concept of Law* (2nd edn, Clarendon 1994)

Healey J, ‘Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities’ (Testimony to United States House of Representatives Committee on Armed Services, 1 March 2017) <http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Bio-HealeyJ-20170301-U1.pdf> accessed 1 July 2019

Heickerö R, ‘Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations’ (Swedish Defence Research Agency, 30 March 2010) <http://goo.gl/bG6ljJ> accessed 1 April 2016

Heintschel von Heinegg W, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ *in* C Czosseck, R Ottis, K Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (CCD COE 2012)

Heintschel von Heinegg W, ‘Territorial Sovereignty and Neutrality in Cyberspace’ (2013) 89 Intl L Studies

Henderson H, *Encyclopedia of Computer Science and Technology* (Infobase Publishing 2009)

Henkin L, *How Nations Behave: Law and Foreign Policy* (Council on Foreign Relations 1979)

Herz JH, 'Idealist Internationalism and the Security Dilemma' (1950) 2(2) World Politics

Herzog S, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4(2) J of Strategic Security

Hessbruegge J, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law' (2004) 36(2) NYU J Intl L & Pol

Higgins KJ, '"Red October" Attacks: The New Face of Cyberespionage' (Dark Reading, 14 January 2013) <darkreading.com/attacks-breaches/red-october-attacks-the-new-face-of-cyberespionage/d/d-id/1138972> accessed 1 August 2019

Hinkle KC, 'Countermeasures in the Cyber Context: One More Thing to Worry About' Yale (2011) 37 Yale J of Intl L Online <https://bit.ly/33I55TN> accessed 12 August 2019

Hirsch M, 'Game Theory, International Law, And Future Environmental Cooperation in the Middle East' (1998-1999) 27 Denver J of Intl L and Policy

Hock Lai H, *A Philosophy of Evidence Law* (OUP 2008)

Hoffmann S, 'International Law and the Control of Force' *in* Karl Deutsch & Stanley Hoffmann (eds), *The Relevance of International Law* (Schenkman Publishing 1968)

Hollis DB, 'Private Actors in Public International Law: Amicus Curiae and the Case for the Retention of State Sovereignty' (2002) 25 Boston College Intl & Comp L Rev

Holtzmann HM, 'Fact-finding before the Iran-United States Claims Tribunal*' in* Richard Lillich (ed), *Fact-finding before international tribunals* (Transnational Publishers 1992)

Honoré T, *Responsibility and Fault* (Hart Publishing 1999)

Hoppe C, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 EJIL

Horvath R, *Putin's "Preventive Counter-Revolution": Post-Soviet Authoritarianism and the Spectre of Velvet Revolution* (Routledge 2013)

Hufbauer GC, Schott JJ & Elliott KA, *Economic Sanctions Reconsidered: History and Current Policy* (Vol 1, Peterson Institute 1990)

Hughes R, 'A Treaty for Cyberspace' (2010) 86(2) Intl Affairs

Human Rights Watch, '"Race to the Bottom" Corporate Complicity in Chinese Internet Censorship' (vol 18, no 8, August 2006) <https://www.hrw.org/reports/2006/china0806/china0806web.pdf> accessed 13 August 2019

Hunker J, Hutchinson R & Margulies J, 'Attribution of Cyber Attacks on Process Control Systems' *in* Papa M & Shenoi S (eds), *Critical Infrastructure Protection II. ICCIP 2008* (vol 290, Springer 2008)

Hyun Kim S, Wang QH & Ullrich JB, 'A comparative study of cyberattacks' (2012) 55(3) Communications of the ACM

Ilves TH, 'Address by H.E. Mr. Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly' (25 September 2013) <http://goo.gl/kyKNbD> accessed 8 February 2015

Information Sciences Institute University of Southern California, 'DOD Standard: Internet Protocol' (Prepared for US Defense Advanced Research Projects Agency, January 1980) <https://tools.ietf.org/html/rfc760> accessed 1 April 2018

International Law Association Committee on Formation of Customary (General) International Law, 'Statement of Principles Applicable to the Formation of General Customary International Law' (Final Report of the Committee, London Conference, 2000)

International Telecommunication Union, 'CIRT Programme' <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx> accessed 7 January 2018

International Telecommunication Union, 'National Strategies Repository' <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx> accessed 8 January 2018

International Telecommunication Union & ABI Research, 'Cybersecurity Index of Indices' (Geneva, 2 July 2015) <goo.gl/DIjNto> accessed 30 September 2016

Jackson W, 'Stuxnet shut down by its own kill switch' (*GCN*, 26 June 2016) <https://gcn.com/Articles/2012/06/26/Stuxnet-demise-expiration-date.aspx> accessed 28 July 2019

Jennings R & Watts A (eds), *Oppenheim's International Law* (9th edn, vol I Peace, Longman 1992)

