STRATHMORE LAW SCHOOL

ATTRIBUTION AND STATE RESPONSIBILITY IN CYBER WARFARE: A CASE STUDY OF THE NOTPETYA ATTACK

Submitted in partial fulfilment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

WANDUGI LEWIS KIIRU

095832

Prepared under the supervision of

Mr. Allan Mukuki

December 2019

Word count (26,477)

Contents

Declaration

I, WANDUGI LEWIS KIIRU, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed: .....

Date: .....

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed: .....

Mr. Allan Mukuki

Acknowledgments

I am especially thankful for the invaluable assistance afforded to me by Mr. Allan Mukuki who has guided me through the period of my writing of this dissertation and has gone over and above his duty in his capacity as supervisor. I would also like to acknowledge the support I received from my family.

Abstract

This dissertation addresses attribution and the attaching of state responsibility in cyber-attacks using primarily a case study methodology. It seeks to address its three objectives: an analysis on the threshold in which cyber-operation could be considered a cyber-attack, look into the relevant issues on establishing state responsibility and the standards of proof; and a further analysis on the possible consequences for a state-attributed cyber-attack. The methodology used to conduct this research was desk research with the relevant materials being analysed to give relevant insight as well as a case study to put the discourse into context which will have a direct impact on this paper's hypothesis.

List of Cases

Permanent Court of Arbitration (PCA) cases

Air Service Agreement of 27 March 1946 between the United States of America and France, Arbitral award, Permanent Court of Arbitration, 1978.

Eritrea-Ethiopia Claims Commission - Partial Award: Jus Ad Bellum - Ethiopia's Claims 1-8, Reports of International Arbitral Awards, 2005.

Liability of Germany for Damage caused in the Portuguese colonies in South Africa (Germany v. Portugal), Arbitral award, Permanent Court of Arbitration, 1928.

Liability of Germany for acts committed after 31 July 1914 and before Portugal took part in the war (Portugal v. Germany), Arbitral award, Permanent Court of Arbitration, 1930.

International Court of Justice case law

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

Asylum Case (Colombia v. Perú), Judgment, ICJ Reports 1950.

Barcelona Traction (Belgium v. Spain), ICJ Reports 1970.

Case Concerning Application of the Convention on The Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgement, ICJ Reports 2007.

Case Concerning Avena and Other Mexican Nationals (Mexico v. United States of America), Judgement, ICJ Reports 2004.

Case Concerning the Gabcikovo-Nagumaros Project (Hungary v. Slovakia), ICJ Reports, 1997.

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

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US), ICJ Reports 1986.

Oil Platforms (Iran v. U.S.), Judgment, ICJ Reports 2003.

The Corfu Channel Case (Assessment of the amount of compensation due from the People's Republic of Albania to the United Kingdom of Great Britain and Northern Ireland), ICJ Reports 1949.

The Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua Intervening) (El Salvador v. Honduras), ICJ Reports 1992.

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

International Criminal Tribunal for the former Yugoslavia (ICTY) case law

Prosecutor v Tadic (Sentencing Judgment), Case No. IT-94-1-T, ICTY, 14 July 2007.

List of legal instruments

International instruments

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

Convention on Cybercrime, 23 November 2001, ETS No. 185.

Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949, 75 UNTS 135.

Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), 12 August 1949, 75 UNTS 135.

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3.

Statute of the International Court of Justice, 26 June 1945, 33 UNTS 933.

The North Atlantic Treaty, 4 April 1949.

Vienna Convention on Diplomatic Relations, 18 April 1961.

Vienna Convention on the Laws of Treaties, 23 May 1969, 1155 UNTS 331.

List of acronyms and abbreviations

ARISWA	Articles on State Responsibility
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CIL	Customary International Law
DDoS	Distributed Denial of Service
GRU	Glavnoye Razvedovatel'noye Upravlenie
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
IP	Internet Protocol
ICTY	International Criminal Tribunal for the former Yugoslavia
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NSA	National Security Agency
TOR	The Onion Router
UN	United Nations
US	United States of America
UK	United Kingdom
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
VPN	Virtual Private Network

CHAPTER 1

1.1. INTRODUCTION

1.2. Background

International law has regulated war and the limits to acceptable wartime conduct.[1] These regulations, especially international customary law, speak to the more traditional means through which war takes place.[2] In view of the existing law governing war and wartime conduct and technological developments in cyberspace, it is necessary to examine the extent to which these regulations are applicable to cyber warfare as one of the means of modern warfare.[3] Questions on cyber-security are becoming common place evidence of the increasing awareness of the threat posed by cyber-attacks.[4]

Yelena Tumanova, mother to a 21-year-old service man who was torn apart by a rocket attack in Eastern Ukraine on August 13th, only learnt about his son's death through his comrade who scooped up his lifeless body. However, according to the Kremlin not a single Russian soldier had entered Ukraine to support pro-Russia separatists militia.[5] Russia's undeclared war has seen it turn Ukraine into a scorched-earth testing ground for Russian cyber-attack tactics.[6] In June 2017, a group of Kremlin-linked hackers, released a piece of malware that became known as NotPetya.[7] The effect of this malware was disastrous, to say the least, with figures to the tune of an upwards of 1.2 billion in company losses.[8] The wounds are still fresh.

---

[1] https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm - on Saturday, 1st December 2018.

[2] https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2567&context=faculty_scholarship –on Saturday, 1st December 2018.

[3] https://www.nato.int/cps/en/natohq/topics_78170.htm - on Saturday, 1st December 2018.

[4] https://edition.cnn.com/2018/05/06/opinions/opinion-andelman/index.html - on Saturday, 1st December 2018.

[5] https://www.telegraph.co.uk/news/worldnews/europe/russia/11314817/Secret-dead-of-Russias-undeclared-war.html - on Friday, 14 December 2018.

[6] https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html - on Friday, 14 December 2018.

[7] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ - on Friday, 14 December 2018.

[8] https://www.cfr.org/blog/year-review-malware-attacks-impact-operations-and-bottom-line - on Friday, 14 December 2018.

In cyber-space, battle fields, in the classical sense, are reduced to keyboards and the ammunition is in binary. Finding out who did what becomes a daunting task due to the anonymous nature of cyberspace.[9] It is established that international law is applicable to cyber-warfare, this position is also buttressed by the wording of Rule 80 of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual), as it notes that international law applies to cyber warfare. The law of state responsibility concerns states while attribution standards establish which acts are state or public acts for which the state can be held responsible.[10] It is within these parameters that this paper seeks to delve into a detailed analysis of the NotPetya attack.

1.3. Statement of problem

Being aware of the fact that the ambit of cyberspace and consequently cyberwarfare is uncertain, this paper will now point to three main distinct sources of uncertainty;[11]

a) Blurring of distinctions previously believed to be solid such as what is public or private.
b) Novelty of cyber-attacks and the consequent difficulty in attributing them to actors.
c) The lack of historical experience and reliance on metaphors and analogies.

The second source of uncertainty shall form the main focus of this paper as the attribution factor is invariably linked to establishing state responsibility for particular acts of cyber-aggression.[12] Owing to the complexities of attribution and establishing a state as being responsible for cyber-attacks,[13] the paper shall mitigate the complexity of a generalization to

---

9 http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/McDougall_20161021.pdf - on Friday, 14 December 2018.

10 https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1 – on Friday, 14 December 2018.

11 Kessler O and Werner W, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' *Leiden Journal of International Law* 26, 2013, 798. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/F72E80E8768C66B8C0CBEBB413E643C5/S0922156513000411a.pdf/expertise_uncertainty_and_international_law_a_study_of_the_tallinn_manual_on_cyberwarfare.pdf on Tuesday, 19 February 2019.

12 Tsagourias N, 'Cyber-attacks, self-defence, and the problem of attribution,' *Journal of Conflict and Security Law* 17(2), 2012.

13 Tran D, 'The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack' 20 *Yale Journal of Law and Technology* 2018, 387.

attribution by utilizing contemporary literature to attempt to explicate and contextualize the NotPetya attack.

1.4. Objectives

Primacy shall be to set out and apply the attribution standards and attempt to attach responsibility to a specific instance of cyber-aggression which has already met the criteria for a cyber-attack. This flows from the preceding objectives which are, firstly, to establish the threshold where a cyber-operation could be considered a cyber-attack. Thereafter, to inform this paper on state responsibility and standards of proof when it comes to cyber-attacks. Link the tests for establishing state responsibility to the NotPetya attack. Lastly, to bring out the possible consequences in the event it is established that a state has perpetrated unlawful acts of cyber-aggression.

1.5. Research questions

This research will seek to investigate through a case study of the NotPetya attack; as to what extent is a cyber-operation considered to be an act of aggression? How would responsibility be attached to an offending state and the standard of proof when it comes to cyber-attacks? This is with the view of conducting an inquiry into its applicability in the NotPetya attack. What are the consequences in the event a state is deemed to have committed such unlawful attacks?

1.6. Hypothesis

These research questions are directed towards answering the hypothesis that establishing state responsibility when it comes to cyber-attacks is a challenge in the context of existing international laws and customs regulating cyber-warfare, therefore, rendering states, companies and people worldwide vulnerable to indiscriminate acts of cyber aggression. The logical conclusion following the bad man theory.[14]

1.7. Justification of the study

The importance of this paper should not be understated. As the discourse of state responsibility regarding cyber-warfare is mainly theoretical, this research seeks to add flesh

[14] Jimenez M, 'Funding the good in Holms's bad man' 79(5), *Fordham Law Review*, 2011, 2098.

to it and consequently, gain better incite to the highly controversial attack that still sparks international debate to this day with various governments such as the United Kingdom and the United States of America pointing fingers at Russia.[15] This will potentially aid in analyzing state conduct with the view of establishing or absolving responsibility of states in cyber-attacks. It has been noted that contemporary challenges presented within the scope of state responsibility, such as the inconclusively of the current formulation dealing with questions concerning state responsibility, do merit a discourse on the same.[16]

1.8. Theoretical Framework

This paper asserts that in an international arena where acts could not be attributed to a particular state actor and responsibility attached the result would be an unmitigated frenzy of indiscriminate use of such means to advance their own interests since there will be little to no risk of incurring the potential penalties. Although Oliver Wendell Holms' view of law as being predictive in terms of what will be decided by the determining courts and other legal institutions will do, essentially how the law functions,[17] this paper, however, contends that this although instructive, will further a partial reliance to the extent that rather than a prediction of what courts will do (as is the focus of American Legal Realism) or the extremely external view of the "bad man" it should maintain the Realist emphasis on prediction, while accommodating positivist insights when it comes to the psychology of effective sanction-regimes that is; they are internally binding regardless of whether they are never permanent or uncontested.[18]

That this paper relies on another theory differing from proponents of the rational choice paradigm to articulate how Customary International Law works (CIL), why states comply and why and how rules change due to the inadequacies within them. Fundamentally, that their conclusions often contradict traditional CIL doctrine and the understanding of the legal mechanism consisting of lawyers, judges, and officials as to how CIL works serving to

[15] https://www.bbc.com/news/uk-politics-43062113 - on Friday, 14 December 2018.
[16] Makory C, 'Cyberwarfare regulation: A liability and regulation disquisition' Unpublished LLB Dissertation, Strathmore University Law School, Nairobi, 2018, 36.
[17] Holms O, 'The path of the law', *Harvard Law Review*, 457, 1897, 17.
[18] Mitchelle R, 'Sovereignty and normative conflict: international legal realism as a theory of uncertainty' *58 Harvard International Law Journal*, 2, 2017, 435. http://www.harvardilj.org/wp-content/uploads/HLI204_crop.pdf on Tuesday, February 19, 2019.

obstruct the dialogue between explanatory and normative or doctrinal debates about CIL.[19] The theory that this paper proposes takes into account that CIL advances new legal and institutional features[20]as well as applying common knowledge that CIL is accompanied by a shared understanding of its workings which run against a "tit for tat" balance based on direct reciprocity. This, although undermining decentralized punishment mechanisms as advanced by previous theories, leads to an alternative rationale for compliance in which a state may comply because of the fact that it knows its decision to defer creates a precedent that may undermine a cooperative norm it values and may be restated thus: that where a state (the actor in this case) can defect from a norm and retained cooperation from another norm it values it may choose the alternative for defection and still enjoy the continued compliance by others.[21]

1.9. Literature Review

1.9.1. The extent to which a cyber-attack is considered an act of aggression

In Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel's paper *'the Law of Cyber-Attack',* they provide a diagrammatical representation of cyber-operations with respect to varying criteria which can be expressed as follows;[22]

1) Cyber-crime involves violations by non-state actors and must be a violation of criminal law which is committed by means of a computer system.
2) Cyber-attack and cyber warfare both fit in the criterion of having the intention to undermine a computer network as well as having a political or national security purpose.

[19] Verdier P and Voeten E, 'Precedent, compliance and change in customary international law: an explanatory theory' 108 *American Journal of International Law*, 389, 2014, 390.
[20] These consist of detailed obligations, flexibility clauses, and structured countermeasures-to support reciprocity or retaliation.
[21] Verdier P and Voeten E, 'Precedent, compliance and change in customary international law: an explanatory theory' 108 *American Journal of International Law,* 389, 2014, 391.
[22] Hathaway A, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W and Spiegel J, 'the law of cyber-attack' 100 *California Law Review*, 817, 2012, 823.

3) That the effects must be equivalent to an armed attack or activity take place in the context of an armed conflict is the criterion that distinguishes cyber-attacks form cyber-warfare with the latter falling within this scope.

It is important for this paper, at this point, to briefly highlight the significance of these distinctions or risk the confounding of this concept. From the above distinctions, it is undoubtedly clear that cyber-attacks and cyber-warfare are analogous to the extent that they both fit in the second criterion, in essence, both have the intention aspect of undermining a security network coupled with having a political or national security purpose. Both directly in the ambit of primarily state actors. This paper will make reference to cyber-attacks and cyber-warfare in this manner as it is concerned with attaching state responsibility as opposed to responsibility on independent actors.

Further, in the article '*Offensive Cyber Operations and the Use of Force*' by the author Herbert S. Lin, postulates that the question to ask is not what constitutes a use of force, instead, the question to be asked is whether a cyber-attack with a specified effect constitutes a use of force. Informed by Article 51 of the United Nations (UN) Charter, he advances that such direct and indirect effects would constitute an armed attack if produced by other means. Following this such a cyber-attack would be treated in the same manner as an armed attack.[23]

According to author Michael N. Schmitt in his article, '*Cyber Operations and the Jus Ad Bellum Revisited*', he notes cyber-operations do not fall squarely into the paradigm of use of force according to article 2(4) of the UN Charter, that although they are not forceful (they do not use kinetic means) their possible consequences could range from mere annoyance to death. Acknowledging that the term "use of force" denotes kinetic means and their resultant consequences, he asserts that it would be no less absurd to suggest that cyber-attacks whose consequences are analogous to those resulting from kinetic force lie beyond the scope of the prohibition than to exclude other non-kinetic means such as biological or radiological warfare. Logically, cyber-operations that directly result or a

[23] Lin H, 'Offensive cyber operations and the use of force' 4 *Journal of National Security Law and Policy* 63, 2010, 73.

likely to result in physical harm to individuals or tangible objects equate to armed force and consequently constitute uses of force.[24]

1.9.2. State responsibility and the standard of proof in cyber-attacks

Cynthia Jade Makory, in her writing of '*Cyberwarfare regulation: A liability and regulation disquisition*', duly noted that if a state's agent attacks another state the hostile conduct is indeed attributable to that state.[25] When it comes to state responsibility, the Draft Articles on State Responsibility (ARISWA) is the primary reference point although serving as soft law.[26] Article 1 of the same provides that internationally wrongful acts ought to be attributed to the state responsible of such acts and international responsibility is required.[27] This is in line with state practice and *opinio juris*.[28]Analogously, Rule 6 of the Tallinn Manual provides that a state is legally responsible for cyber-operations attributable to it.[29]

It is prudent to note that the International Court of Justice (ICJ) neither requires specific standards of proof nor indicate probative methods of proof to be considered by the court in order to meet a certain standard.[30] Informed by this, Marco Roscini in his article, '*Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations',* went on to discuss the issue noting the difficulty and undesirability of the identification of a common standard of proof that would be applicable in inter-state litigation generally. He does adopt the view that there are indications, for instance, that claims relating to jus ad bellum in particular in relation to the invocation of an exception to the use of force in international relations have been considered as requiring clear and convincing evidence. The inquiry that would consequently follow would be that considering that use of armed

[24] Schmitt M, 'Cyber operations and the jus ad bellum revisited' 56 *Villanova University Charles Widger School of Law* 3, 2011, 573. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1019&context=vlr on Tuesday, 19 February 2019.
[25] Makory C, 'Cyberwarfare regulation: A liability and regulation disquisition' Unpublished LLB Dissertation, Strathmore University Law School, Nairobi, 2018, 36.
[26] Makory C, 'Cyberwarfare regulation: A liability and regulation disquisition' Unpublished LLB Dissertation, Strathmore University Law School, Nairobi, 2018, 35.
[27] Article 1, ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[28] Gervais M, 'Cyber-Attacks and the Laws of War' 30 *Berkeley Journal of International Law* 2, 2012.
[29] Rule 6, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' *New York: Cambridge University Press (2013).*
[30] Statute of the International Court of Justice, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, 1978 I.C.J. Acts & Docs. 6.

force the standard of proof used would be that of clear and convincing evidence, would their exist a special and lower standard in the cyber context especially considering claims of self-defence against cyber operations?[31]

Karine Bannelier-Christakis, in the author's literature, '*Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations*' she brings out the knowledge aspect in order to prove intent as applied by the ICJ in its decision in the case of *United States of America v Iran*[32], to engage responsibility on Iran's part by establishing that the Iranian authorities;

a) Firstly, by virtue of the prescription under the Tallinn Manual at Rule 5 providing that states shall not allow cyber infrastructure in its territory or under its exclusive governmental control to be used for acts that have adverse effects to other states,[33] which was not positively satisfied.
b) were fully aware of the urgency on the need for action on their part,
c) had the means to perform their obligations,
d) and completely failed to comply with these obligations.