Jensen ET, 'Cyber Sovereignty: The Way Ahead' 50 (2) Texas J of Intl L

Jervis R, 'Security Regimes' (1982) 36(2) Intl Organisation

Johnson DR & Post D, 'Law and Borders - The Rise of Law in Cyberspace' (1996) 48 Stanford L Rev

Jones A, Martin T, 'Digital forensics and the issues of identity' (2010) 15(2) Information Security Technical Report

Jones MA, *Textbook on Torts* (Blackstone Press 1998)

Jorgensen NHB, 'A Reappraisal of Punitive Damages in International Law' (1997) 68(1) British Ybk of Intl L

Joyce D, 'Fact-Finding and Evidence at the International Court of Justice: Systemic Crisis, Change or More of the Same' (2007) 18 Finnish Ybk of Intl L

Joyner CC, 'Coercion' in *Max Planck Encyclopedia of Public International Law* (December 2006) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749?prd=EPIL> accessed 19 May 2019

Kanno-Youngs Z, 'Homeland Security Chief Cites Top Threat to U.S. (It's Not the Border)' *New York Times* (18 March 2019) <https://nyti.ms/2J2oHu0> accessed 29 June 2019> accessed 12 August 2019

Kanuck S, 'Sovereign Discourse on Cyber Conflict Under International Law' (2010) 88 Texas L Rev

Katz-Bassett E et al, 'Towards IP geolocation using delay and topology measurements' in *IMC '06 Proceedings of the 6th ACM SIGCOMM* (ICM October 2006)

Kazazi M, *Burden of Proof and Related Issues: A Study on Evidence Before International Tribunals* (Kluwer Law International 1996)

Kees A, 'Responsibility of States for Private Actors' in *Max Planck Encyclopaedia of Public International Law* (March 2011) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1092> accessed 12 August 2019

Keizer G, 'Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable' *Computer World* (9 December 2010) <http://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html> accessed 8 January 2018

Kelsen H, *Principles of International Law* (Lawbook Exchange 2003)

Kennedy KA & Pronin E, *Bias Perception and the Spiral of Conflict in Jon Hanson, Ideology, Psychology, and Law* (OUP 2012)

Keohane R, 'The demand for international regimes' (1928) 36(2) Intl Organisation

Keohane R, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton University Press 2005)

Khan K, Dixon R & Fulford A, ‘Archbold International Criminal Courts’ (Sweet & Maxwell 2014)

Klimburg A (ed), ‘National Cyber Security Framework Manual’ (NATO CCD COE, 2012)

Kokott J, *The Burden of Proof in Comparative and International Human Rights Law: Civil and Common Law Approaches with Special Reference to the American and German Legal Systems* (Kluwer Law International 1998)

Kolb R, ‘Reflections on Due Diligence Duties and Cyberspace’ (2015) 58 GYIL

Kramer AE, ‘Russia, This Time the Victim of a Cyberattack, Voices Outrage’ *New York Times* (14 May 2017) https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html> accessed 13 August 2019

Kunz JL, ‘Sanctions in international law’ (1960) 54(2) AJIL

Kurbalija J, ‘E-Diplomacy and Diplomatic Law in the Internet Era’ *in* Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCD COE 2013)

Lacey N, *State punishment* (Routledge 1988)

Lauterpacht H, ‘Revolutionary Activities by Private Persons Against Foreign’ (1928) 22 AJIL

Lauterpacht H, ‘The Grotian Tradition in International Law’ (1946) 23 British Ybk of Intl L

Lederman J, ‘Cuba mystery: U.S. doctors find brain abnormalities in victims’ *CBC* (6 December 2017) <http://www.cbc.ca/news/world/cuba-mystery-brain-1.4435900> accessed 14 January 2018

Lentz CE, ‘A State's Duty to Prevent and Respond to Cyberterrorist Acts’ (2010) 10(2) Chicago J of Intl L

Levy MA, ‘Is the Environment a National Security Issue?’ (1995) 20(2) Intl Security

Lindsay JR, ‘The Impact of China on Cybersecurity’ (2014/15) 39(3) Intl Security

Lundbohm E, ‘Understanding nation-state attacks’ (2017) 2017/10 Network Security

Lye Myers S, ‘Russia Rebukes Estonia for Moving Soviet Statue’ *New York Times* (27 April 2007) <http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html> accessed 1 July 2019

MAHER, ‘Identification of a New Targeted Cyber-Attack’ (28 May 2012) <web.archive.org/web/20131105160213/http://www.certcc.ir/index.php?name=news&file=article&sid=1894> accessed 28 July 2019

Mandiant, ‘APT1 – Exposing One of China’s Cyber Espionage Units’ (2013) <http://goo.gl/H3IkzR> accessed 7 January 2018