Because states exercise exclusive control over its territory, proof of a state's knowledge as to the acts would become an evident *probatio diabolica*[34] for victims. The ICJ, to avoid this situation, in its judgement of the *Corfu Channel case*[35] found that it should be allowed a more liberal recourse to interference of fact and circumstantial evidence, provided they do not leave room for reasonable doubt in the former.[36]

When it comes to responsibility of states when cyber-operations were carried out by a non-state actor, Michel N. Schmitt and Liis Vihul in their article, '*Proxy Wars in Cyberspace: The International Law of Attribution*' the authors find that direct control of non-state actors

[31] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations' 50 *Texas International Law Journal*, 2015, 250.
[32] *United States Diplomatic and Consular Staff in Tehran*, Judgment, ICJ Reports 1980, 3.
[33] *Rule 5, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2013).*
[34] Probatio diabolica/devil's proof law is defined as a legal requirement to achieve an impossible proof. https://definitions.uslegal.com/p/probatio-diabolica-devils-proof/ on Tuesday, February 19, 2019.
[35] *The Corfu Channel Case (Assessment of the amount of compensation due from the People's Republic of Albania to the United Kingdom of Great Britain and Northern Ireland),* ICJ Reports 1949.
[36] Christakis K, 'Cyber diligence: a low intensity due diligence principle for low intensity cyber operations' 14 *Baltic Yearbook of International Law*, 7, 2014.

by the state is limited to the conduct of specific operations. This is contrasted with merely supplementing a state's activities or assuming responsibility for a particular function. Their article further notes that the ICJ, in a standard that is acknowledged by the International Law Commission, determined the critical requirement of effective control over the non-state actor by the state for responsibility to be established on the latter actor.[37]

1.9.3. Consequences in the event that responsibility attaches on a state in a cyber-attack

Brian J. Egan, the author of the article, '*International Law and Stability in Cyberspace',* noted that the victim state has certain avenues of recourse when responsibility is attached, such as the option of states to undertake any unfriendly acts which are not inconsistent with any of its international obligations to influence the behaviour of other states. These acts are referred to acts of retorsion[38].[39]

This paper recognizes that article 2(4) of the United Nations Charter has two exceptions such that the use of force is permissible when undertaken as part of collective security operations or where it is done out of self-defence.[40] Article 39 of the UN Charter provides for the exception authorizing the United Nations Security Council may determine existence of threats to peace, breach thereof or acts of aggression and consequently make recommendations or decide appropriate restorative measures for international peace.[41] The Security Council is given the freedom to employ other means that may not constitute the use of force, unless the use of such force becomes unavoidable by virtue of Article 41 and 42 of the UN Charter.[42] Article 51 then provides for the other exception where use of force is acceptable under the right of an individual to self-defence if an armed attack occurs, in this case, it applies to such acts that are at the degree of cyber-attack to cyber-warfare.[43]

---

[37] Vihul L and Schmitt M, 'Proxy wars in cyberspace: the evolving international law of attribution' 1 *Fletcher Security Review* 62, 2014.
[38] These include the imposition of sanctions or declaration that a diplomat is persona non grata.
[39] Egan B, 'International law and stability in cyberspace' 35 *Berkeley Journal of International Law* 1, 2017, 178. https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf on Wednesday, February 20, 2019.
[40] Article 2(4), *Charter of the UN*.
[41] Article 39, *Charter of the UN*.
[42] Article 41 and 42, *Charter of the UN*.
[43] Article 51, *Charter of the UN*.

1.10. Research Design

This paper will proceed primarily relying on qualitative research utilizing varying sources of literature. In essence, this shall be through use of secondary sources such as books, journals articles and reports by exemplary authors when it mainly to attributing certain cyber-operations to state actors and establishing responsibility. Case law shall also form part of this papers approach more so, on issues relating to enforcement and advisory opinions necessary for evaluating the unresolved issues this paper contends with. This dissertation shall attempt to interview state actors to add to the depth of the discourse.

A single case study shall be used qualitatively to guide this paper's discourse descriptively, to contextualize the real-life application which has occurred. The author concedes that the major motivation of this case study is, in large part, exploratory.

1.11. Assumptions

a) That the existing contemporary literature will be adequate to relate the various dynamics of the case study this paper seeks to tackle considering relatively novel aspects that accompany cyber-operations.

b) As is common in the discourse on cyber-warfare, the lack of a clear definition of what cyber warfare is. Therefore, using the interpretive model within the framework of jus ad bellum to then attempt to apply attribution standards towards establishing state responsibility.

1.12. Limitations

Owing to the nature of cyber-operations that involve sensitive and largely classified information not in the public domain, primary sources of such information is inaccessible. This paper's primary focus is on the legal issues owing to the lack of required expertise in the thoroughly technical scope that constitutes cyberspace.

That although the author will attempt to use means of data collection such as interviews, information that could be key to guide the discourse may be left out and save from declassified documents only public information will be used throughout. One could view this as an external observer looking in. This is aside from the difficulty in procuring interviews

with relevant state actors. The author will be unable to source interviews from the state actors that are directly relevant and primary to this discussion.

1.13. Chapter Breakdown

Chapter 1 will provide an introduction to the dissertation, a statement of the problem to be tackled, a justification of the inquiry, the hypothesis, assumptions made in the research, research objectives, research questions, the theoretical framework and limitations of the dissertation.

Chapter 2 will cover discussions around the scope of use of force where a cyber-operation could be considered as an act of aggression.

Chapter 3 will cover state responsibility and the aspects of standard of proof in cyber-attacks.

Chapter 4 serves to bring out the possible consequences when responsibility is attached to state actors and the resultant effects.

Chapter 5 will provide recommendations in line with the findings of this dissertation. Thereafter, provide a conclusion to this paper.

CHAPTER 2

Cyber-attack - An act of aggression?

2.1. Introduction

This chapter is the initial stage towards proving or disproving the dominant hypothesis in this dissertation, particularly, the nexus between cyber-attacks and acts of aggression in answering the first research question as set out in Chapter 1. The premise of this chapter – as the corresponding research question suggests as having a threshold determining approach – is hardly contentious.

At this point it is important to distinguish between international actors, which are states in most cases and non-state actors in order to have a basic understanding of this duality. In International Humanitarian Law (IHL) "armed attack" is a legal term referring to two different types of conflict; international armed conflicts which fits into the former distinction and non-international armed conflicts, as in the latter distinction, either between a state and an organised armed group or between organized armed groups. In any other event not qualifying as any of these two human rights law and domestic law will be applicable as opposed to IHL.[44] Unlike the concept of armed attack, the prohibition of the use of force and the instance of armed attack - which, if established, confers upon a state the right of self-defence – are creatures of a different body of law known as *jus ad bellum* which has as its primary source the UN Charter which regulates state to state conduct as opposed to individuals or state to individuals.

The first step in this interrogation would, of necessity, require an interpretive approach of the UN Charter. This should be in good faith, in accordance to the ordinary meaning of the terms of the treaty in question as used contextually and in line with its object and purposes.[45] Terminologies that are the subject of this chapter include "force" "armed" and "attack" as used in the relevant treaties. In Article 2(4) of the UN Charter, "armed" does not appear with "force". This can be contrasted with the wording as per the preamble of the same Charter which uses "armed force" when excluding the use of such except when in the common

[44] Schmitt M, '" Attack" as a term of art in international law: the cyber operations context' 4th International Conference on Cyber Conflict, International Law Department, United States Naval War College, Newport, 2012, 285.

[45] Article 31, *Vienna Convention on the Laws of Treaties*, 23 May 1969, 1155 UNTS 331.

interest. In the same manner, "armed force" is used when excluding it form those non-forceful Security Council measures which it may authorize[46] as well as when referring to planning for "armed force" vis a vis forceful measures [47]. "Armed attack" is similarly used in delineating the instance when forceful defensive actions are allowed.[48]

Apparent conflation between these terms creates an ambiguity that may be cured with a dose of supplements (referring to the VCLT's provision for supplementary means of interpretation).[49] These include the relevant preparatory works and circumstances of its conclusion. To begin with, a proposal to extend the scope of Article 2(4) to include economic coercion was rejected as indicated by the Charter's *travaux preparatoirs*.[50] On a related premise, the issue of whether force included all forms of pressure - presumably extending the Article's applicability of force to include political or economic pressure threatening territorial integrity or political independence of a state - arose and was negated in proceedings that precede the UNGA's Declaration on Friendly Relations.[51] By way of inference, as force is neither political nor economic pressure it may then be asserted that cyber-operations having the character of political or economic coercion do not fall within the ambit of prohibited uses of force. Also the proposals to limit "force" to "armed force" and otherwise limit the extent to which force would be considered an armed attack were similarly rejected.[52] From the antecedent premise, this dissertation advances that "force" is not synchronous with "armed force" thereby solidifying the basis their distinction in the discussion that follows.

This chapter moves to interrogate the relevant categories which the paper advances having informed itself of the variances ensuing from particular instances. It now looks into: Cyber-operations with the character of a use of force and cyber-operations having a character falling within the categorization of an armed attack. Both are determinations to be made within the ambit of *jus ad bellum* – established norms in conflict management of an international nature involving states directing or precluding instances when force may be used in dispute

[46] Article 41, *Charter of the UN*.
[47] Article 42, *Charter of the UN*.
[48] Article 51, *Charter of the UN*.
[49] Article 32, *Vienna Convention on the Laws of Treaties*.
[50] Schmitt M, 'Cyber Operations in international law: The use of force, collective security, self-defense and armed conflicts,' *Durham University Law School*, 2010, 154.
[51] Schmitt M, 'Cyber Operations in international law', 155.
[52] Schmitt M, 'Cyber Operations in international law', 155.

resolution.[53] A further analysis of *jus in bello* considerations will be included to contextualize the larger implications arising out of cyber-operations.

2.2. Cyber-operations with the character of a use of force

This stems from the International law prohibition on states from the threat or use of force as against another state and by extension, the principle of non-intervention[54] by virtue of Articles 2(4) and 2(7) of the UN Charter respectively. At this point and in reference to the preceding statement, this dissertation takes cognizance of the fact that the inherent individual or collective right to self-defence in response to armed attacks acts as an exception.[55] This position was affirmed by the International Court of Justice (ICJ) where, after finding against a purported right of intervention in support of an opposition within another state, concluded that acts in contravention with the CIL principle of non-intervention through either direct or indirect characterizations of the use of force will invariably amount to a breach of the principle precluding use of force in international relations.[56]

The UN Charter and international bodies have but vaguely defined the term "use of force" [57] consequently, there being no international consensus, individual nations may assert different definitions and apply different thresholds for what it constitutes.[58]

The Corfu Channel case demonstrates the intricacies at play in determining whether particular actions constitute uses of force. Basing their actions primarily on the legal exercise of their right of passage - which was upheld by the ICJ,[59] the ICJ held that the action of the British in sending warships through the channel was not in violation of Albania's sovereignty but that their action in sending an armed force in Albanian territorial waters to remove mines on November 12th and 13th, 1946 was a violation of international law and described it as a policy of force, prone to abuse, with no place in international law.[60] The ICJ by not expressly

[53] Moore J, 'The use of force in regulating international relations: Norms concerning the initiation of coercion' in Moore J and Turner R, *National Security Law*, 2nd ed, Carolina Academic Press, Durham, North Carolina, 2005, 69.
[54] Makory J, 'Cyberwarfare regulation', 21.
[55] Article 51, *Charter of the UN*.
[56] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US)*, ICJ Reports 1986, 99, para.209.
[57] Barkham J, 'Information warfare and international law on the use of force', 70.
[58] Unclassified Senate Testimony by Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command, April 15, 2010.
[59] *The Corfu Channel Case (United Kingdom v Albania)*, ICJ Reports, 1949, 30
[60] *The Corfu Channel Case*, ICJ, 35.

declaring it an illegal use of force, impliedly put it out of the scope of an Article 2(4) violation. Albania's actions to fire on the British ships was similarly characterized as a use of force (19).[61]

This dissertation further moves to an analysis following the parameter of consequence as a base for which the author Michael N. Schmitt in his article *"Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework,"* laid out a criterion consisting of several factors for analysing uses of forces with basis in the recognition that states balance their freedom of action which favours a low threshold and avoidance of harmful consequences that acts as an incentive for setting a higher threshold.[62] He asserts that the approach he proposed has endured.[63] It consists of an analysis of the following factors; Severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.

2.2.1. Severity[64]

Consequences that involve physical harm to individuals and property, this fact alone amounts to a use of force. Consequences that can be categorized as a minor inconvenience or irritation will never amount to a use of force. Considering these two extreme positions, the more that, as a consequence, critical national interests are infringed upon, the more the act will lead to a characterization of the operation as a use of force. This factor is seen as the most significant as the subsequent ones, such as duration of the consequences, will qualify it.

2.2.2. Immediacy[65]

This considers the period of time when the consequences manifest coupled with a state's opportunity in which it may seek peaceful accommodation or otherwise obstruct the operation's harmful effects. It would proceed in a manner that if the consequences of the cyber-operation manifest sooner the more it would resemble the characteristic immediacy of an armed attack and accord a state less opportunity to seek peaceful accommodation or

[61] *The Corfu Channel Case*, ICJ, 19.
[62] Schmitt M, 'Computer network attack and use of force in international law: Thoughts on a normative framework,' 37, *Colombia Law Journal of Transnational Law*, 1999, 914-916.
[63] Schmitt M, 'Cyber Operations in international law', 155.
[64] Schmitt M, 'Cyber Operations in international law', 155.
[65] Schmitt M, 'Cyber Operations in international law', 156.

prevent the effects in question. Consequences that are delayed or build slowly over time are of a lesser concern to states.

2.2.3. Directness[66]

What is considered under this is the chain of causation between the initial act and the consequences that arise as a result of it such that the greater the reduction in relation between the initial action and the consequences borne out of the it the less likely states will deem the actor responsible and in violation of the use of force prohibition. The consequences of armed force are more directly linked to the *actus reus* as opposed to other means of economic coercion, therefore, the use of force prohibition precludes negative consequences with greater certainty and will not depend on contributory factors to operate unlike in the latter instance.

2.2.4. Invasiveness[67]

This considers penetration to the particular system. The higher the level of security of the targeted system the more the concern as to the fact of its penetration. Contrast the operation of armed coercion which may involve crossing into the state which is its target on one hand and an instance of economic coercion which may not involve any intrusion at all. In the former instance the acts may infringe upon the rights of a state which qualifies as a use of force devoid of legal justification while the latter instance is clearly not a use of force.

2.2.5. Measurability[68]

In applying this factor, it would follow that the more identifiable and quantifiable the consequences of a particular action are the more a state's interests will be deemed to have been negatively affected. In considering this, an act of armed coercion would qualify even if the consequence is only a limited degree of destruction. In the converse, an act of economic coercion it is difficult to identify or quantify the consequent harm. Regardless, economic coercion is not viewed as a prohibited use of force in international law.

[66] Schmitt M, 'Cyber Operations in international law', 156.
[67] Schmitt M, 'Cyber Operations in international law', 156.
[68] Schmitt M, 'Cyber Operations in international law', 156.

2.2.6. Presumptive Legitimacy[69]

The nature of international as well as domestic law is generally prohibitory. Logically, acts which are not expressly prohibited are impliedly permitted. International law governing use of force does not prohibit espionage or other means of coercion not otherwise armed coercion. To the degree that these operations are carried out in cyber space they are necessarily presumed to be legitimate.

2.2.7. Responsibility[70]

When considering actions among states, the greater the nexus between a state and the operations, the more likely other states are to categorize it as a use of force due to the heightened risk of international stability being threatened. State responsibility lies along a spectrum from actions which a state is only involved in some fashion to actions solely conducted by a state.