Marauhn T, ‘Customary Rules of International Environmental Law – Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace’ *in* Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE 2013)

Markoff J & Kramer AE, ‘U.S. and Russia Differ on a Treaty for Cyberspace’, *New York Times* (27 June 2009) <nytimes.com/2009/06/28/world/28cyber.html> accessed 29 June 2019

Markoff M, ‘Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security’ (*US Mission to the UN*, 23 June 2017) <https://usun.state.gov/remarks/7880> accessed 1 July 2019

Marxsen C, ‘The Crimea Crisis – An International Law Perspective’ (2014) 74(2) Heidelberg J of Intl L

Maslow AH, ‘A Theory of Human Motivation’ (1943) 50 Psychological Rev

Mason J, ‘Obama sanctions Russia for intervening in 2016 election’ (*Reuters*, 29 December 2016) <http://www.reuters.com/article/us-usa-russia-cyber-obama-idUSKBN14I1W2> accessed 29 July 2019

Masters J, ‘Theresa May's full statement on Russian spy's poisoning’ *CNN* (13 March 2018) <https://edition.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html> accessed 13 August 2019

Mathews JT, ‘Power Shift’ (1997) 76(1) Foreign Affairs

Mattis P, ‘The Analytic Challenge of Understanding Chinese Intelligence Services’ (2012) 56(3) Studies in Intelligence

Maurer T, *Cyber Mercenaries – The State, Hackers, and Power* (CUP 2018)

McAfee, ‘W32/DistTrack, W64/DistTrack’ (17 August 2012) 5 <https://goo.gl/mAZRTR> accessed 12 April 2016

McDonald A & Brollowski H, ‘Security’ in *Max Planck Encyclopedia of Public International Law* (May 2011) <https://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e399?rskey=321VIt&result=1&prd=EPIL> accessed 19 May 2019

McKirdy E & Ilyushina M, ‘Putin: “Patriotic” Russian hackers may have targeted US election’ *CNN* (2 June 2017) <https://edition.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html> accessed 13 August 2019

Mearsheimer JJ, *The Tragedy of Great Power Politics* (WW Norton 2001)

Mearsheimer JJ, 'Structural Realism' *in* Tim Dunne, Milja Kurki, Steve Smith (eds) *International Relations Theories* (OUP 2010)

Messerschmidt J, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' (2013) 52(1) Columbia J of Transnational L

Miller R, 'Congressman John Carter: "Cyber is just pounding me from every direction"' (*The Verge*, 27 March 2015) <https://www.theverge.com/tldr/2015/3/27/8299577/john-carter-the-Internet-is-a-series-of-cyber-poundings> accessed 1 July 2019

Mirkovic J & Kissel E, 'Comparative Evaluation of Spoofing Defenses' (2009) 8(2) IEEE Transactions on Dependable and Secure Computing

Mirkovic J, Prier G & Reiher P, 'Attacking DDoS at the Source' *Network Protocols* 2002 *(Proceedings of the 10th IEEE International Conference)*

Mitchell C, 'Panel: Still no sense of consequence for violating cyber 'norms' of behaviour' (Inside Cybersecurity, 9 August 2018) <insidecybersecurity.com/daily-news/panel-still-no-sense-consequence-violating-cyber-'norms'-behavior> accessed 12 August 2019

Mitchell S & Hensel P, 'International Institutions and Compliance with Agreements' (2007) 51(4) American J of Political Science <http://www.paulhensel.org/comply.html> accessed 28 July 2019

MNA, 'Iran unveils upgraded missile, five pieces of military hardware' *Mehr News* (21 August 2012) <en.mehrnews.com/news/52172/Iran-unveils-upgraded-missile-five-pieces-of-military-hardware> accessed 24 February 2019

Morgenstern O, 'Game Theory: Theoretical Aspects' *in* David L Sills (ed), *International Encyclopedia of the Social Sciences* (vol 6, Macmillan 1968)

Morgenthau HJ, *Politics Among Nations: The Struggle for Power and Peace* (McGraw-Hill 1993)

MWC Pinto, 'The duty of Co-Operation and the United Nations Convention on the Law of the Sea' *in* Adriaan Bos & Hugo Siblesz, *Realism in Law-Making: Essays on International Law in Honour of Willem Riphagen* (Martinus Njihoff 1986)

Myers SL, 'Russia Rebukes Estonia for Moving Soviet Statue' *New York Times* (27 April 2007) <nytimes.com/2007/04/27/world/europe/27cnd-estonia.html> accessed 11 December 2018

Naim M, ‘What Is a GONGO?’ *Foreign Policy* (13 October 2009) <http://goo.gl/9FbNF1> accessed 1 April 2016