2.2.8. A use of force analysis on NotPetya

Considering severity, according to a White House assessment, the cost of NotPetya was in upwards of 10 Billion Dollars in total damages.[71] Described as an almost global pandemic, NotPetya crossed Ukraine's boarders. It impacted several ministries of the Ukrainian government, companies in the country that operate critical infrastructure[72] and multinational companies with either branches or subsidiaries in Ukraine.[73]

The effects of the virus were nearly immediate such that, in a matter of hours, it is estimated that ten percent of all computers in the country were destroyed.[74]

Servers at the headquarters of Linko's group, whose purpose were to push out updates for an accounting software known as M.E.Doc routinely, served as the ground zero for the attack.

---

[69] Schmitt M, 'Cyber Operations in international law', 156.
[70] Schmitt M, 'Cyber Operations in international law', 156.
[71] - https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf on Monday, 23 September 2019.
[72] These comprise of four hospitals in its capital Kiev, six power companies, two airports more than twenty-two Ukrainian banks and almost every federal agency.
[73] Osawa J, 'The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem?' *Asia-Pacific Review*, 114 - https://doi.org/10.1080/13439006.2017.1406703 on September 27, 2019.
[74] Carrazana L, 'The economics of cybersecurity and cyberwarfare: A case study,' Economics Colloquium, 5 December 2018, 3. – http://austrianstudentconference.com/wp-content/uploads/2019/02/ASSC-2019-Lorenzo-Carrazana.pdf on Monday, 23 September 2019.

Linko's group is a small family-run software business in Ukraine operating since 1991.[75] The Russian military hackers then hijacked the servers in question granting them access to PC's, in their thousands, that had the specific accounting software installed. Through that back door, they released the NotPetya malware which was designed to spread automatically, rapidly and indiscriminately causing a devastating chain of events.[76]

The costs of the attack are far reaching and quantifiable. To demonstrate this, a sample from the malware's worst hit companies shall be used. Pharmaceutical company Merck reported eight hundred and seventy million USD in damages, delivery company FedEx through its European subsidiary TNT Express reported seven hundred million USD, French construction company Saint-Gobain reported three hundred and eighty-four million USD, Danish shipping company Maersk reported three hundred million USD, snack company Mondelez reported damages amounting to one hundred and eighty eight million USD and British manufacturer Reckitt Benckiser reported damages worth one hundred and twenty nine million USD.[77] In addition, the attack was reported to the local police by 1508 Ukrainian legal entities and individuals to the police. Among these were 178 with official documents comprising of 152 from private organizations and 26 from various government agencies.[78]

Ratification of the Budapest Convention[79] in 2006 by Ukraine[80] and the subsequent adoption of the law in the Ukrainian Criminal Code under Chapter XVI on criminal offences related to the use of computers, systems, computer networks and telecommunication networks rebuts the presumptive legitimacy of the operation. Specific to NotPetya, the criminal code criminalizes the unauthorized interference with the workings of computers, automated systems and computer as well as telecommunication networks.[81] The creation for purposes of usage, dissemination and distribution of harmful software or hardware coupled with their factual dissemination and distribution is similarly criminalized.[82]

---

[75] - https://www.linkos.ua/ on Monday, 23 September 2019.
[76] - https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf on Monday, 23 September 2019.
[77] - https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf on Saturday, 28 September 2019.
[78] - https://www.pravda.com.ua/news/2017/06/29/7148210/ on Saturday, 28 September 2019.
[79] *Budapest Convention on Cybercrime.* 23 November 2001, ETS 185.
[80] Ukraine ratified the Budapest Convention with 11th October, 2005 being the effective date when it entered into force. - https://zakon.rada.gov.ua/rada/anot/ru/2824-15/sp:max100 on Friday, September 27, 2019.
[81] Article 361, *Criminal Code of Ukraine* (2001).
[82] Article 361(1) and (2), *Criminal Code of Ukraine* (2001).

Hardly risking an inconclusive analysis of the NotPetya with respect to the last factor of state responsibility, this paper shall refrain from pre-empting the discussion on responsibility as it shall be conclusively dispensed with in the subsequent chapter.

This analysis leads to the conclusion of the attack's characterisation as falling within what may be considered an illegal use of force. NotPetya need not satisfy all the factors but a combination of these may lead to this conclusion. Factual dissemination of the malware was *de jure* illegal. The severity was of such a degree that it went beyond Ukraine's boarders and the malware's effects manifested within hours with measurable consequences that had an uninterrupted cause and effect relation. It is unnecessary to go into the circumstances surrounding the attack, however, it is prudent to note that to describe the Ukraine-Russia relation as tense will be a thorough understatement.[8384]

2.3. Cyber-operations with the character of an armed attack

"Armed attack" has not been specifically defined by any treaty or any other international agreement. The ICJ, in its advisory opinion on *Nuclear Weapons of 1996*, commented that under Article 51 provisions no specific weapon has been made reference to, incidentally extending its application to any type of armed attack regardless of the weapon used.[85] The distinguishing feature in "armed attack" is in its place under Article 51 of the UN Charter and the customary international law norm of states' right of self-defence.[86]This is because a violation of the prohibition of the use of force would not confer to states the right of self-defence. In the Nicaragua case, the determination by the ICJ acknowledged the distinction between use of force and armed attack by noting that there are actions that involve a use of force but which do not constitute an armed attack.[87] This distinction has it that all armed attacks constitute uses of force while the converse would not hold. The remedies available for uses of force that do not amount to an armed attack are restricted to lawful non-forceful means such as countermeasures or Security Council recourse. Meaning that without

[83] Russia's hybrid aggression on Ukraine that led to annexation of the Crimean Peninsula and occupation the districts of Donetsk and Lugansk regions forms a substantial part of the surrounding circumstances to consider.
[84] Scientific and Research Centre of Military History, 'Means of Russia hybrid warfare against Ukraine,' National Defense University of Ukraine, Kyiv, 2017. - https://nuou.org.ua/assets/documents/scientific-edition.pdf on Thursday, October 3, 2019.
[85] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, 35.
[86] Article 51, *Charter of the UN*.
[87] *Nicaragua v US*, ICJ, 100, para.191.

authorization from the Security Council, a state - having been a victim of an unlawful use of force - may not retaliate with a use of force unless such force rises to a level equivalent to an armed attack.

The place of data in the armed attack framework on cyber-operations has remained relatively obscure. Can destruction or interference with data result to the inference of a degree of aggression on the scale of the use of force and rising to its characterization as an armed attack considering the various forms and purposes of data in question? A brief answer to this could be based on the direct consequences of such destruction or interference. By inference, mere destruction of data would not be considered to be in the scope of an armed attack as it has the flaw of being too broad a threshold. The destruction of data designed to be directly converted to tangible objects, for example banking data, may be viewed as fitting within the boundaries of an armed attack, in this case interference may not result to the effects anticipated as it lacks a permanent character. Interference of data may be seen to rise to this level when it results in physical consequences arising from its effect on the targeted system. Take for instance a malfunction resulting to the explosion of the affected system. This would be a clear instance of an armed attack.[88] This study acknowledges that the specific data aspect of cyber operations may require a detailed exposition. However, it shall take a broad view of cyber operations in the discussions that follow.

There is international consensus favouring a set of criteria proposed by Jean Pictet so as to establish the existence of an international armed conflict under common Article 2 of the 1949 Geneva Conventions[8990] which also act as a guide for assessing if a use of force has been deemed to have risen to the level of an armed attack. Under the test, when a use of force is of sufficient scope, duration and intensity it is deemed to be an armed attack.[91] The UNGA's "Definition of Aggression" resolution has furthered the application of Pictet's criteria - although it does not define the term "armed attack" it gives examples of actions of states that may be deemed to qualify as such - which have gained considerable acceptance internationally, specifically, "the blockade of the ports or coasts of a State by armed forces of

[88] Schmitt M, 'Cyber operations and the jus ad bellum revisited,' 56(3) *Villanova Law Review*, 2011, 589.
[89] Which affirms the applicability of the convention to all cases of declared war or any other armed conflict which may arise between two or more parties to the convention regardless of whether it is recognised by either party.
[90] Article 2, *Geneva Convention Relative to the Treatment of Prisoners of War*, 12 August 1949, 75 UNTS 135.
[91] Sharp G, *Cyberspace and the use of force*, Aegis Research Corporation, 1999, 60.

another State and an attack by armed forces of a State on the land, sea, or air forces or marine and air fleets of another State."[92] More recently, three distinct analytical models have been advanced to further the application of Pictet's use of force criteria to fit into unconventional models such as cyber-attacks. These are; the instrument-based approach, the effects-based approach and the strict liability approach.[93]

2.3.1. Instrument-based approach

This model requires an assessment to be conducted as to whether damage caused by a cyber-attack could previously only have been achieved by way of a kinetic attack.

This author takes cognisance of the fact that traditionally, the instrument-based approach was essentially a qualitative one where prohibitions were activity oriented (such as deployment of military forces and other destructive elements). The actions within the prohibition on use of force rising to the level of an armed attack have, in a way, adapted to modern cyber-warfare because of the long-standing awareness that it extends beyond the application of kinetic force and logically requiring the employment of this criterion so as to identify particular non-kinetic actions that result in quantitatively unacceptable consequences that may evoke the state's right of self-defence.[94]

NotPetya fits into the non-kinetic type of attack and by way of implication a quantitative approach will be employed. Then begs the question, whether it is conceivable that the damage incurred as a result of the malware could only have been achieved by a kinetic attack? Damage caused by the malware was of such a scale that could have only been effected by kinetic means considering that they surpass anticipated damages resulting from economic coercion or any other equivalent means on the spectrum having the temporal consideration in mind.

2.3.2. Effects-based approach

What is in consideration under this model is the overall effect of the cyber-attack on the victim state. This is premised on the fact that the intrinsic character of "armed attacks" is not so much in the modalities used but the direct and conceivably indirect consequences of a

[92] UNGA, Definition of aggression, UN A/Res/3314 (XXIX) 14 December 1974.
[93] Graham D, 'Cyber threats and the law of war,' 4(1) *Journal of National Security Law and Policy*, 2010, 91.
[94] Schmitt M, 'Cyber operations and the jus ad bellum revisited,' 604.

cyber-attack, therefore, legal interpretation should follow with a results-oriented approach to such attacks inquiring as to whether their results have sufficient parallels to kinetic attacks.[95] The dissertation will favour a holistic approach to effects, not restricting effects to violent consequences (such as a power plant exploding or a plane crashing) but employing a broader scope favoured by legal experts that acknowledges society's reliance on connectivity and information infrastructure.[96] Such an approach would consider a cyber-attack as evoking the right to self-defence when it results in a degree human suffering or economic destruction similar to a military attack.[97]

The effects having been already described in detail and with no need for further emphasis, this analysis certainly favours the view that, under this criterion, the consequences of the NotPetya attack severely affected the state of Ukraine in a manner consonant to an armed attack.

2.3.3. Strict liability approach

This model automatically deems cyber-attacks targeted at critical national infrastructure (CNI) to be an armed attack. This is because of the severe consequences that could result from an attack on CNI's.[98]

Different countries have varying definitions of CNI. The United States define critical infrastructure as both systems and assets that are either of a virtual or physical nature which are of such an indispensable character that their incapacity or destruction would have a debilitating impact on, security, national economic security, national public health or safety or a combination of these.[99] Germany delineate the substance of CNI to be those facilities or systems (or parts of these) that belong to the energy, information technology, telecommunications, transport, health, water, food, finance or insurance sectors which are to be conjunctive with their necessity in ensuring proper functioning of society as their failure would result in considerable supply disruptions or that put public safety and security at

[95] Owens W, Dam K, Lin H, 'Technology, policy, law and ethics regarding U.S. acquisition and use of cyberattack capabilities,' National Research Council of the National Academies, 2009, 33-34.
[96] Waxman M, 'Self-defence force against cyber attacks: Legal, strategic and political dimensions,' 89 *International Law Studies*, 2013, 111.
[97] Geers K, 'The challenge of cyber attack deterrence,'26 *Computer Law and Security Review*, 2010, 302.
[98] Sharp G, *Cyberspace and the use of force*, 129-131.
[99] Section 5195c(e), *Critical Infrastructure Protection Act* 42 USC.

risk.[100] The United Kingdom prescribes that those facilities, systems, sites, information, people, processes and networks necessary for the functioning of the state and provision of vital services though which everyday life in the nation depends constitute CNI.[101]

Contrary to prior legislation in Ukraine,[102] not only does the new National Security Strategy for Ukraine list threats to critical infrastructure under their current national security threats but also acknowledges the vulnerability of critical infrastructure objects and public information attacks in its provision for cyber-security and informational assets threats.[103] This is despite the fact that there lacks a definition of critical infrastructure in the applicable legislations.

Assuming, at this level, the perpetrators of the NotPetya attack were state-linked actors then it may be concluded that the strict liability test for destruction or interference of CI would be answered in the affirmative. Noting that multiple government and banking institutions were incapacitated,[104] there are clear and logical parallels with Germany's categorization of vital socioeconomic service infrastructure as well as the United States' comprehensive list of CI's.[105]

2.4. *Jus in bello* considerations of cyber operations

Wartime conduct is governed by IHL meaning that once there is established the existence of an armed conflict any action taken as a result of such a state of affairs must be in compliance with IHL.[106] Although this dissertation recognises the applicability of IHL to non-international armed conflicts,[107] it's scope is limited to addressing armed conflicts of an international nature as is the case in the NotPetya Attack. This conclusion may be drawn by

---

[100] - https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2_7/Kapitel2_7_5/kapitel2_7_5_node_en.html on 3 October 2019.

[101] - https://www.cpni.gov.uk/critical-national-infrastructure-0 on 3 October 2019.

[102] Kondratov S, Dmytro B, Horbulin V, Sukhodolia O, Ivaniuta S, Nasvit O, Biriukov D, Riabtsev G, 'Developing the critical infrastructure protection system in Ukraine,' National Institute for Strategic Studies, 2017, 12. - http://www.niss.gov.ua on 27 September 2019.

[103] Lytvynenko O, Fluri P, Badrack V, 'The security sector legislation of Ukraine,' Geneva, Kyiv, 2017,140.

[104] - https://en.hromadske.ua/posts/unknown-virus-attacks-ukraines-state-banks-and-enterprizes on Saturday, 28 September 2019.

[105] - https://www.dhs.gov/cisa/critical-infrastructure-sectors on 3 October 2019.

[106] Melzer N, *International Humanitarian Law a comprehensive introduction*, International Committee of the Red Cross, Geneva, 2016, 52.

[107] Common Article 3, ICRC *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention)*, 12 August 1949, 75 UNTS 135.

inference from common article 2 which asserts the applicability of the convention to cases of declared war or of any other armed conflict between or among state parties regardless if such a state of war is not recognized by any one of them.[108]

It is however contended that there is yet to be a consensus within the international community on how IHL applies to cyber-warfare.[109] Nonetheless, contentions regarding the non-applicability are thoroughly inconsistent with the objects and purpose of IHL, specifically, the requirement for a mandatory review of new means and methods of warfare.[110] This requirement has been observed to be reflective of the crystallization of customary international law towards this practice.[111]

Due to the dichotomy extant in the international sphere on warfare – *jus in bello* and *jus ad bellum* – essentially two separate bodies of law with varying objects and purposes, the meaning of "attack" will depend on its source. Attacks are defined in Article 49(1) of Additional Protocol I as acts of violence against the adversary whether they may be offensive or defensive.[112] Attack here is similarly a threshold concept in that its restrictions and prohibitions will only apply once particular operations qualify. A commonality in the dichotomy proceeds in such a manner that a legal analysis of an "attack" will lead to approximately the same conclusion albeit with employment of varying parameters.[113] In contrast with *jus ad bellum*, IHL triggers legal protections predominantly deriving from the principle of distinction mandating parties to a conflict to distinguish between; civilian objects and military objects and civilian population and combatants consequently directing their actions to only military objectives.[114]

---

[108] Common Article 2, ICRC *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*, 12 August 1949, 75 UNTS 287.

[109] Kelsey T, 'Hacking into International Humanitarian Law: The principles of distinction and neutrality in the age of cyber warfare,' 106(7) *University of Michigan Law School*, 2008, 1430.

[110] Article 36, ICRC *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, 1125 UNTS 3.

[111] Rule 110, Schmitt M N, 'Tallinn manual 2.0 on the international law applicable to cyber operations: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2017).

[112] Article 49(1), *Protocol* I.

[113] Schmitt M, '"Attack" as a term of art in international law: the cyber operations context', 291.

[114] Article 48, *Protocol I.*

2.5. Conclusion

Although instructive, these approaches to categorize cyber-attacks as either uses of force or rising to the level of an armed attack are not binding.[115] Different states may take different approaches.[116] There is insufficiency of state practice to such an extent that it may be argued that it is directed towards what has been termed as 'the sound of silence'[117]. This same deficiency plagues IHL, where, despite multiple studies having been carried out by ICRC towards determining state practice and *opinio juris* coupled with the fact that the ICRC regularly informed states of this work has fallen to deaf ears not eliciting response from most States.[118] Due to such a state of affairs in the international sphere, decisions on the determination of whether particular cyber-attacks constitute uses of force or are forms of armed attacks are left to a free-for-all arena of states with competing and conflicting interests and different cyber-capabilities.

This chapter has attempted to clear the vagaries that pervade the policy, technical and legal communities on conjecture related to or regarding "attack" in the cyber space with the aim of having a nuanced discussion of what is author considers to be the initial stage in the inquiry logically preceding a discussion on state responsibility and the standard of proof in cyber-attacks – referring to those *jus in bello* considerations. A foundational chapter feeding into the sphere of liability. As a last remark - without pre-empting the discussion to follow – I assert that liability is an issue that cannot be ignored[119], how else could we hope to unmask this villain that is the bad man[120]?

[115] Makory J, Cyberwarfare regulation, 32.
[116] For example, the United States favour the effects-based approach to determine whether a use of force would give rise to their right of self-defense. (insert the footnote for this).
[117] Fidler D, 'Was Stuxnet an act of war? Decoding a cyberattack,' *IEEE Security & Privacy*, Indiana University, 2011, 57.
[118] Schmitt M and Watts S, 'The decline of International Humanitarian Law opinio juris and the law of cyber warfare,' 50(2) *Texas International Law Journal*, 2015, 196-197.
[119] Makory J, Cyberwarfare regulation, 43.
[120] Holms O, "The path of the law," *Harvard Law Review*, 457, 3 (1897).

CHAPTER 3

State responsibility and aspects of burden and standards of proof in cyber-attacks

3.1. Introduction

A state, so interfered with, may only exercise their inherent right to self-defense when the level of attack against the state in question rose to the level of an armed attack. Save for the threshold considerations of the exercise of self-defense, a state should consider the complicity of the state from whence the attack originated. It is also important to note that if the act of self-defense is not an immediate response the imputation of responsibility is necessitated before an aggrieved state may act in retaliation.[121]

International jurisprudence on state responsibility is articulated in the International Law Commission's 2001 publication of the Articles on the Responsibility of States for Internationally Wrongful Acts (ARISWA). It provides that each State is responsible for every internationally wrongful act of that State.[122] State responsibility is well settled in state practice and *opinio juris*. The preceding statement is qualified by the ICJ ruling in the *Corfu Channel case* where it found, in making a determination on the threshold of attribution of responsibility (within the borders of the state in question), that territorial sovereignty is invariably linked to a State's obligation in CIL to not allow its territory to be used for acts inconsistent with the rights of other States knowingly, among other obligations[123] based on the fact in question of the presence of mines in Albania's territorial waters.[124] The Tallin Manual[125] also recognizes state responsibility as an essential principle of international law

[121] Gervais M, 'Cyber attacks and the law of war', 544.
[122] Article 1, *Draft articles on state responsibility for internationally wrongful acts*, ILC 53rd Report, 2001, UN Doc A/56/10.
[123] The ICJ pointed out Albania's obligation in notifying, for the benefit of shipping in general, the presence of mines in their territorial waters is based on general and well-recognized principles consisting of; elementary principles of humanity and principle of freedom of maritime communication.
[124] *The Corfu Channel Case*, ICJ, 22.
[125] Rule 6, Schmitt M N, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2013).

that states should bear responsibility for acts or omissions that are; attributable to the State and constitute a breach of a legal obligation applicable to the State in question.[126]

Standards of proof are distinct from the inquiry into state responsibility. The latter is concerned with the determination of the level of connection that must, of necessity, exist between conduct of an individual or group of individuals and a State for such conduct to attract liability to the State, the former focuses on the determination of the quantum of evidence necessary to prove the claims of fact made by the parties.[127] The standard of proof is also distinct from the burden of proof. The burden of proof is the obligation on a party to show that they have sufficient evidence on an issue to raise it in a case and this includes the "burden of persuasion" as well as the "burden of production"[128].[129] A discussion on the evidentiary issues relevant to cyber operations will, in a general sense, cement facts that will necessarily be in issue when attributing liability to a particular State.

Considering the basis for state responsibility this dissertation now considers the aspect of liability in two-fold; State liability vis a vis State organs and State liability vis a vis non-State actors - in the context of cyber-operations they comprise of predominantly hacktivists[130].[131] The necessity of this differentiation cannot be overemphasized, more so in cyber-space where a State may be merely responsible by omission or as a result of having coerced complicity of another State in furtherance of an act or omission or the possibility where a State may choose to involve private contractors to carry out the acts in question in the former instance and where a hacktivist(s) perpetrates the acts in question and the State may be wholly, incidentally or not at all associated with the individual or group of hacktivists as the case may be.

---

[126] Rule 6.2, Schmitt M N, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2013).

[127] Green J, 'Fluctuating evidentiary standards for self-defence in the International Court of Justice' 58(1) *the International and Comparative Law Quarterly*, 2009, 165.

[128] Burden of production is the burden to produce the relevant evidence before a court.

[129] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations' 50(2) *Texas International Law Journal*, 2015, 241.

[130] Hacktivists being private citizens who are motivated by ideology in most part and who possess the requisite skills to perpetrate a cyber-attack.

[131] Makory J, 'Cyberwarfare regulation', 38.

3.2. State responsibility

3.2.1. State actors

To reiterate, Article 1 of ARISWA imputes responsibility on a State where it is the perpetrator of the internationally wrongful act. This is the general position regarding State responsibility. It is explicit on the fact that a State is to be deemed responsible for its breaches of international law.

Conduct of State organs are considered to be the conduct of that State regardless of their functions or the position they hold in the State's organization notwithstanding their character.[132] These organs consist of any person or entity bearing such a status as per the internal laws of the State.[133] The preceding ARISWA provisions are indicative of the crystallization of CIL regarding the assumption that a state is responsible for the conduct of its agents even if they act *ulta-vires.*[134] The ICJ decision in *Armed Activities on the Territory of the Congo* found the Republic of Uganda in breach of its obligations under international law for acts carried out by its armed forces in the territory of the Democratic Republic of the Congo (DRC) as well as its failure to comply with its obligations as an occupying power owed to DRC to prevent the acts that were in question.[135] Explicitly acknowledging that by virtue of an established rule of CIL (that the conduct of any State organ is deemed as being an act of that State) the conduct of the armed forces – both of individual soldiers and officers - under the control of Uganda (in this instance it was the Uganda People's Defense Force) are attributable to Uganda.[136] This similarly applies to persons or entities that are not state organs but are empowered under the law of that State to exercise governmental authority, or elements of it, with the rider that this person or entity should be acting in that capacity in the instance in question.[137] By implication this means that state responsibility may be attributed to that State regarding acts carried out by public or private entities exercising governmental authority having been so empowered.

---

[132] Article 4(1), ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[133] Article 4(2), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[134] Gervais M, 'Cyber attacks and the law of war', 545.
[135] *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda),* ICJ Reports 2005, 116.
[136] *Armed Activities on the Territory of the Congo,* ICJ, 213.
[137] Article 6, ILC, *Draft articles on state responsibility for internationally wrongful acts.*

A State is internationally responsible for wrongful acts which another State commits under their direction and control if; the former acts in such a manner having knowledge of the internationally wrongful act and the act in question would be internationally wrongful if it was the party which had carried out such acts.[138] This may be considered reflective of the ruling in the *Corfu Channel case* that emphasized on a State's obligation to not knowingly allow its territory to be used for acts that are inconsistent with obligations owed to other States.

3.2.2. Non-State actors

Article 51 on the United Nations Charter does not speak to the fact as to whether the State's inherent right of self-defense applies in response to attacks by non-State actors. Different standards of attributing state responsibility are applicable as the subsequent discussion on various ICJ decisions will show. Also key in this discussion will be the presumed implication of the 9/11 terrorist attacks as it has been argued in scholarly circles that there has been a notable shift in the doctrine of State responsibility as a result.[139]

As alluded to, the lack of express provisions on the validity of attributing State liability due to the actions of non-State actors leaves a legal loophole that may be exploited by hacktivists.[140] Moreover, the approach taken must be with due regard to international relations as it exists. For example, foreseeable questions of State sovereignty that will arise if it were the case that a State responds to actions of individuals operating in a third party State without direction from that State. This is just one among the plethora of possibilities made so by latent cyber-capabilities.

Custom and practice show that States have responded with force to non-State actors. This is buttressed by the international community's response to the 9/11 attacks on the territory of the United States where the United Nations Security Council (UNSC) reaffirmed the United States' right of inherent self-defense as per Article 51 of the UN Charter through its

[138] Article 17, ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[139] Cenic S, 'State responsibility and self-defence in international law post 9/11: Has the scope of article 51 of the United Nations Charter been widened as a result of the US response to 9/11?' 14 *Australian International Law Journal*, 2007, 202.
[140] Makory J, 'Cyberwarfare regulation', 38.

unanimous passing of Resolution 1368.[141] When the material fact that it was indeed non-State actors that perpetrated the attacks in question became certain, the United States received nearly universal support in invoking its right to self-defense not to mention a unanimous UNSC vote in its favour through Resolution 1373.[142]

With basis in the *Corfu Channel* decision - where the CIL obligation of a State to prevent its territory from being used to perpetrate acts that cause harm to other States was explicated – this formulation analogously applies to non-State actors such that a State may not knowingly allow these actors, within its borders, to cause harm to another State. The Tallin Manual extends this formulation to the cyber-space by providing that a State is not to allow cyber-infrastructure within its territory or within its exclusive governmental control to be used for acts that are unlawful and with an adverse effect on another State.[143]

By implication, liability may attach itself to a State under whose direction and control these non-State actors operate under in perpetration of an attack on another State.[144] The preceding ARISWA provision is consistent with the effective control formulation articulated in the *Nicaragua case*.[145] It was decided that the United States' participation in financing, organizing, training, supplying and equipping the contras together with selection of its targets and planning of the entirety of its operation was insufficient for attributing State responsibility to the US for acts carried out by the contras in the course of their operations in Nicaragua as they could as well do so by their own agency. A general control of a force with a high dependency was considered insufficient absent evidence of direction or enforcement of the acts in question. For legal responsibility to attach to the United States, proof of effective control of the contras in the course of the acts in question would need to be demonstrated.[146] This extraterritorial nature of State liability demonstrates that a State may be found liable for those specific acts of non-State agents in cyber-space which are

[141] UNSC S/RES/1368 (2001) Threats to international peace and security caused by terrorist acts.
[142] UNSC S/RES/1373 (2001) On threats to international peace and security caused by terrorist acts.
[143] Rule 5, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2013).
[144] Article 8, ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[145] *Nicaragua v US*, ICJ, 100, para.115.
[146] *Nicaragua v US*, ICJ, 100, para.116.

inconsistent with the rights of the victim State provided that the specific acts are carried out under its direction or enforcement implying effective control.

A distinction is drawn by the International Tribunal for the Former Yugoslavia in the *Tadic case*[147], on the standard of overall control needed to impute State responsibility from actions of non-State actors between participants in an organized group that is hierarchically structured and individuals and unorganized groups. What is referred to as the *Tadic* standard favours a lower threshold when the non-State actors in question fall within the former category as the tribunal, in consideration of this distinction, noted was due to the fact that an organized group such as a military or paramilitary unit have an inherent structure, chain of command, set of rules and outward symbols of authority. This implies that individual members in this form of grouping do not act on their own but rather conform to the standards that prevail and are subject to the successive hierarchical chain of command up to the head of the group. Thus, the tribunal found for attribution to a State for acts of such a group it is deemed sufficient to require the group as a whole to be under the overall control of the State.[148] With individuals and unorganized groups, the *Tadic* tribunal finding was consistent with the higher effective control standard as expressed in the *Nicaragua case* save from an added factor where, in the absence of direction, public approval on the part of a State regarding those acts following their commission would impute liability on its part.[149]

ARISWA provides at Article 11 that retrospective adoption of these non-State agents' conduct by a State would render those acts in question to be considered as act of that State.[150] Retroactive adoption is demonstrated in practice by the ICJ's judgement in the *United States Diplomatic and Consular Staff in Tehran* where it found Iran in breach of various treaty obligations[151] and in violation of applicable rules general international law by endorsing and

[147] *Prosecutor v Tadic (Sentencing Judgment),* Case No. IT-94-1-T, ICTY, 14 July 2007.
[148] *Prosecutor v. Tadic*, 120
[149] *Prosecutor v. Tadic*, 132.
[150] Article 11, ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[151] In particular, the treaty obligations imposed on Iran by the Vienna Conventions on Diplomatic and Consular Relations of 1961 and 1963, Treaty of Amity, Economic Relations, and Consular Rights of 1955. The ICJ also emphasized the inviolability of diplomatic envoys and their embassies by stating, "There is no more fundamental prerequisite for the conduct of relations between States…."

maintaining seizure of the US embassy and its personnel in Iran by Iranian students (who were not categorized as an organized armed group).[152]

Even without the aspect of endorsement, international law does require that States adopt reasonable preventive measures against the operations of independent hackers. This can be seen through treaty requirements of State signatories to criminalize cyber-attacks in their domestic laws.[153] However the extent of the duty to prevent is obscure, more so considering the phenomenon of lone-wolf hacktivists.[154] When a State has knowledge of a cyber-attack it must discharge its duty of prevention (through stopping and prosecuting the attackers) as non-cooperation on its part may result to the injured State invoking its inherent right of self-defence. As has previously been discussed, knowingly allowing perpetration of internationally wrongful acts on another State by non-State actors (either by act or omission) will lead to attribution of liability on that state - sufficient measures not having been taken.[155]

An argument can be made that pre-9/11 the effective control standard would have applied as formulated. The post 9/11 shift[156] brings into question the additional aspect of harboring perpetrators of internationally wrongful acts as was explicitly stated by the UNSC in Resolution 1386. Support by the international community for the US action against Al-Qaeda is demonstrative of this change coupled with the unanimous adoption of Resolution 1386 and 1373 by the UNSC. This is the current position regarding State responsibility in so far as can be deduced from State practice. However, scholars who dispute this shift assert that the passing of the aforementioned resolutions by the UNSC was merely an exceptional response to the unprecedented circumstances.[157] The converse of this being that harboring of the perpetrators of the 9/11 attacks was seen to be analogous to endorsing of their actions by way of implication due to the fact that the State had knowledge of the violation of its obligation to prevent attacks from within its territory.[158]

---

[152] *The case of the United States Diplomatic and Consular Staff in Tehran (US v Iran)*, ICJ Reports 1980, 91.
[153] Article 23, Council of Europe, *Convention on Cybercrime*, 23 November 2001.
[154] Gervais M, 'Cyber attacks and the law of war', 2011, 548.
[155] Gervais M, 'Cyber attacks and the law of war', 549.
[156] Cenic S, 'State responsibility and self-defence in international law post 9/11: Has the scope of article 51 of the United Nations Charter been widened as a result of the US response to 9/11?' 201.
[157] Gervais M, 'Cyber attacks and the law of war', 549
[158] Gervais M, 'Cyber attacks and the law of war', 549.

3.3. Burden and standards of proof

3.3.1. Burden of proof

The burden of proof identifies the litigant on which the onus lies to meet the standard of proof through adducing the necessary evidence. Once a litigant's burden has been discharged in line with the required standard, the burden shifts to the other litigant to prove the contrary.[159] Normally, the general principle *onus probandi incumbit actori* is applicable, it directs the onus of proof of a certain fact to lie on the person who is relying on it. This principle is invoked in a consistent manner by the ICJ as well as other international courts and tribunals.[160] It applies to assertions of facts by both the applicant and respondent meaning that the onus is not necessarily placed on the applicant but rather on the party who raised an issue notwithstanding the procedural position.[161] It should be noted that in inter-state litigation, the distinction between applicant and respondent may not always be clear, particularly when a case is brought before an international court by way of special agreement between the parties.[162]

The principle of *onus probandi incumbit actori* is subject to three main limitations. Firstly, undisputed facts or those that are agreed upon by the parties do not require proof.[163] Secondly, the court may relieve a party from the burden of adducing evidence as to facts that are either notorious or of public knowledge. The ICJ in the *Nicaragua* judgement treated the holding manoeuvers, when Nicaragua was relying on that fact and as proof offered newspaper reports, as public knowledge thus sufficiently established.[164] Marco Rocini, author of the article *'Evidentiary Issues in International Disputes Related to State Responsibility For Cyber Operations,'* noted that the notion of what is considered as public knowledge has been expanded owing to the wide availability of information of current events

[159] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations,' 243.
[160] Teitelbaum R, 'Recent fact-finding developments at the International Court of Justice,' 6(1) *The Law and Practice of International Courts and Tribunals*, 2007, 121.
[161] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations,' 243.
[162] Ridddell A and Plant B, 'Evidence before the international court of justice', 2009, 89.
[163] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 245.
[164] *Nicaragua v US*, ICJ, 100, para.92.

both in the press and the internet with companies like; McAfee, Symantec, Mandiant and Project Grey Goose, as well as think tanks like NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) publishing reports of cyber-incidents detailing an analysis of such incidences including those that received extensive coverage by the press. Related to this is the ICJ holding in *Nicaragua* which noted instances that there may be widespread reports of certain facts deriving from a single source, regardless of the number of such reports, the successive reports will have no greater evidentiary value than the original source.[165] On the massive body of information available to the ICJ, it held that such may only be useful to the extent that it is wholly consistent and concordant as to the main facts and circumstances of the case.[166] Thirdly, the principle of *onus probandi incumbit actori* only applies to facts as opposed to law which need not be proven. However, a party relying on the existence of municipal law has the onus of proving that fact in inter-state litigation.[167] In the *Asylum case*, treaty law was distinguished from CIL where in the latter, existence of customary rules must be proven as its element of state practice is a factual issue.[168] This directly applies to cyber-specific customs in which a party relying on the existence of such a custom will have the onus of producing relevant evidence before the court with jurisdiction.