Nakashima E & Warrick J, ‘Stuxnet was work of U.S. and Israeli experts, officials say’ *Washington Post* (2 June 2012) <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c7a1c56dd3e1> accessed 13 August 2019

Nazario J, ‘Politically Motivated Denial of Service Attacks’ *in* Christian Czosseck & Kenneth Geers (eds) *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)

NCSC-NL (National Cyber Security Centre of The Netherlands), ‘CERT-in-a-box’ <https://www.first.org/resources/guides/cert-in-a-box.zip> accessed 7 January 2018

Newton M & May L, *Proportionality in International Law* (OUP 2014)

Ney M & Zimmermann A, ‘Cyber-Security Beyond the Military Perspective: International Law, “Cyberspace”, and the Concept of Due Diligence’ (2015) 58 GYIL

Nolte G, ‘From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Inter-state Relations’ (2002) 13(5) EJIL

Nye J, *Bound to Lead: The Changing Nature of American Power* (Basic Books 1991)

Nye J, *The Future of Power* (Hachette UK 2011)

Nyst C & Crowe A, ‘Unmasking the Five Eyes’ global surveillance practices’ *in* Alan Finlay (ed), *Global Information Society Wat014* (Global Information Society Wat014) <http://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices> accessed 11 January 2018

O’Connell ME, ‘Evidence of Terror’ (2002) 7(1) J of Conflict and Security L

O’Connell ME, ‘Cyber Mania’ *in* Mary E O’Connell, Louise Arimatsu, & Elizabeth Wilmshurst (eds), *International Law: Meeting Summary: Cyber Security and International Law* (Chatham House 2012)

O’Connell ME, The Prohibition of the Use of Force’ *in* Nigel White & Christian Henderson, *Research Handbook on International Conflict and Security Law* (Edward Elgar 2013)

O’Keefe R, ‘Proportionality’ *in* James Crawford, Alain Pellet & Simon Olleson, *The Law of International Responsibility* (OUP 2010)

OAS & IDB, ‘Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report’ (2016)

OAS, ‘Best Practices for Establishing a National CSIRT by the Organisation of American States’ (2016) <https://www.thegfce.com/documents/publications/2016/04/01/best-practices-for-establishing-a-national-csirt> accessed 7 January 2018

OECD, ‘Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy’ (2012)

Ohlin JD, ‘Nash Equilibrium and International Law’ (2012) 23(4) EJIL

Oppenheim L, *International Law: A Treatise* (vol I, Ronald Roxburgh (ed), 3rd edn, Lawbook Exchange 2005)

Oppenheim L, *International Law: A Treatise* (vol II, Longmans 1952)

Ottis R & Lorents P, ‘Cyberspace: Definition and Implications’ in *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April* (Academic Publishing Limited 2010)

Pagliery J, ‘The inside story of the biggest hack in history’ *CNN* (5 August 2015) <http://money.cnn.com/2015/08/05/technology/aramco-hack/> both accessed 9 June 2019

Park J & Cho M, ‘South Korea blames North Korea for December hack on nuclear operator’ *Reuters* (17 March 2015) <reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317> accessed 1 July 2019

Paruchuri V et al, ‘Authenticated Autonomous System Traceback’ (2004) Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA’04)

Peel J, *Science and Risk Regulation in International Law* (CUP 2010)

Pellet A, ‘The Opinions of the Badinter Arbitration Committee: A Second Breath for the Self-Determination of Peoples’ (1992) 3(1) EJIL

Pellet A & Miron A, ‘Sanctions’ in *Max Planck Encyclopedia of Public International Law* (August 2013)

Peng T, Leckie C & Ramamohanarao R, ‘Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring’ *in* Nikolas Mitrou et al, *Networking 2004 - Lecture Notes in Computer Science* (vol 3042, Springer 2004)

Pennock J, Smith D & Wilson G, ‘Design and Implementation of a Remote Forensics System’ (Mcafee Foundstone, 2 May 2005) <http://goo.gl/4eB7Bo> accessed 1 April 2016

Perlroth N, ‘Hackers in China Attacked the Times for Last 4 Months’ *New York Times* (30 January 2013 <http://goo.gl/OMxZ4u>

Perlroth N & Krauss C, ‘A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try’ *New York Times* (15 March 2018) <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html> accessed 12 August 2019

Perlroth N & Sanger D, ‘New Computer Attacks Traced to Iran, Officials Say’ *New York Times* (24 May 2013) <http://goo.gl/NF01cW> accessed 1 April 2019

Petlevoï V, ‘Russian authorities step up cybersecurity’ *Russia Beyond* (27 January 2013) <http://rbth.com/politics/2013/01/26/russian_authorities_step_up_cybersecurity_22229.html> accessed 8 January 2017

Phillips D, ‘Estonia Charts Legal, Military Future of Cyber Warfare (Including Applicability of NATO’s Article V)’ (Cable 08TALLINN326_a, 22 September 2008) <https://goo.gl/QiY4gK> accessed 1 April 2016

Phillips D, ‘Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State’ (4 June 2017) <https://wikileaks.org/plusd/cables/07TALLINN366_a.html> accessed 1 July 2018

Phillips I & Isachenkov V, ‘Putin: Russia doesn’t hack but “patriotic” individuals might’ (*Associated Press*, 1 June 2017) <https://apnews.com/281464d38ee54c6ca5bf573978e8ee91/Putin:-Russian-state-has-never-been-involved-in-hacking?utm_campaign=SocialFlow&utm_source=Twitter&utm_medium=AP> accessed 13 August 2019

Pirker B, ‘Territorial Sovereignty and Integrity and the Challenges of Cyberspace’ *in* Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCD COE 2013)

Pisillo-Mazzeschi R, ‘The Due Diligence Rule and the Nature of the International Responsibility of States’ (1992) 35 GYIL

Plakokefalos I, ‘Causation in the Law of State Responsibility and the Problem of Overdetermination’ (2015) 26(2) EJIL

Proulx VJ, *Transnational Terrorism and State Accountability: A New Theory of Prevention* (Hart Publishing 2012)

Ragazzi M, *The Concept of International Obligations Erga omnes* (Clarendon Press 1997)

Randelzhofer A, ‘Article 2(4)’ *in* Bruno Simma (ed), *The Charter of the United Nations: A Commentary* (vol I, OUP 2002)

Rashid FY, ‘Inside the Aftermath of the Saudi Aramco Breach’ (Dark Reading, 8 August 2015) <https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676> accessed 11 August 2019

Razumovskaya O, ‘Russia and China Pledge Not to Hack Each Other’ *Wall Street Journal* (8 May 2015) <https://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/> accessed 1 July 2019

Reinisch A & Beham M, ‘Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State’ (2015) 58 GYIL

Reisman M & Armstrong A, ‘The Past and Future of the Claim of Preemptive Self-Defense’ (2006) 100 AJIL

Reisman MW, ‘The Enforcement of International Judgments’ (1969) 63(1) AJIL

Rid T & Buchanan B, ‘Attributing Cyber Attacks’ (2015) 38(1–2) J of Strategic Studies

Riddell A & Plant B, *Evidence Before the International Court of Justice* (BIICL 2009)

Riley M & Robertson J, ‘Russian Hacks on U.S. Voting System Wider Than Previously Known’ (*Bloomberg*, 13 June 2017) <https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections> accessed 28 July 2019

Roberts P, ‘Whodunnit? Conflicting accounts on ARAMCO hack underscore difficulty of attribution’ (*Sophos*, 30 October 2012) <https://goo.gl/R8opxE> accessed 1 April 2016

Robertson J, ‘A Decoy Computer Was Set Up Online. Which Countries Attacked It the Most’ *Bloomberg* (24 September 2014) <bloomberg.com/news/2014-09-23/a-decoy-computer-was-set-up-online--which-countries-attacked-it-the-most.html> both accessed 11 August 2019

Roche A, ‘Kremlin loyalist says launched Estonia cyber-attack’ *Reuters* (13 March 2009) <http://goo.gl/Wcq4oe> accessed 1 April 2016

Rodriguez E, ‘HOWTO - Spoofed DoS Attacks’ (*Skullbox*, 21 March 2011) <http://goo.gl/kwbq4K> accessed 1 April 2016

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP 2014)

Roscini M, ‘Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations’ *in* Jens David Ohlin, Kevin Govern & Claire Finkelstein (eds), *Cyber War* (OUP 2015)

Rosenne S, *The Law and Practice of the International Court 1920–2005* (4th edn, Brill/Nijhoff 2006)

Rowe B et al, ‘The Role of Internet Service Providers in Cyber Security’ (Institute for Homeland Security Solutions 2011)

Salmon J, ‘Duration of the Breach’ *in* James Crawford, Alain Pellet & Simon Olleson, *The Law of International Responsibility* (OUP 2010)

Sandifer DV, *Evidence before international tribunals* (University Press of Virginia 1975)

Sanger DE & Markoff J, ‘After Google’s Stand on China, U.S. Treads Lightly’ *New York Times* (14 January 2010) <http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology> accessed 13 August 2019

Schmitt MN, ‘Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’ (1999) 37 Colum J of Transnat'l L

Schmitt MN, ‘Cyber Operations and the Jus Ad Bellum Revisited’ (2011) 56(3) Villanova L Rev

Schmitt M (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013)

Schmitt MN, ‘“Below the Threshold” Cyber Operations: The Countermeasures Response Option and International Law’ (2014) 54(3) Virginia J of Intl L