Earlier on in the Chapter it was established that mere knowledge on the part of a state would not automatically entail attribution. This finding was consistent with the attribution requirements according to the *Corfu Channel* formulation of exclusive control. Contrary to arguments by some scholars who propose shifting the burden of proof from the investigator and accuser to the nation whose cyber-infrastructure was used (where the attack software was launched) this paper asserts that the purported reversal of the onus is at variance with the ICJ's *jurisprudence constante*.[169] This position is further buttressed in *Armed Activities in the Congo* as the ICJ did not shift the burden of proving Zaire had been in a position to stop the armed group's actions originating from its border regions as was Uganda's claim, from Uganda to the DRC. Therefore, in cyber-space it is still upon the claimant to demonstrate

[165] *Nicaragua v US*, ICJ, 100, para. 63.
[166] *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran),* ICJ Reports 1980, para. 13.
[167] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 245.
[168] *Asylum Case (Colombia v. Perú),* Judgment, ICJ Reports 1950, 276.
[169] *The Corfu Channel Case,* ICJ, 18.

responsibility on the part of the territorial State or that the State was in breach of its duty of vigilance.[170]

Closely related is the question of the availability of evidence. Does the onus shift when the relevant evidence is in the hands of the other party? In the *Avena case* the ICJ determined that in as much as the information in question might have been, in part, in the hands of Mexico, it was incumbent on the United States to seek out such pertinent information from the Mexican authorities and to demonstrate this was done and the authorities declined or failed to respond to the specific requests. It was then concluded that the United States had not met its burden of proof.[171]

In the context of cyber-operations conducted in an armed conflict, the normal application of the burden of proof is not affected. The ICJ in *Nicaragua* highlighted that it is not only in situations of armed conflicts that evidence is difficult to come by - pursuant to which the court has made allowances for – therefore, even in such a circumstances, it is on the party seeking to establish a fact that the onus of proof lies upon.[172] A presumption of evidence not yet adduced as well as a presumption that such unavailable evidence would have supported a particular party's claim (if had been adduced) was rejected by the ICJ be it as it may that the difficulty in producing the evidence was as a result of interference with governmental action caused by acts of violence.[173] The fact of a covert operation and the possibility of asymmetry in discharging the burden of proof by litigants does not similarly affect application of the principle *onus probandi incumbit actori.*[174]

3.3.2. Standards of proof

From the onset, it is prudent to distinguish between standards of proof in civil law systems and in common law systems. In the former there are no specific standards of proof that

[170] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations,' 246.
[171] *Case Concerning Avena and Other Mexican Nationals (Mexico v. United States of America),* Judgement, ICJ Reports 2004, para. 57.
[172] *Nicaragua v US,* ICJ, 100, para. 101.
[173] *Oil Platforms (Iran v. U.S.),* Judgment, ICJ Reports 2003, para. 46.
[174] *The Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua Intervening) (El Salvador v. Honduras),* ICJ Reports 1992, para. 63.

judges have to apply while the latter utilizes a rigid classification of standards.[175] These standards classified in order from the least stringent to the most stringent are; prima facie evidence, preponderance of evidence or balance of probabilities, clear and convincing evidence and beyond reasonable doubt.[176] The Statute of the ICJ and the Rules of the Court neither require specific standards of proof nor do they indicate what methods of proof the court will consider as being probative so as to meet a specified standard.[177][178] The ICJ has avoided clearly indicating the standards of proof expected form litigants during proceedings, normally referring to the applicable standard in its judgements (post-pleadings).[179]

H.E. Judge Rosalyn Higgins, then president of the ICJ, noted in her speech that there is no agreement on what standard of proof the ICJ should expect form the parties appearing before it.[180] The standard of proof in international criminal courts, due to their inherent nature, is beyond reasonable doubt in contrast to the more appropriate standard for inter-state litigation which is analogous to certain types of civil litigation.[181] This is applied with certain variations. For instance, in establishing international responsibility on a State, Judge Krylov in his dissenting opinion in the *Corfu Channel* case proffered a standard of clear and indisputable facts.[182] While it has been argued that the jurisdiction of an international court over a dispute should be established beyond reasonable doubt, the ICJ has applied a standard more akin to the preponderance of evidence in disputes that involve State responsibility.[183] Others have maintained that this standard only applies to cases not involving responsibility for internationally wrongful acts.[184] Evident in these varying positions regarding a predominant standard of proof is the difficulty or avoidance of identifying a uniform standard of proof that may be applicable in inter-state litigation, however, the Court has developed the practice of looking at issues as they arise and this does not logically preclude the possibility

[175] Milanovic M, 'State responsibility for genocide', 17(3) *European Journal of International Law*, 2006, 594.
[176] Green J, 'Fluctuating evidentiary standards for self-defence in the International Court of Justice', 248.
[177] *Statute of the International Court of Justice*, 26 June 1945, 33 UNTS 933.
[178] *Rules of Court*, ICJ 1978.
[179] Teitelbaum R, 'Recent fact-finding developments at the International Court of Justice', 124.
[180] H.E. Judge Rosalyn Higgins, President of the International Court of Justice, Speech to the Sixth Committee of the General Assembly 4 (November 2, 2007).
[181] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 249.
[182] *The Corfu Channel Case*, ICJ, 72.
[183] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 249.
[184] Ridddell A and Plant B, 'Evidence before the international court of justice', 133.

of establishing a similar evidentiary standard for similar allegations.[185] Based on the forgoing premise, the consequent discussion on evidentiary standards for claims whose locus consist of *jus ad bellum* violations is justified.

Decisions of international courts point to the fact that the standard of clear and convincing evidence is expected for claims on issues involving the violation of the prohibition of the use of force. The ICJ in its *Nicaragua* judgement referred to "convincing evidence" of the facts forming the basis of the claim and to a lack of "clear evidence" of the degree of control exercised over the contras by the US government.[186] Evidence pointing to responsibility on the part of Iran for mine laying was rejected by the ICJ owing to the fact it was "highly suggestive but not conclusive" going on to hold that evidence that establishes Iran's responsibility for the attack was insufficient in the *Oil Platforms* case.[187] A standard that facts "convincingly established by the evidence" was referred to by the ICJ in *DRC v Uganda* as well as "evidence weighty and convincing."[188] Save from the ICJ, the Eritrea-Ethiopia Claims Commission found for the fact of "clear evidence" that the events in Badme were minor incursions not rising to the level of an armed attack.[189]

In contrast to this position other authoritative reports[190] and claims by States[191] point to a lower evidentiary threshold for cyber-operations basing their arguments on the fact that identification and attribution pose a challenge in the digital environment in contrast to the analog world where capabilities could be judged with a high degree of accuracy.[192] These claims are aptly countered by the fact that the standard of proof is so, not with the intention of placing the claimant at a disadvantage but to shield the respondent against false attribution which is an increasingly serious risk in cyber-space.[193] Several reports show that the views

[185] Green J, 'Fluctuating evidentiary standards for self-defence in the International Court of Justice', 169.
[186] *Nicaragua v US*, ICJ, 100, paras. 24, 29, 62, 109.
[187] *Oil Platforms*, ICJ, 161, paras. 71 and 61.
[188] *Armed Activities on the Territory of the Congo*, ICJ, paras. 72, 91 and 136.
[189] *Eritrea-Ethiopia Claims Commission - Partial Award: Jus Ad Bellum - Ethiopia's Claims 1-8*, Reports of International Arbitral Awards, 2005, para. 12.
[190] Project Grey Goose, Russia/Georgia cyber war – findings and analysis (phase 1 report) 2008. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.- on 13 November 2019.
[191] Advance questions for Lieutenant Keith Alexander, USA nominee for commander, United States Cyber Command. - https://epic.org/privacy/nsa/Alexander_04-15-10.pdf- on 13 November 2019.
[192] Graham D, 'Cyber threats and the law of war,' 87.
[193] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 251.

are inconsistent within and among governments all which lean towards the necessity of reliable attribution with sufficient certainty as to the identity of the author of an attack.[194]

It is undesirable to propose a divergent standard for cyber-operations from that of clear and convincing evidence applicable to violations of the prohibition of the use of force with regard to conventional armed attacks.[195] Considering that an appropriate standard should neither be so low such as a *prima facie* or preponderance of evidence (increasing the possibility of false attribution) nor too stringent as to render the proof unduly exacting as underscored by Judge Lauterpacht in the *Norwegian Loans* case.[196] It is also important to emphasize the position taken by Judge Higgins in her separate opinion in the *Oil Platforms* judgement where she noted that the graver the charge the more confidence there must be in the evidence proffered.[197] A similar position was taken by the ICJ in the *Bosnian Genocide* case which confirmed that claims against a State that involve charges considered to be of exceptional gravity must be proved by evidence that is fully conclusive, also applicable to proof of attribution for the acts in question.[198]

Logically, gravity is inherent in any violation of a peremptory norm of *jus cogens*.[199] A distinction may be made between a violation of the prohibition of acts of genocide for which fully conclusive evidence is necessitated and a violation to prevent acts of genocide which requires proof at a high level of certainty applicable to the seriousness of the issue forming the claim following from the *Bosnian Genocide* judgement.[200] It then proceeds that this differentiated standard of proof is applicable for cyber-operations such that the standard for those operations that constitute international crimes will be higher as compared to the standard required to prove violation of a due diligence obligation to prevent its cyber-

[194] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 251.
[195] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 252.
[196] *Certain Norwegian Loans (France v. Norway)*, Judgment, ICJ Reports 1957, 39.
[197] *Oil Platforms*, ICJ, 161, para. 33.
[198] *Case Concerning Application of the Convention on The Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgement, ICJ Reports 2007, para. 209.
[199] Knuchel S, 'State immunity and the promise of *jus cogens*,' 9(2) *Northwestern Journal of International Human Rights*, 2011, 172.
[200] *Case Concerning Application of the Convention on The Prevention and Punishment of the Crime of Genocide*, ICJ, para. 209.

infrastructure from being used by other actors – be they State or non-State – to commit international crimes.[201]

3.4. A NotPetya analysis of responsibility, burden of proof and the applicable standard of proof.

Inherent in the character of cyber-operations is the problem it poses to the attribution doctrine - as had been previously identified. Its importance forms the substance of the previous discussion. The reason for this lies in the manipulation of internet protocol (IP) addresses - which are assigned to devices that are connected to the internet – through anonymizing techniques and anonymizing software with Botnets being an example of the former and software such as Virtual Private Networks (VPN's) and the Onion Router (Tor) as examples of the latter which have made it that much more improbable for authors of particular cyber-operations to be identified.[202] Moreover, IP addresses only serve to identify the device's geographical location as opposed to revealing the specific identity of a device to other users.[203] These anonymizing techniques and software negatively affect technical attribution in a significant way as they serve to reroute malicious cyber-operations through cyber-infrastructure of other states, through this process they are assigned different IP addresses which indicate to the victim that the operation was initiated by a computer in a geographical location that differs from the originating source. Although recent technological developments have enabled accurate cyber-tracing, it remains an extreme difficulty.[204] This may very well be the main reason as to why there is no case law relating to claims arising from inter-state cyber-operations.[205]

On the author of the NotPetya attack, experts from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have maintained that it was probably launched by a state

[201] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations', 254.
[202] Buchan R, 'Cyberspace, non-state actors and the obligation to prevent transboundary harm' 21(3) *Journal of Conflict and Security Law,* 2016, 3.
[203] Buchan R, 'Cyberspace, non-state actors and the obligation to prevent transboundary harm,' 3.
[204] Buchan R, 'Cyberspace, non-state actors and the obligation to prevent transboundary harm,' 3.
[205] Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations,' 250.

actor or a non-state actor with endorsement or support from a state.[206] Although the facts are far less than definitively established officials from various governments have pointed a finger at Russia.[207] Foreign Office Minister for Cyber Security Lord Ahmad of Wimbledon on behalf of the government of the United Kingdom judged that the Russian Government, specifically the Russian Military[208], to be responsible for the attack.[209] The US Government - through the then White House press secretary Sarah Sanders – stated that the NotPetya cyber-attack was launched by the Russian Military as part of the Kremlin's efforts to destabilize Ukraine.[210] Russia's military is an organ of the State. Therefore, following the judgement in *DRC v Uganda*, acts carried out by the Russian military would be considered as acts of the state of Russia.

The Sandworm is a hacking team based out of Russia[211] that has been reported to be under the Russia military intelligence service known as the *Glavnoye Razvedovatel'noye Upravlenie* (GRU).[212] It is prudent to note that the GRU has been seen to be one of the engines for advancing cyber-operations on behalf of the Russian government.[213] Going by the official reports on the NotPetya attack by the US and UK governments, it may be inferred that the Sandworm team that authored this attacks is not merely linked to the Russian military but a team within the military under the GRU. Therefore, for purposes of this analysis, Sandworm will be assumed to be part of Russia's military, essentially state actors.

It has been established that the GRU is a branch of Russia's military that deals with intelligence and this fact per se leads to the conclusion that it is a state organ. The Sandworm team is part of the GRU therefore, acts carried out by the group can be considered to be on its behalf. Article 4 of ARISWA speaks to conduct of state organs. It provides that conduct of

---

[206] -https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/- on Sunday, 17 November 2019.

[207] -https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/- on 17 November 2019.

[208] The United Kingdom's National Cyber Defence Centre advanced that the Russian Military was "almost certainly responsible for the NotPetya attack. - https://www.ncsc.gov.uk/- on 17 November 2019.

[209] -https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks- on 17 November 2019.

[210] -https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/- on 17 November 2019.

[211] - https://www.trackingterrorism.org/group/sandworm – on 21 November 2019.

[212] - https://www.reuters.com/article/russia-cyber/hackers-accused-of-ties-to-russia-hit-3-e-european-companies-cybersecurity-firm-idUSL8N1WP37F - on 21 November 2019.

[213] -https://www.globalsecurity.org/intell/world/russia/gru-ops.htm – on 21 November 2019.

organs of a state is considered to be an act of that state according to international law. Following the judgment of the ICJ in *Armed Activities on the Territory of the Congo* Russia would be considered responsible for the NotPetya attack in Ukraine by analogy as acts of the GRU (more specifically Sandworm) under whose control they operate under will be considered to be Russia's conduct. The *Corfu Channel* formulation would have it that Russia, who exercise sovereignty over their territory have an obligation to not knowingly allow its territory to be used for acts that contravene the rights of other states which extends to its cyber-infrastructure as per Rule 5 of the Tallin Manual.

Onus probandi incumbit actori as a guiding principle of the burden of proof would necessarily apply in the context of the NotPetya cyber-attack evidenced by its consistent application by international courts and tribunals. If a claim were to be raised against Russia for the attack against Ukraine the burden of proof would not be so rigid as to focus on the parties' respective positions but would rather be placed on a party raising as issue. This burden is not affected by the information asymmetry that may exist between the parties again supported by the ICJ's *jurisprudence constante* and in particular the judgment in *Armed Activities in the Congo*, as Russia's GRU has the character of being the key intelligence apparatus for the Russian government and as such is synonymous to covert operations whose information is unavailable to the general public. The *Avena case* does relieve some of the pressure to discharge its burden by requesting for such pertinent information from the other party's government.

Having in mind the lack of a uniform standard of proof in inter-sate litigation, this dissertation assumes that as international courts dispose of issues in a case by case basis this does not preclude the establishment of similar standards applying to similar allegations. In the case of the NotPetya attack - which involves *jus ad bellum* violations – a discernable standard(s) can be identified. Various international courts have settled on such issues to be established by the standard of clear and convincing evidence such as the *Eritrea-Ethiopia Claims Commission*, ICJ judgements in *DRC v Uganda*, *Nicaragua* and the *Oil Platforms* case. Therefore, the standard of clear and convincing evidence would be applicable if the primary issue was concerned with the violation of the prohibition of the use of force. In contrast to this standard is the lower standard advanced in the *Bosnian Genocide* judgement –

this standard being not as low as a *prima facie* or preponderance of evidence – if what was at issue was the violation of Russia's obligation in CIL to prevent its cyber-infrastructure from being used by other state or non-state actors to cause harm in the territory of another state.[214]

3.5. Conclusion

Despite the fact that the case study would apply only certain aspects that this dissertation has explicated its aim was to give a holistic view of the factors that feed into attribution. In the cyberspace, it has been established that acts in contravention of the prohibition of use of force by a state or its state organs may lead to the offended state exercising its inherent right of self-defense. This is also the position regarding acts of non-state actors following from state practice and the passing of UNSC Resolutions 1368 and 1373. In respect of the burden of proof in inter-state litigation the principle *onus probandi incumbit actori* is instructive. The burden of proof does not shift from the claimant to demonstrate responsibility on the territorial state or a breach of that state's duty to vigilance cemented by the ICJ in *Armed Activities in the Congo.* International courts have demonstrated an avoidance of identifying a uniform standard of proof in inter-state litigation however, a similar standard may apply to similar allegations. Invariably, depending on the gravity of the claims in question different standards may apply such that the violations of *jus cogens* norms requiring relatively higher standards of proof.[215]

Liability is not only fundamental towards proving or disproving the dominant hypothesis but is also an issue that cannot be ignored considering the trends prevalent in contemporary warfare favoring cyber-operations due to the inherent difficulty in attribution. Some scholars going as far as suggesting that this reason necessitates a shift of the burden of proof. State practice towards attribution in cyber-operations has been limited to public accusations.[216]

However, latest trends have seen a positive step by states to address this problem. In a joint report from the US National Security Agency (NSA) and Britain's NCSC it has been stated

---

[214] Shackelford S, Russel S and Kuehn A, 'Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors,' *Chicago Journal of International Law*, 2016, 10.
[215] *Case Concerning Application of the Convention on The Prevention and Punishment of the Crime of Genocide*, ICJ, para. 209.
[216] - https://www.bbc.com/news/uk-politics-43062113 - on 17 November 2019.

that Russian hackers referred to as the Turla group compromised Iranian tools and infrastructure to carry out cyber-operations for the purpose of intelligence collection, aimed at governmental departments, military establishments, scientific organizations and universities in at least 35 countries.[217] This has been part of an ongoing investigation by the NCSC looking into two specific tools (known as Neuron and Nautilus) used by the group to target the United Kingdom.[218] However, even as the UK is seen to be ready to react to such attacks the cyber-grounds are still favourable for battle. Although it has been stated that the recent Distributed Denial of Service (DDoS) against the UK's Labour Party was not linked to a state, a source from within the party said that the attacks originated from computers in Russia and Brazil.[219] It then begs the question, how long will the status quo among states endure? It is only a matter of time.

Finally, it should be noted that, especially for purposes the case study, certain assumptions were made and expressly stated to be so. A contributing factor to such assumptions is insufficiency of information available to the public inherent in the disquisition of cyber-attacks. Additionally, the analysis of the NotPetya attack remains theoretical although logical inferences have been made regarding Russia's involvement. Notwithstanding, the subsequent topic will deal with the consequences once attribution requirements have been dispensed with. From this point onwards the discussions will form the metaphorical demise of the bad man.

[217] - https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims - on 17 November 2019.
[218] - https://www.ncsc.gov.uk/news/turla-group-malware - on 17 November 2019.
[219] - https://www.bbc.com/news/election-2019-50388879 - on 17 November 2019.

CHAPTER 4

Consequences in the event that responsibility attaches itself on a state in a cyber-attack

4.1. Introduction

Proceeding from the discussion on liability are the corresponding measures available to states for conduct falling either under uses of force or armed attacks. For the purpose of emphasis, the two are similar in so far as all armed attacks constitute uses of force but the converse does not hold. Cyber-operations constituting uses of force meet the Schmitt criterion that consists of an analysis of the factors of; severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.[220] On the other hand Pictet's criteria[221] of analysing whether uses of force rise to the level of an armed attack has been placed in the cyber-context through the use of the following analytical models; the instrument-based approach, the effects-based approach and the strict liability approach.[222]

Cyber-operations rising to the level of an armed attack implicates that the injured state may employ its right of self-defence under Article 51 of the UN Charter using forcible means.[223] As cyber-operations are in vogue in that there are increasingly prevalent, it necessitates availability of a quick and effective recourse to states due to their potentially disruptive effects.[224] Countermeasures provide such required recourse in responding to uses of force that fall below the armed attack threshold and as a result, have a pivotal role in governing responses by injured states to cyber-operations.[225] Thus, the first stage of this analysis will be an inquiry into how states might use countermeasures to respond to cyber-operations constituting uses of force contemplated by Article 2(4) of the UN charter.

---

[220] Schmitt M, 'Cyber Operations in international law', 155.
[221] Sharp G, *Cyberspace and the use of force*, 60.
[222] Graham D, 'Cyber threats and the law of war,' 91.
[223] Article 51, *Charter of the UN*.
[224] Hinkle K, 'Countermeasures in the cyber context: One more thing to worry about', *the Yale Journal of International Law* 37, 2011, 12. - https://www.arnoldporter.com/~/media/files/perspectives/publications/2011/09/countermeasures-in-the-cyber-context-one-more-th__/files/publication/fileattachment/countermeasures-in-the-cyber-context_one-more-th__.pdf – 24 November 2019.
[225] Hinkle K, 'Countermeasures in the cyber context: One more thing to worry about', 12.

It should be noted that a State is at liberty to undertake unfriendly acts not at variance with its international obligations, such as imposition of sanctions or declaring a diplomat as *persona non grata*, so as to influence other states' behaviour.[226] Certain circumstances may allow a state to act in response to a cyber-operation in a manner that would otherwise constitute a violation of international law and this could be the use of force for purposes of self-defence pursuant to an actual or impending armed attack and likewise where a state relies on the plea of necessity, having fulfilled certain conditions, would preclude the wrongfulness of such an act if it is the only way for the state to safeguard its interests against what may be termed as a grave and imminent peril.[227]

4.2 Use of force countermeasures

The fact that states bear responsibility for their internationally wrongful acts is well established in the law of state responsibility and various judgements by the ICJ have confirmed this position as previously discussed. Countermeasures, as a doctrine of CIL[228] and cemented in the law of state responsibility, are measures (could be actions or omissions) taken by a state directed against another state that would otherwise constitute a violation of an obligation owed to that state with the purpose of causing it to comply with its international obligations.[229] Because of the fact that acts falling under countermeasures have the character of being otherwise unlawful, there are strict restrictions imposed on their use by international law as they limit the employment of countermeasures as to their purpose, how they are to apply considering other legal rights and duties, means and scope and originators and targets.[230] Countermeasures have further been recognized by the ICJ in the *Danube Dam* case[231] and *Nicaragua*[232] as well as by various arbitral tribunals[233].

---

[226] Egan B, 'International law and stability in cyberspace', *Berkeley Journal of International Law* 35(1), 2017, 177.
[227] Egan B, 'International law and stability in cyberspace', 178.
[228] Egan B, 'International law and stability in cyberspace', 178.
[229] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 54(3) *Virginia Journal of International Law*, 2014, 700.
[230] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 701.
[231] *Case Concerning the Gabcikovo-Nagumaros Project (Hungary v. Slovakia)*, ICJ Reports, 1997, 82.
[232] *Nicaragua v US*, ICJ, 100, 249.
[233] *Liability of Germany for Damage caused in the Portuguese colonies in South Africa (Germany v. Portugal)*, Arbitral award, Permanent Court of Arbitration, 1928, 1025; *Liability of Germany for acts committed after 31 July 1914 and before Portugal took part in the war (Portugal v. Germany)*, Arbitral award, Permanent Court of

It is important to note that although, in this case, countermeasures are employed in response to cyber-operations that constitute uses of force, the law of countermeasures does not restrict the mode of countermeasures to be also cyber-based. On the contrary, countermeasures in response to an internationally wrongful act carried out through the cyberspace may be either cyber-based or non-cyber-based and vice versa.[234] Because of this, not much emphasis will be placed on the form of countermeasures. Instead this dissertation will take a broad approach and address the substantive law of countermeasures without particular references to cyber-based countermeasures although it will be assumed that the countermeasures were triggered as a result of cyber-operations constituting internationally wrongful acts.

Countermeasures, as a possible avenue available for victim states against offensive cyber-operations constituting internationally wrongful acts are only available once certain preconditions have been met, these being that there must be breach of an international legal obligation that as owed to the victim state and that the acts are attributable to the state in question.[235] As this dissertation has exhaustively dealt with attribution requirements it shall, at this point, restrict itself to addressing the requirements and restrictions in the employment of countermeasures.

4.2.1. Countermeasures: Requirements and restrictions

4.2.1.1. Purpose

Countermeasures have the sole purpose of inducing the responsible state to comply with its international obligations owed to the offended state thereby returning a situation to lawfulness.[236] ARISWA provides that the responsible state is under an obligation to cease an act (if ongoing) and to make assurances of non-repetition if required by the prevailing circumstances.[237] The responsible state has the additional obligation of making full

---

Arbitration, 1930, 1035 and 1052; *Air Service Agreement of 27 March 1946 between the United States of America*
and France, Arbitral award, Permanent Court of Arbitration, 1978, 443-446.

[234] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 718.

[235] Article 2, ILC, *Draft articles on state responsibility for internationally wrongful acts.*

[236] Article 49(1), ILC, *Draft articles on state responsibility for internationally wrongful acts*.

[237] Article 30, ILC, *Draft articles on state responsibility for internationally wrongful acts.*

reparations for the injury[238] caused by its internationally wrongful act.[239] These provisions preclude countermeasure employed for other purposes such as retaliation or punishment.

Since the aim of countermeasures is to induce the responsible state to return to lawful relations between the states in question the ICJ has advanced a general requirement that they must be reversible.[240] The *Commentary*[241] to ARISWA, however, points to the fact that this is not an absolute requirement and countermeasures are not barred merely because they have some irreversible effects. As countermeasures are viewed generally as being temporary they should as far as possible be reversible in their effects in view of future legal relations between the two states.[242]

Another factor to consider under purpose is the risk of escalation. A countermeasure that will serve to only aggravate the situation will be viewed to be aimed at retaliation. The *Air Services* arbitration correctly noted that countermeasures should be used with moderation and are to be accompanied by "*a genuine effort at resolving the dispute*."[243] It should also be noted that countermeasures are reactive as opposed to prospective this is to mean that they may not be employed in anticipation of a hostile use of force.[244]

4.2.1.2. Situations precluding the employment of countermeasures

Countermeasures are not available for an internationally wrongful act that is complete and not likely to be repeated.[245] Article 53 of ARISWA directs for countermeasures to be terminated after compliance by the responsible state. However, countermeasures may continue if reparations are due although the internationally wrongful act is complete and this is also the case where the internationally wrongful act is part of a series of wrongful acts.[246]

---

[238] ARISWA provides that injury is any damage (could be material or moral) caused by the act of a state that is internationally wrongful.
[239] Article 31, ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[240] *Case Concerning the Gabcikovo-Nagumaros Project*, ICJ, 87.
[241] Crawford J, The International Law Commission's articles on State responsibility: Introduction, text and commentaries, Cambridge University Press, 2002.
[242] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 714.
[243] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 91.
[244] *Case Concerning the Gabcikovo-Nagumaros Project,* ICJ, 83.
[245] Article 49(2) and 52(3), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[246] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 715.

Another obstacle to the use of countermeasures is that it may not be employed or must be suspended once the internationally wrongful act has ceased and the dispute is pending before a court or tribunal[247] that may issue a binding decision.[248] This preclusion only applies once the matter is *sub judice* and is moderated by the requirement that the court or tribunal must have the authority to order interim means of protection.[249] A significant restriction on this requirement implies that the victim state may initiate or maintain countermeasures.[250]

Regarding reprisals, as recognised by the *Naulilaa* arbitration, a request for the responsible state to remedy its conduct must precede the countermeasure.[251] This position was cemented by the ICJ judgement in the *Danube dam* case requiring that the injured state directs the responsible state to discontinue its unlawful conduct or make reparations.[252] ARISWA reflects this requirement as it provides that the injured state should specify the conduct it deems unlawful and the form of reparations.[253] Related to this is the requirement that the victim state to notify the responsible state of its intended use of countermeasures and make an offer for negotiations, depending on the situation both notifications can be provided simultaneously.[254]

These requirements are not absolute and certain circumstances may necessitate immediate action from the injured state so as to preserve its rights and avoid or mitigate further injury. This is supported by the *Air Services* arbitration which submitted that it is impractical to establish a rule that may work to preclude countermeasures during negotiations.[255] The Author Michael Schmitt in writing, *'"Below the threshold" cyber operations: The countermeasures response option and international law'* gave the example of a wrongful cyber-operation directed at a State's banking system. He posits that the injured State can respond with cyber-countermeasures designed to block electronic access to bank accounts belonging to the responsible State and may not be well served to notify the latter of its

[247] The commentary to ARISWA notes that the phrase "court or tribunal" refers to any third party dispute settlement procedure.
[248] Article 52(3)(b), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[249] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 95 and 96.
[250] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 96.
[251] *Liability of Germany for Damage caused in the Portuguese colonies in South Africa,* PCA, 1026.
[252] *Case Concerning the Gabcikovo-Nagumaros Project,* ICJ, 84.
[253] Article 43(2) and 52 (1)(a), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[254] Article 52(1)(b), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[255] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 91.

intention to do as this would effectively afford the responsible State the opportunity to transfer its assets out of the country or grant the chance to rectify the vulnerabilities identified essentially depriving the injured State of the possibility of employing such countermeasures.

4.2.1.3. Restrictions

The obligation to abide by the prohibition of the use of force according to Article 2(4) of the UN Charter has the status of CIL and works as a restriction.[256] ARISWA reiterates this position.[257] Pursuant to this restriction is the necessity of an analysis to establish when certain acts qualify as uses of force and may not be used as countermeasures.

ARISWA precludes the use of belligerent reprisals as countermeasures.[258] The commentary[259] to this provision acknowledges this preclusion as set out in the 1929 Geneva Convention, the four 1949 Geneva Conventions and the 1977 Additional Protocol 1 to the Geneva Conventions.[260] Michael Schmitt in the same article, *'"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law'* advanced that there is a substantial agreement that this prohibition are reflective of CIL and as such reprisals targeting the persons subject to the conventions in an ongoing armed conflict are not permissible.[261] However, other states refute this position and instead assert that the prohibition against reprisals against civilians is not customary in nature therefore, it only applies to states that are parties to the Additional Protocol 1.[262]

Additionally, states are not allowed to breach certain obligations in undertaking countermeasures. As per Article 50(1) of ARISWA, countermeasures are not to affect obligations whose purpose is to protect fundamental human rights, breaches of peremptory

[256] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 718.
[257] Article 50(1)(a), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[258] Article 50(1)(c), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[259] Crawford J, The International Law Commission's articles on State responsibility: Introduction, text and commentaries.
[260] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 721.
[261] The people subject to these conventions are; the wounded, sick, shipwrecked, medical personnel, religious personnel and prisoners of war.
[262] The Commander's Handbook on the Law of Naval Operations, Department of the Navy Office of the Chief of Naval Operations and Headquarters, 2017, 6.2.4.

norms are not permitted[263] as well as countermeasures infringing on diplomatic or consular inviolability[264]. Schmitt gives the example that it would be forbidden to carry out attacks against an enemy's wounded personnel by cutting electricity to a medical facility in a way that would essentially affect their treatment in response to a kinetic or cyber-attack on one's own wounded soldiers. Similarly, an injured State may neither use kinetic nor cyber-means to incite genocide through manipulating the content of news reports as such invariably, cannot qualify as a countermeasure. Considering consular inviolability, a cyber-operation directed against an embassy's computer system or that is geared to intercepting encrypted diplomatic communications would not qualify as a countermeasure.[265]

4.2.1.4. Proportionality

By the wording of Article 51 of ARISWA *"Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."* This speaks to proportionality. The principle was established in the *Naulilaa* arbitration where it was stated that a disproportionate countermeasure amounts to a punishment or reprisal thus inconsistent with the objects and purpose of the law of countermeasures.[266] This effectively means that such acts will be regarded as illegal.

Later decisions have advanced a broader approach to proportionality that necessitates consideration of the right involved.[267] The broader approach to proportionality is not limited to the quantitative comparison of consequences. The tribunal in the *Air Service* arbitration advanced that in inter-state disputes, it is crucial to also take into account "*the importance of the principle arising from the alleged breach"*[268] going on to conclude that judgement of the proportionality of countermeasures is not simple and can at best be attained by approximation.[269] This broad approach was confirmed in the *Danube Dam* case.[270]

---

[263] 50(1), ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[264] 50(2)(b), ILC, *Draft articles on state responsibility for internationally wrongful acts*.
[265] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 723.

[266] *Liability of Germany for Damage caused in the Portuguese colonies in South Africa,* PCA, 1028.
[267] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA; *Case Concerning the Gabcikovo-Nagumaros Project,* ICJ.
[268] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 83.
[269] *Air Service Agreement of 27 March 1946 between the United States of America and France,* PCA, 83.
[270] *Case Concerning the Gabcikovo-Nagumaros Project,* ICJ, 84.