Schmitt MN, ‘The Law of Cyber Warfare: Quo Vadis?’ (2014) 25 Stanford L & Pol Rev

Schmitt MN, ‘Cyber Responses “By The Numbers” in International Law’ (*EJIL: Talk!*, 4 August 2015) <http://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/> accessed 7 January 2018

Schmitt MN, ‘In Defense of Due Diligence in Cyberspace’ (2015) 125 Yale L J Forum <http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace> accessed 13 August 2019

Schmitt M (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

Schmitt MN, ‘Estonia Speaks Out on Key Rules for Cyberspace’ (Just Security, 10 June 2019) <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/> accessed 23 July 2019

Schmitt M, ‘France’s Statement on International Law and Cyber: An Assessment’ (Just Security, 16 September 2019) < https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/> accessed 12 February 2020

Schmitt M & Fahey S, ‘WannaCry and the International Law of Cyberspace’ (22 December 2017)

Schmitt M & Vihul L, ‘International Cyber Law Politicised: The UN GGE’s Failure to Advance Cyber Norms’ (Just Security, 30 June 2017) <justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> accessed 29 June 2019

Schmitt MN & Vihul L, ‘Proxy Wars in Cyberspace: The Evolving International Law of Attribution’ (2014) 1(2) Fletcher Security Rev

Schmitt MN & Vihul L, ‘Respect for Sovereignty in Cyberspace’ (2017) 95 Texas L Rev

Schrivjer N, ‘The Ban on the Use of Force in the UN Charter’ *in* Marc Weller (ed), *The Oxford Handbook on the Use of Force in International Law* (OUP 2015)

Schulhofe SJ, ‘An international right to privacy? Be careful what you wish for’ (2016) 14(1) Intl J of Constitutional L

Schulte C, *Compliance with Decisions of the International Court of Justice* (OUP 2004)

Schwarzenberger G, ‘The Principle of International Responsibility (087)’ *in* Hague Academy of International Law (ed), *Collected Courses of the Hague Academy of International Law* (Brill Nijhoff 1955)

Selby J, ‘Fact-finding before the Iran-United States Claims Tribunal: The View from the Trenches*’ in* Richard Lillich (ed), *Fact-finding before international tribunals* (Transnational Publishers 1992)

Shachtman N, ‘Kremlin Kids: We Launched the Estonian Cyber War’ (*Wired,* 13 November 2009) <http://goo.gl/OyIHL7> accessed 1 April 2016

Shackelford S & Andres R, ‘State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem’ (2014) 42(4) Georgetown J of Intl L

Shackelford S, Russell S & Kuehn A, ‘Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors’ (2016) 17(1) Chicago J of Intl L

Shanker T & Sanger DE, ‘U.S. Suspects Iran Was Behind a Wave of Cyberattacks’ *New York Times* (13 October 2012) <http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html> accessed 21 July 2019

Shaw MN, *International Law* (7th edn, CUP 2014)

Shelton D, ‘Righting Wrongs: Reparations in the Articles on State Responsibility’ (2002) 96(4) AJIL

Shelton D (ed), *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System* (OUP 2013)

Simma B & Pulkowski D, ‘Of Planets and the Universe: Self-contained Regimes in International Law’ (2006) 17(3) EJIL

Simoes AJG & Hidalgo CA, 'The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development’ (Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence, 2011) <http://atlas.media.mit.edu/en/visualize/stacked/hs92/export/prk/usa/show/2005.2015/> accessed 19 July 2019

Sklerov MJ, ‘Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent’ (2009) 201 Military L Rev

Smith B, ‘The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack’ (*Microsoft*, 14 May 2017) <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack> accessed 13 August 2019

Spencer D & Smeltzer M, ‘Nashi: Russian Youth Movement’ (translation, *School of Russian and Asian Studies*, 6 December 2011) <http://goo.gl/FNRTXK> accessed 1 April 2016

Stang G, ‘Global commons: Between cooperation and competition’ (2013) 17 European Union Institute for Security Studies Brief

Stapleton J, ‘Legal Cause: Cause-in-Fact and the Scope of Liability for Consequences’ (2001) 54 Vanderbilt L Rev

Stein A, *Foundations of Evidence Law* (OUP 2005)

Stephens T & Duncan French, ‘ILA Study Group on Due Diligence in International Law’ (2nd Report, ILA 2016)

Stokes M, Lin J & Hsiao R, ‘The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure’ (The Project 2049 Institute, 11 November 2011) <https://goo.gl/LuWhZN> accessed 1 April 2016

Symantec Security Response, ‘Flamer: Urgent Suicide’ (*Symantec*, 6 Jun 2012) <https://www.symantec.com/connect/blogs/flamer-urgent-suicide> accessed 28 July 2019