Countermeasures taken as a response to internationally wrongful cyber-operations attributable to a particular state may have the character of cyber-based or non-cyber-based countermeasures.[271] There as similarly neither requirements as to reciprocity[272] nor numerical congruency[273] in the employment of countermeasures the injured state.[274]

4.2.1.5. Evidentiary considerations

As countermeasures are tools of self-help employed by states, the injured state has to make the determination of whether an obligation owed has been breached and as a consequence it has to identify the originating state or non-state actor as the case may be. The problem of attribution has been addressed but particular to countermeasures this determination is important as a countermeasure undertaken by the victim state in error as to the identity of the originator or place of origin may be precluded from unlawfulness if such an error was based on a reasonable belief. [275] This is in contrast to where a claim may be considered as not being well founded the injured states action will not be regarded as a countermeasure therefore its wrongfulness would not be precluded. The *Commentary* to ARISWA suggested the standard of factual attribution to be one of "reasonable certainty" citing the *Iran-United States Claims Tribunal*.[276]

4.2.1.6. Originator and target of countermeasures

It was established in the *Nicaragua* case that only states injured by an internationally wrongful act may resort to the use of countermeasures.[277] ARISWA provides two exceptions to this principle these being that; if the obligation breached is owed to a group of states that include the victim state and is established for purposes of protecting the collective interest of

[271] Egan B, 'International law and stability in cyberspace', 178
[272] An injured state's countermeasures may breach different obligations different from those of the responsible state.
[273] The injured state may, through its countermeasures, respond through the breach of numerous obligations.
[274] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 726.
[275] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 727.
[276] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 727.
[277] *Nicaragua v US*, ICJ, 100, 249.

the group or the obligation breached is owed to the entire international community.[278] The later describes situations that involve violations of *erga omnes* obligations.[279]

Countermeasures are not to be employed against any other state other that the responsible state hence the necessity of attribution. It is important to note that countermeasures employed by one state against another that results in the breach of an obligation of the former to a third state is not precluded from being illegal due to that third state.[280]

4.2.1.7. Location of countermeasures

With respect to cyber-countermeasures the location from with they are launched does not affect its lawfulness. Although, if a countermeasure is launched from a third state, the acts may violate obligations owed to that state but would nonetheless qualify as a lawful countermeasure with reference to the responsible state.[281] Relatedly, the location of cyber-infrastructure through which a cyber-countermeasure against the responsible state passes through does not affect its lawfulness.[282]

4.3. Self-defence and the use of force

Having discussed exceptions to the prohibition of the use of force under Article 51 of the UN Charter - these being exercise of the inherent individual or collective right to self-defence in response to armed attacks and authorization by the UNSC – an important discussion to be had is the modification of Charter rules vis a vis the CIL prohibition on the use of force. This has been discussed by Dapo Akande in a lecture at the Canadian Council of International Law Annual Conference where he advanced the structural issues relating to evolution of Charter rules through state practice as regards the prohibition on the use of force.[283] The

[278] Article 48(1), ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[279] *Barcelona Traction (Belgium v. Spain)*, ICJ Reports 1970, 33.
[280] *Corn Products International, Inc. v. United Mexican States*, Decision on Responsibility, ICSID Case No. ARB(AF)/04/01, 2008, 176.
[281] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 730.
[282] Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 730.
[283] -https://www.ejiltalk.org/the-diversity-of-rules-on-the-use-of-force-implications-for-the-evolution-of-the-law/ - on 5 December 2019.

converse position was taken by Katie Johnson based on those discussions, she proposes that modification of Charter rules could impact the customary prohibition on force.[284]

Dapo Akande, with basis in the *Nicaragua* case[285], noted that UN Charter provisions under Article 2(4) and 51 exist independently as CIL. He argues that an interpretation of the UN Charter through subsequent practice with reference to Article 31(3)(b) of the VCLT a UNGA *Uniting for Peace* resolution, that has its basis in the Charter[286], would be viewed as not being contrary to the prohibition of the use of force in a similar way as through an authorizing UNSC resolution. Also according to what he terms as a dynamic (as opposed to static) reference to the inherent right of self-defence in view of the ICJ ruling in *Nicaragua* is the adaptation of the customary rule to arguably apply to self-defence against non-State actors and by extension Article 51 of the UN charter. To further explain this position, he distinguishes between Article 2(4) and Article 51 in relation to their corresponding customary rules such that in the former custom mirrors the treaty whereas in the latter the treaty provision essentially preserves the customary rules of self-defence hence the relevance of the requirements of necessity and proportionality despite the fact that they do not feature in the provision.

However, Katie Johnston took a pessimistic approach hardly agreeing with the notion that customary rules can modify Charter rules on the use of force. Instead she advances that an interpretation of the UN Charter such that a *Uniting for Peace* resolution was not viewed as an unlawful use of force would not affect the customary prohibition with basis in the fact that they exist independently. This may be reconciled through the presumption that a Charter rule would prevail over the customary prohibition to the extent that they conflict, however this approach becomes problematic considering the fact that the customary rule is possibly a *jus cogens* norm. She takes the view that the interpretation of the UN Charter would be analogous to a new treaty amendment that is in conflict with a *jus cogens* norm hence invalid under article 53 of the VCLT.

---

[284] -http://www.ejiltalk.org/reconciling-new-interpretations-of-the-un-charter-with-the-customary-international-law-on-the-use-of-force/ - on 5 December 2019.
[285] *Nicaragua v US*, ICJ.
[286] Article 11(2), *Charter of the UN*.

Resolution may be found in taking the view that reference to the inherent right of self-defence[287] is dynamic in nature, its content adapting as customary law changes and by extension changes the content of the UN Charter's Article 2(4) exception as the CIL on self-defence changes without requiring modification of the corresponding treaty provision. Katie Johnson refers to the Article 51 of the UN charter as being ambulatory and further proposes that the collective security exception to the customary prohibition is also ambulatory. Therefore, State practice under Article 31(3)(b) would work as an exception whose content will track the changes in the treaty law.[288] The upshot of this would be that acts taken in self-defence against non-State actors would be legitimized both under Article 51 of the UN Charter and in CIL.[289]

4.3.1. Necessity, proportionality and immediacy

A cyber-operation having crossed to the threshold of an armed attack allows the victim state to exercise its inherent right of self-defence according to Article 51 of the UN Charter. This avenue is, of course, available once attribution requirements have been met. Additionally, the exercise of a states right of self-defence should be done with due regard to the dictates of necessity, proportionality and immediacy,[290] this is reflected in the Tallin Manual.[291]

In the *Nicaragua* case it was confirmed that the principles of necessity and proportionality have the status of CIL.[292] Necessity limits the degree of force that a victim state may use against legitimate targets to the degree that is strictly necessary. In the *Caroline* case the then US Secretary of State captured the necessity requirement as being satisfied where the attacks

[287] Article 51, *Charter of the UN*.
[288] - http://www.ejiltalk.org/reconciling-new-interpretations-of-the-un-charter-with-the-customary-international-law-on-the-use-of-force/ - on 5 December 2019.
[289] -https://www.ejiltalk.org/the-diversity-of-rules-on-the-use-of-force-implications-for-the-evolution-of-the-law/ - on 5 December 2019.
[290] Holmberg E, 'Armed attacks in cyberspace do they exist and can they trigger the right to self-defence?' Unpublished LLM Thesis, Faculty of Law Stockholm University, Stockholm, 2015, 40.
[291] Rule 14 and 15, Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2013).
[292] *Nicaragua v US*, ICJ, 100, 176.

were instant and overwhelming such that it leaves neither choice of means nor moment for deliberation.[293]

Proportionality as a principle of *jus in bello* requires that the means and extent of measures taken in self-defence have to be proportionate with the gravity of the armed attack.[294] This principle derives from the Additional Protocol 1 which protects civilians and their property.[295] Immediacy as a requirement is understood to mean that self-defence measures may only be undertaken within a reasonable time after the offending action has occurred.[296]

In the context of cyber-operations amounting an armed attack triggering the injured State's right of self-defence, even if were the case that such an attack was of a scale and magnitude comparable to a kinetic attack these requirements would be hard to fulfil (necessity, proportionality and immediacy). Factors contributing to this are; the attribution problem owing to masking techniques in cyberspace and the fact that self-defence in response to a cyber-attack has been seen to only be proportional when the malicious attack under extreme circumstances, for example attacks with catastrophic results.[297]

4.3.2. Anticipatory self-defence

With the recognition that aggression does not necessarily begin with shots being fired or territorial sovereignty being infringed, especially considering acts in the cyberspace, anticipatory self-defence functions to allow states to defend themselves against such attacks.[298] Anticipatory self-defence as a doctrine was established in the *Caroline* case where the US and UK agreed that the anticipatory self-defence measure was lawful when its

[293] Letter from U.S. Secretary of State, Daniel Webster, to Lord Ashburton, Aug. 6, 1842. - https://avalon.law.yale.edu/19th_century/br-1842d.asp - on 26 November 2019.
[294] Holmberg E, 'Armed attacks in cyberspace do they exist and can they trigger the right to self-defence?' Unpublished LLM Thesis, Faculty of Law Stockholm University, Stockholm, 2015, 41.
[295] Article 51(5)(b), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*, 8 June 1977, 1125 UNTS 3.
[296] Dinstein Y, War, aggression and self-defence, 4th ed', Cambridge University Press, Cambridge, 2005, 237.
[297] Holmberg E, 'Armed attacks in cyberspace do they exist and can they trigger the right to self-defence?' Unpublished LLM Thesis, Faculty of Law Stockholm University, Stockholm, 2015, 42.
[298] Sklerov M, 'Solving the dilemma of state responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent', Published LLM Thesis, Judge Advocate General's School, 2009, 40.

necessity is instant, overwhelming neither leaving choice of means nor moment for deliberation.[299]

Acts of self-defence in anticipation of an armed attack depends on the immanency of the attack. This derives from the principle of immediacy and generally allows a state to use force in advance of an armed conflict in order to repel such an attack before it is carried out by an identified aggressor. Immanency precludes the illegality of force in advance of an attack when there is evidence supporting the fact that an aggressor has committed to carrying out an armed attack and the delay would otherwise equate to hindering the defender's ability to put up a meaningful defence.[300]

4.4. Conclusion

The foregoing discussions in this chapter do show that there are indeed measures available for a state that has fallen victim to uses of force and armed attacks these being countermeasures and self-defence measures respectively. Still, regarding countermeasures, availability does not speak to effectiveness and the restraints on them – necessity and proportionality – have been viewed as not providing adequate limitations as currently formulated when applied to cyberspace.[301] With international law slowly adapting to the phenomenon of the cyberspace it may be too early to judge how effective the current avenues will be especially regarding uses of force that do not rise to the level of an armed attack as there will be foreseeably more and more cyber-operations meeting that threshold as opposed to the more serious degree both offensively and defensively of an armed attack.

"A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all"

Jens Stoltenberg, the North Atlantic Treaty Organization (NATO) Secretary General, in no unclear terms, advanced NATO's position in writing for the Prospect Magazine.[302] He correctly noted the unique nature of cyber-operations whereby a single cyberattack has the

[299] Sklerov M, 'Solving the dilemma of state responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent', Published LLM Thesis, Judge Advocate General's School, 2009, 41.
[300] Schmitt M, 'Preemptive strategies in international law'24(2) *Michigan Journal of International Law*, 2003, 513 and 534.
[301] Hinkle K, 'Countermeasures in the cyber context: One more thing to worry about', 21.
[302] - https://www.prospectmagazine.co.uk/world/nato-will-defend-itself - on 25 November 2019.

potential to inflict damages to the tune of billions of dollars, paralyze critical infrastructure, cripple military capabilities and even destabilize governments. This concern is amplified, as cyber-threats to the NATO alliance are becoming frequent with more complexity and increased destructive capabilities. The upshot of this statement is that NATO has committed to triggering Article 5 of the North Atlantic Treaty which has the character of a collective defence measure involving the exercise of their individual and collective rights of self-defence. This statement may very well set the tone for international relations on how states respond to cyber-operations.

Having gone into relevant analyses of aspects of cyber-operations it is evident that the international law governing cyber-operations is at its infancy and therefore wanting. The next chapter will be aimed at addressing the gaps identified and will propose recommendations that feed into the hypothesis.

CHAPTER 5

Recommendations and conclusion

5.1. Introduction

The information revolution inevitably opened the doors to a new arena of warfare with the potential to harm other States and cripple their economies. Borders are reduced to a mere formality by existing cyber-capabilities. With the proliferation of cyber-operations globally there needs to be a corresponding push for solutions to address this phenomenon.

As this dissertation is directed towards attribution and State responsibility the recommendations proposed will be aligned to meet the gaps that have been identified. This is with the aim of satisfying this dissertation's hypothesis that if the current trend continues where States evade responsibility for malicious cyber-operations then there will inevitably be more and more instances of cyber-attacks with foreseeably graver effect and magnitude.

This being the final chapter it will propose various recommendations and conclude the dissertation. These recommendations will be mostly regulatory in nature as their focus will be on attribution and State responsibility in international law.

5.2. Recommendations

5.2.1. A treaty on cyberwarfare

The post-World War II environment was characterised by the nuclear arms race particularly among the world powers. These unchecked nuclear capabilities came with them a heightened risk of nuclear war. The nuclear arms race culminated in arms control agreements that restored a sense of calm in that, although there are still potential risks of nuclear threats, the agreements have with them a binding nature on State parties that greatly mitigated the situation and outweighs a free-for-all environment.[303] By analogy, this dissertation advances that the same logic applies to cyber-capabilities.

Discussions have brought out the risks in latent cyber-capabilities, even more clearly with the analysis of the NotPetya attack. There is additionally the finding that current laws governing

[303] Makory J, 'Cyberwarfare regulation', 54.

cyberwarfare merely serve as soft-law with no binding force on States. This coupled with the fining that more and more cyber-incidents are being reported begs for resolution through a binding treaty on cyberwarfare.[304]

The prospect of cyberwarfare remains as real a possibility as the possibility of nuclear war was with unchecked capabilities therefore the international community should have a legitimate concern over these capabilities and work towards setting standards that are to be agreed upon by States with clear parameters.[305] Through the United Nations – the organization with the mandate of maintaining international peace and security – a treaty of this nature whose aim would be to secure peace and justice would serve its ends. This is owing to the fact that such a treaty would bring about a common standard under which State parties will be held resulting to certainty and predictability with respect to the place of cyberwarfare in international law.[306]

Considering the fact that a regulatory framework of governing cyber-war does not exist unlike where conventional means of war are regulated by various international treaty laws which are well respected in the international community, this similarly needs to be remedied.[307] To this end IHL may be extrapolated, as a relatively short term measure, to meet the ends of regulating the cyberwarfare and by extension cyberspace, with the awareness that *lex specialis* (law designed to govern a specific subject matter) will unquestionably be more effective.[308]

This dissertation advances that there are certain key areas that such a treaty will be well served to clarify, these being;

i) Definite standards for the international community to apply when determining whether particular cyber-operations quality as either uses of force or when they cross that threshold and can be termed as an armed attack.

---

[304] - https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents - on 2 December 2019.

[305] The Guardian, Mueller B, 'Why we need a cyberwar treaty' - https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty - on 2 December 2019.

[306] Makory J, 'Cyberwarfare regulation', 55.

[307] The Guardian, Mueller B, 'Why we need a cyberwar treaty' - https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty - on 2 December 2019.

[308] The Guardian, Mueller B, 'Why we need a cyberwar treaty' - https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty - on 2 December 2019.

ii) What is to be considered permissible behaviour among States.

iii) The form that countermeasures and self-defence measures should take in the event a State is found to be in breach of its obligations under international law.

It is crucial for many States to be party to the treaty as this will give it a large backing and secure commitment from a large portion of the international community.[309] A treaty on cyberwarfare will be advantageous in the following ways;

i) Government organs, such as the military, will have standards within which they will be expected to conduct themselves and this will result to duties and obligations by States.[310]

ii) An effective sanction regime particular to internationally wrongful acts committed in cyberspace will act as a deterrent to States in carrying out unscrupulous cyber-operations.[311]

iii) A treaty would secure international cooperation which would be invaluable due to the transboundary nature of cyberspace and more particularly, cyber-attacks.[312]

5.2.2. An international tribunal for cyberspace

At the 13th International Criminal Law Congress that was held in Queenstown Judge Stein Schjolberg presented a paper arguing for an International Criminal Tribunal for Cyberspace (ICTC).[313] He correctly argues that the UNSC could establish an ICTC under Chapter 7 of the UN Charter whose mandate would be investigating, prosecuting and sentencing of cyber-attacks in the purview of cyberwarfare and that the UN would be the most effective means, reason being that, due to its relatively large membership, it would be binding on member States.[314] This is hardly an unprecedented recommendation following the UNSC decision in establishing the ICTR and the ICTY based on the charter.[315]

He proposes a fully independent ICTC and would be established with the goal of ensuring that perpetrators of the most serious cyber-attacks are not left unpunished. In terms of

[309] Makory J, 'Cyberwarfare regulation', 56.
[310] Makory J, 'Cyberwarfare regulation', 56.
[311] Makory J, 'Cyberwarfare regulation', 56.
[312] Makory J, 'Cyberwarfare regulation', 57.
[313] Schjolberg S, 'An international criminal tribunal for cyberspace' East West Institute Cybercrime Legal Working Group, 2012. - https://www.cybercrimelaw.net/documents/ICTC.pdf - on 2 December 2019.
[314] Schjolberg S, 'An international criminal tribunal for cyberspace'.
[315] Article 39, *Charter of the UN*.

composition he advances that there should 16 permanent judges who are UN appointees to be divided between 3 trail chambers and a sole appeals chamber, the judges serving a period not exceeding 4 years.[316] He proposed that, regarding cyber-incidences, the office of the prosecutor may start investigations *ex-officio* or from information obtained from any other source, with an emphasis on governments, UN organs, intergovernmental and non-governmental organizations. Of particular weight was that the prosecutor's office had the power to collect evidence and conduct investigations and to seek assistance in carrying out investigations by INTERPOL and the INTERPOL Global Complex.[317] This will resolve what this paper termed as state practice directed towards 'the sound of silence'.[318] Just as the treaty, this ICTC though the office of the prosecutor shall be crucial in remedying the current situation of State responsibility as regards the requirement that such acts must be attributable to a State.