Symantec Security Response, ‘Mirai: what you need to know about the botnet behind recent major DDoS attacks’ (*Symantec*, 27 October 2016) <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks> accessed 28 July 2019

TAIA, ‘Russian Federal Security Service (FSB) Internet Operations Against Ukraine’ (TAIA Global Report, 2015) 4–5 <https://goo.gl/PMDY58> accessed 1 April 2016

Tarakanov D, ‘Shamoon The Wiper: Further Details (Part II)’ (*Kaspersky Lab*, 11 September 2012) <https://goo.gl/7wPP44> accessed 1 April 2016

Teitelbaum R, ‘Recent Fact-Finding Developments at the International Court of Justice’ (2007) 6(1) L & Practice of Intl Courts and Tribunals

Tellis AJ et al, *Measuring National Power in the Postindustrial Age* (Rand 2000)

Teti A, ‘Operation “Red October”: and it is Cyber Espionage’ (2013) 1 GNOSIS, L'Agenzia Informazioni e Sicurezza Interna <gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavigE/34-09.pdf/$File/34-09.pdf?openElement> accessed 18 May 2019

The ThreatConnect Research Team, ‘Khaan Quest: Chinese Cyber Espionage Targeting Mongolia’ (*ThreatConnect*, 7 October 2013) <https://www.threatconnect.com/khaan-quest-chinese-cyber-espionage-targeting-mongolia/> accessed 7 January 2018

The ThreatConnect Research Team, ‘Divide and Conquer: Unmasking China's 'Quarian' Campaigns Through Community’ (*ThreatConnect*, 11 November 2013) <https://www.threatconnect.com/blog/divide-and-conquer/> accessed 7 January 2018

Thompson A, ‘Applying Rational Choice Theory to International Law: The Promise and Pitfalls’ (2002) 31(1) J of L Studies

Thurlway H, ‘The Sources of International Law’ *in* Malcolm D Evans, *International Law* (4th edn, 2014 OUP)

Tikk E & Kerttunen M, ‘The Alleged Demise of the UN GGE: An Autopsy and Eulogy’ (Cyber Policy Institute 2017) <cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf> accessed 3 August 2019

Tikk E, Kaska K & Vihul L, *International Cyber Incidents: Legal Considerations* (CCD COE 2010)

Tikk-Ringas E, 'International Cyber Norms Dialogue as an Exercise of Normative Power' (2016) 17 (3) Georgetown J of Intl Affairs

Tonkin H, S*tate Control over Private Military and Security Companies in Armed Conflict* (CUP 2011)

Torruella Jr RA, 'Determining Hostile Intent in Cyberspace' (2014) 75 Joint Force Quarterly

Toth B, 'Estonia under cyber attack' (*Hun-CERT*, 2007) 1 <https://goo.gl/Zy9r8o> accessed 13 August 2019

Traynor I, 'Russia accused of unleashing cyberwar to disable Estonia' *The Guardian* (17 May 2007) <theguardian.com/world/2007/may/17/topstories3.russia> accessed 29 June 2019

TrendMicro, 'Utilising Island Hopping in Targeted Attacks' (25 September 2014) <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks> accessed 13 August 2019

Trend Micro, 'Hacktivist Group CyberBerkut Behind Attacks on German Official Websites' (*Trend Micro*, 20 January 2015) <http://goo.gl/lDtt3W/> accessed 1 April 2016

Tsagourias N, 'Cyber Attacks, Self-Defence and the Problem of Attribution' 17 (2012) J of Conflict and Security L

Tsagourias N, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' (2012) 15 Ybk of Intl Humanitarian L

Tsagourias N, 'Economic cyber espionage and due diligence' (Syracuse University, May 2015) <http://insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf> accessed 7 January 2018

Tzanakopoulos A, *Disobeying the Security Council: Countermeasures against Wrongful Sanctions* (OUP 2011)

UNIAN, 'Putin on Crimea: Russia has not annexed anything' (*Ukrainian Independent Information Agency*, 17 September 2016) <https://www.unian.info/politics/1526324-putin-on-crimea-russia-has-not-annexed-anything.html> accessed 1 July 2019

Väljataga A, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly' (CCD COE, 1 September 2017) <ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html> accessed 7 November 2017

Vallance C, ‘Ukraine cyber-attacks could happen to UK’ *BBC* (London, 29 February 2016) <http://www.bbc.co.uk/news/technology-35686493> accessed 1 April 2016

Van der Meer S, ‘Foreign Policy Responses to International Cyber-attacks’ (Clingendael Institute, September 2015) <https://bit.ly/2JQU4In>

Veeramachaneni K et al, ‘AI^2: Training a big data machine to defend’ (2016) IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (New York, 9–10 April 2016)

Vidalis S & Jones A, ‘Analyzing Threat Agents & Their Attributes’ in *Proceedings of the 5th European Conference on i-Warfare and Security* (Academic Conferences 2006)