5.2.3. The Definition of Aggression

The UNGA through Resolution *3314 (XXIX)* adopted the *Definition of Aggression* with the aim of strengthening international peace and security. As it is, situations that are construed as constituting such acts are provided for under Article 3 of the *Definition of Aggression* resolution and are markedly restricted to conventional means of warfare. Jade Makory in her writing of *'Cyber Warfare Regulation: A Liability and Jurisdiction Disquisition'* aptly notes that an argument could be made that the broad provisions under the resolution could, by analogy, apply to cyber-attacks more so due to the fact that the resolution was seen to further the application of Pictet's criteria directed towards establishing the existence of an international armed conflict. She proposes that due to the inherent complexity of cyberspace a definition of aggression that specifies the particulars that would constitute aggression in cyberspace is necessitated. Therefore, the Assembly of State Parties should establish a definition of aggression that addresses the challenges that subsist in cyberspace as well as taking into consideration the challenge posed by various actors in cyberspace with a focus on non-State actors where there has yet to be sufficient clarity as a result of there being no

[316] Schjolberg S, 'An international criminal tribunal for cyberspace'.
[317] Schjolberg S, 'An international criminal tribunal for cyberspace', 21.
[318] Fidler D, 'Was Stuxnet an act of war? Decoding a cyberattack', 57.

express provision on the validity of attributing State responsibility due to actions of non-State actors.

5.2.4. Extraterritorial application of domestic law

Domestic law is a significant factor in combating cyber-attacks as observed in the NotPetya case study, particularly as a rebuttal to presumptive legitimacy for malicious cyber-attacks characterized as uses of force. Noting that not all cyber-attacks may fall within the definitional categorization of cyber-crimes, many cyber-attacks are also cybercrimes including those than involve non-State actors in cyberspace.[319] Despite this being the case, a relatively small number of existing domestic criminal laws governing cyber-attacks provide for extraterritorial reach.[320]

Extraterritorial reach, if so provided for under domestic laws of States, will not only significantly affect global enforcement but also aid solving the challenge posed by lone-wolf hackers and non-State actors in particular. *A priori*, a legitimate and effective application of extraterritorial application will be more so, if it were to work in tandem with a treaty which establishes basic shared standards regarding cyber-attacks.[321] However, it is conceded that this recommendation may be significantly affected by jurisdictional issues as regards enforcement. On the other hand, strengthening extradition relationships will overcome this perceived hurdle and compliment increased extraterritorial of domestic law.

5.3. Conclusion

The focus of this dissertation has been on matters pertinent to attribution and State responsibility as regards cyber-attacks. To further the analysis, it employed the use of the NotPetya attack as a case study.

Chapter 2 found that a cyber-attack can indeed qualify as an act of aggression. *Jus ad bellum* considerations dealt with cyber-operations that range from permissible ones to those rising to the level of an armed attack. It also addressed *jus in bello* considerations which are the subject of IHL. In the NotPetya analysis of whether it could fit within the conceived

[319] Hathaway O, 'Law of cyber attack', 878.
[320] Hathaway O, 'Law of cyber attack', 878.
[321] Hathaway O, 'Law of cyber attack', 878.

parameters, the dissertation concluded that the particular attack satisfied the Schmitt criterion for uses of force. It similarly satisfied each of Pictet's criteria for an armed attack.

Chapter 3 dealt with State responsibility and issues of burden and the requisite standards of proof applicable to cyber-attacks. State responsibility may attach to both State and non-State actors as both are subjects of international law. The various requirements in respect to both categories of actors were outlined. Interestingly, the complexity of attribution became much clearer in this discussion. Various characteristics particular to cyber-operations were brought out. The burden of proof and standards of proof as regards cyber-attacks were conclusively dispensed with. Oliver Wendell Holm's theory as well as the counterintuitive theory proposed where States are seen to comply only when such compliance secures a corresponding cooperation are pervasive throughout the discussions but more so in the discussions on State responsibility.

The fourth chapter addressed consequences in the event a State were to be found liable for acts that constitute a use of force or an armed attack. This discussion was vital as it served as a resolution to the question of State responsibility and goes a step further to anticipate possible repercussions for cyber-operations. The specific discussions were on; countermeasures dealing with acts categorized as uses of force and self-defence measures applicable to acts that surpassed the threshold of a use of force rising to the level of an armed attack.

Chapter 5 of this dissertation proposed various recommendations and concludes the dissertation. The recommendations were global regulatory and institutional recommendations advanced in order to meet the gaps identified during the discussions. These were specifically the need for a treaty governing cyberwarfare, establishing of an ICTC, expanding the definition of aggression to incorporate cyberwarfare and extending the extraterritorial reach of domestic laws. These are to be tailored in such a way that will meet the challenges posed by advance cyber-capabilities at the international level.

It is the author's hope that the recommendations will serve to aid in discussions at various decision making levels on matters concerning attribution and State responsibility. Additionally, it should greatly assist in any retrospective analysis of the NotPetya attack against Ukraine.

BIBLIOGRAPHY

Books

Dinstein Y, War, aggression and self-defence, 4th ed', Cambridge University Press, Cambridge, 2005

Lytvynenko O, Fluri P, Badrack V, 'The security sector legislation of Ukraine,' Geneva, Kyiv, 2017.

Moore J, 'The use of force in regulating international relations: Norms concerning the initiation of coercion' in Moore J and Turner R, *National Security Law*, 2nd ed, Carolina Academic Press, Durham, North Carolina, 2005.

Journal articles

Buchan R, 'Cyberspace, non-state actors and the obligation to prevent transboundary harm' 21(3) *Journal of Conflict and Security Law*, 2016.

Cenic S, 'State responsibility and self-defence in international law post 9/11: Has the scope of article 51 of the United Nations Charter been widened as a result of the US response to 9/11?' 14 *Australian International Law Journal*, 2007.

Christakis K, 'Cyber diligence: a low intensity due diligence principle for low intensity cyber operations' 14 *Baltic Yearbook of International Law*, 2014.

Egan B, 'International law and stability in cyberspace', *Berkeley Journal of International Law* 35(1), 2017.

Geers K, 'The challenge of cyber attack deterrence,'26 *Computer Law and Security Review*, 2010.

Gervais M, 'Cyber-Attacks and the Laws of War' 30 *Berkeley Journal of International Law* 2, 2012.

Graham D, 'Cyber threats and the law of war,' 4(1) *Journal of National Security Law and Policy*, 2010.

Green J, 'Fluctuating evidentiary standards for self-defence in the International Court of Justice' 58(1) *the International and Comparative Law Quarterly,* 2009.

Hathaway A, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W and Spiegel J, 'The law of cyber-attack' 100 *California Law Review,* 2012.

Holms O, 'The path of the law', *Harvard Law Review,* 1897.

Jimenez M, 'Funding the good in Holms's bad man' 79(5), *Fordham Law Review,* 2011.

Kelsey T, 'Hacking into International Humanitarian Law: The principles of distinction and neutrality in the age of cyber warfare,' 106(7) *University of Michigan Law School,* 2008.

Lin H, 'Offensive cyber operations and the use of force' 4 *Journal of National Security Law and Policy* 63, 2010.

Milanovic M, 'State responsibility for genocide', 17(3) *European Journal of International Law,* 2006.

Ridddell A and Plant B, 'Evidence before the international court of justice', 2009.

Roscini M, 'Evidentiary issues in international disputes related to state responsibility for cyber operations' 50 *Texas International Law Journal,* 2015.

Shackelford S, Russel S and Kuehn A, 'Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors,' *Chicago Journal of International Law,* 2016.

Schmitt M, '"Below the threshold" cyber operations: The countermeasures response option and international law', 54(3) *Virginia Journal of International Law,* 2014.

Schmitt M, 'Computer network attack and use of force in international law: Thoughts on a normative framework,' 37, *Colombia Law Journal of Transnational Law,* 1999.

Schmitt M, 'Cyber Operations in international law: The use of force, collective security, self-defense and armed conflicts,' *Durham University Law School,* 2010.

Schmitt M, 'Preemptive strategies in international law'24(2) *Michigan Journal of International Law,* 2003.

Schmitt M and Watts S, 'The decline of International Humanitarian Law opinio juris and the law of cyber warfare,' 50(2) *Texas International Law Journal,* 2015.

Schmitt M N, 'Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' *New York: Cambridge University Press (2013).*

Schmitt M N, 'Tallinn manual 2.0 on the international law applicable to cyber operations: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence' New York: Cambridge University Press (2017).

Teitelbaum R, 'Recent fact-finding developments at the International Court of Justice,' 6(1) *The Law and Practice of International Courts and Tribunals,* 2007.

Tran D, 'The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack' 20 *Yale Journal of Law and Technology* 2018.

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

Verdier P and Voeten E, 'Precedent, compliance and change in customary international law: an explanatory theory' 108 *American Journal of International Law,* 389, 2014.

Vihul L and Schmitt M, 'Proxy wars in cyberspace: the evolving international law of attribution' 1 *Fletcher Security Review,* 2014.

Waxman M, 'Self-defence force against cyber attacks: Legal, strategic and political dimensions,' 89 *International Law Studies,* 2013.

Internet sources

Carrazana L, 'The economics of cybersecurity and cyberwarfare: A case study,' Economics Colloquium, 5 December 2018.– http://austrianstudentconference.com/wp-content/uploads/2019/02/ASSC-2019-Lorenzo-Carrazana.pdf on Monday, 23 September 2019.

Egan B, 'International law and stability in cyberspace' 35 *Berkeley Journal of International Law* 1, 2017, 178. https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf on Wednesday, February 20, 2019.

Hinkle K, 'Countermeasures in the cyber context: One more thing to worry about', *the Yale Journal of International Law* 37, 2011. - https://www.arnoldporter.com/~/media/files/perspectives/publications/2011/09/countermeasures-in-the-cyber-context-one-more-th__/files/publication/fileattachment/countermeasures-in-the-cyber-context_one-more-th__.pdf – 24 November 2019.

Kessler O and Werner W, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' *Leiden Journal of International Law* 26, 2013, 798. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/F72E80E8768C66B8C0CBEBB413E643C5/S0922156513000411a.pdf/expertise_uncertainty_and_international_law_a_study_of_the_tallinn_manual_on_cyberwarfare.pdf on Tuesday, 19 February 2019.

Kondratov S, Dmytro B, Horbulin V, Sukhodolia O, Ivaniuta S, Nasvit O, Biriukov D, Riabtsev G, 'Developing the critical infrastructure protection system in Ukraine,' National Institute for Strategic Studies, 2017. - http://www.niss.gov.ua on 27 September 2019.

Mitchelle R, 'Sovereignty and normative conflict: international legal realism as a theory of uncertainty' *58 Harvard International Law Journal*, 2, 2017, 435. http://www.harvardilj.org/wp-content/uploads/HLI204_crop.pdf on Tuesday, February 19, 2019.

Osawa J, 'The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem?' *Asia-Pacific Review.* - https://doi.org/10.1080/13439006.2017.1406703 on September 27, 2019.

Schjolberg S, 'An international criminal tribunal for cyberspace' East West Institute Cybercrime Legal Working Group, 2012. - https://www.cybercrimelaw.net/documents/ICTC.pdf - on 2 December 2019.

Schmitt M, 'Cyber operations and the jus ad bellum revisited' 56 *Villanova University Charles Widger School of Law* 3, 2011. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1019&context=vlr on Tuesday, 19 February 2019.

Scientific and Research Centre of Military History, 'Means of Russia hybrid warfare against Ukraine,' National Defense University of Ukraine, Kyiv, 2017. - https://nuou.org.ua/assets/documents/scientific-edition.pdf on Thursday, October 3, 2019.

https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm - on Saturday, 1st December 2018.

https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2567&context=faculty_scholarship –on Saturday, 1st December 2018.

https://www.nato.int/cps/en/natohq/topics_78170.htm - on Saturday, 1st December 2018.

https://edition.cnn.com/2018/05/06/opinions/opinion-andelman/index.html - on Saturday, 1st December 2018.

https://www.telegraph.co.uk/news/worldnews/europe/russia/11314817/Secret-dead-of-Russias-undeclared-war.html - on Friday, 14 December 2018.

https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html - on Friday, 14 December 2018.

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ - on Friday, 14 December 2018.

https://www.cfr.org/blog/year-review-malware-attacks-impact-operations-and-bottom-line - on Friday, 14 December 2018.

http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/McDougall_20161021.pdf - on Friday, 14 December 2018.

https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1 – on Friday, 14 December 2018.

https://www.bbc.com/news/uk-politics-43062113 - on Friday, 14 December 2018.

https://www.linkos.ua/ on Monday, 23 September 2019.

https://www.pravda.com.ua/news/2017/06/29/7148210/ on Saturday, 28 September 2019.

https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2_7/Kapitel2_7_5/kapitel2_7_5_node_en.html on 3 October 2019.

https://www.cpni.gov.uk/critical-national-infrastructure-0 on 3 October 2019.

https://en.hromadske.ua/posts/unknown-virus-attacks-ukraines-state-banks-and-enterprizes on Saturday, 28 September 2019.

https://www.dhs.gov/cisa/critical-infrastructure-sectors on 3 October 2019.

https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/- on Sunday, 17 November 2019.

https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/- on 17 November 2019.

https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks- on 17 November 2019.

https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/- on 17 November 2019.

https://www.trackingterrorism.org/group/sandworm – on 21 November 2019.

https://www.reuters.com/article/russia-cyber/hackers-accused-of-ties-to-russia-hit-3-e-european-companies-cybersecurity-firm-idUSL8N1WP37F - on 21 November 2019.

https://www.globalsecurity.org/intell/world/russia/gru-ops.htm – on 21 November 2019.

https://www.bbc.com/news/uk-politics-43062113 - on 17 November 2019.

https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims - on 17 November 2019.

https://www.ncsc.gov.uk/news/turla-group-malware - on 17 November 2019.

https://www.bbc.com/news/election-2019-50388879 - on 17 November 2019.

http://www.ejiltalk.org/reconciling-new-interpretations-of-the-un-charter-with-the-customary-international-law-on-the-use-of-force/ - on 5 December 2019.

https://www.ejiltalk.org/the-diversity-of-rules-on-the-use-of-force-implications-for-the-evolution-of-the-law/ - on 5 December 2019.

https://www.prospectmagazine.co.uk/world/nato-will-defend-itself - on 25 November 2019.

https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents - on 2 December 2019.

The Guardian, Mueller B, 'Why we need a cyberwar treaty' - https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty - on 2 December 2019.

Thesis and Dissertations

Holmberg E, 'Armed attacks in cyberspace do they exist and can they trigger the right to self-defence?' Unpublished LLM Thesis, Faculty of Law Stockholm University, Stockholm, 2015.

Makory C, 'Cyberwarfare regulation: A liability and regulation disquisition' Unpublished LLB Dissertation, Strathmore University Law School, Nairobi, 2018.

Sklerov M, 'Solving the dilemma of state responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent', Published LLM Thesis, Judge Advocate General's School, 2009.

Other UN documents

Draft articles on state responsibility for internationally wrongful acts, ILC 53rd Report, 2001, UN Doc A/56/10.

Reports

Melzer N, *International Humanitarian Law a comprehensive introduction*, International Committee of the Red Cross, Geneva, 2016.

Owens W, Dam K, Lin H, 'Technology, policy, law and ethics regarding U.S. acquisition and use of cyberattack capabilities,' National Research Council of the National Academies, 2009.

Sharp G, *Cyberspace and the use of force*, Aegis Research Corporation, 1999.

Schmitt M, '" Attack" as a term of art in international law: the cyber operations context' 4th International Conference on Cyber Conflict, International Law Department, United States Naval War College, Newport, 2012.

United Nations General Assembly

UNGA, Definition of aggression, UN A/Res/3314 (XXIX) 14 December 1974.

United Nations Security Council

UNSC S/RES/1368 (2001) Threats to international peace and security caused by terrorist acts.

UNSC S/RES/1373 (2001) On threats to international peace and security caused by terrorist acts.