Viswanatha A & Hong N, 'U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed’ (*Wall Street Journal*, 22 March 017) <https://www.wsj.com/articles/u-s-preparing-cases-linking-north-korea-to-theft-at-n-y-fed-1490215094> accessed 12 July 2019

Waincymer J, *Procedure and Evidence in International Arbitration* (Kluwer Law International 2012)

Walter C, ‘Obligations of States Before, During, and After a Cyber Security Incident’ (2016) 35 GYIL

Waltz K, ‘Realist Thought and Neorealist Theory’ (1990) 44(1) J of Intl Affairs

Waltz K, *Theory of International Politics* (Waveland Press 2010)

Wang Y et al, ‘Towards Street-Level Client-Independent IP Geolocation’ in *Proceeding NSDI'11 Proceedings of the 8th USENIX conference on Networked systems design and implementation* (USENIX March 2011)

Watts S, ‘International Law and Proposed U.S. Responses to the D.N.C. Hack’ (*Just Security,* 14 October 2016) <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack> accessed 13 August 2019

Waxman MC, ‘Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions’ (2013) 89 Intl L Studies

Weber M, *Economy and Society: An Outline of Interpretive Sociology* (Guenther Roth & Claus Wittich (eds), University of California Press 2013)

Wheeler DA & Larsen GN, ‘Techniques for Cyber Attack Attribution’ (IDA Paper P-3792, US Government Institute for Defense Analyses, 2003)

White ND, *The law of International Organisations* (2nd edn, Manchester University Press 2005)

White ND, 'Due diligence obligations of conduct: developing a responsibility regime for PMSCs' (2012) 31 (3) Criminal Justice Ethics

White ND & Abass A, 'Countermeasures and Sanctions' *in* Malcolm D Evans, *International Law* (4th edn, OUP 2014)

Wilson JQ & Kelling GL, 'Broken Windows' (1982) 249(3) Atlantic Monthly

Winckles A, 'Kill switches, sinkholes and how to stop a cyber attack' (*Anglia Ruskin University*, 19 May 2017) <http://www.anglia.ac.uk/news/kill-switches-sinkholes-and-how-to-stop-a-cyber-attack> accessed 28 July 2019

Wolfers A, '"National Security" as an Ambiguous Symbol' (1952) 67(4) Political Science Quarterly

Wolfers A, *Discord and Collaboration Essays on International Politics* (Johns Hopkins Press 1962)

Wolff C, *Jus Gentium Methodo Scientifica Pertractatum* [Argument on Scientific Methodology Regarding the Principles of Law Applicable to All People] (Joseph H Drake trans., William S. Hein & Co. 1995)

Wolfrum R, 'International Courts and Tribunals, Evidence' *in* Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (OUP 2012)

Woolf N, 'Massive cyber-attack grinds Liberia's Internet to a halt' *Guardian* (3 November 2016) <theguardian.com/technology/2016/nov/03/cyberattack-Internet-liberia-ddos-hack-botnet> accessed 23 July 2019

Wrange P, 'Intervention in national and private cyberspace and international law' *in* Jonas Ebbesson et al (eds), *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, (Brill/Nijhoff 2014)

Wright RW, 'Causation, Responsibility, Risk, Probability, Naked Statistics, and Proof: Pruning the Bramble Bush by Clarifying the Concepts' (1988) 73 Iowa L Rev

Xinhua, 'China publishes latest data of US cyber attack' *China Daily* (20 May 2014) <chinadaily.com.cn/china/2014-05/20/content_17519283.htm> accessed 1 July 2019

Xinhua, 'Stabilising economic growth "top priority"' *China Daily* (11 July 2012) <chinadaily.com.cn/business/2012-07/11/content_15568386.htm> accessed 24 February 2019

Yasmann V, ‘Russia: Monument Dispute with Estonia Gets Dirty’ *Radio Free Europe* (4 May 2007) <http://goo.gl/fbSMLG> accessed 1 April 2016

Yasuaki O, ‘International Law in and with International Politics: The Functions of International Law in International Society’ (2003) 14(1) EJIL

Yiallourides C, Gehring M & Gauci JP, *The Use of Force in relation to Sovereignty Disputes over Land Territory* (British Institute of International and Comparative Law 2018)

Zemanek K, ‘Armed Attack’ in *Max Planck Encyclopedia of Public International Law* (October 2013) <https://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e241?rskey=FxjPfU&result=1&prd=EPIL> accessed 26 January 2019

Zetter K, ‘Everything We Know About Ukraine’s Power Plant Hack’ (*Wired*, 20 January 2016) <http://goo.gl/DkScZ2>

Zoller E, *Peacetime Unilateral Remedies* (Transnational Publishers 1984)