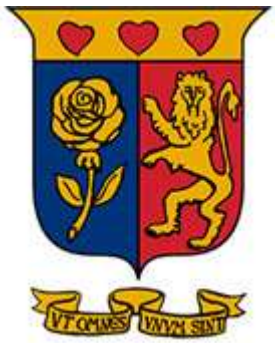

STRATHMORE LAW SCHOOL

CYBERWARFARE REGULATION: A LIABILITY AND JURISDICTION DISQUISITION

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

By

MAKORY JADE CYNTHIA

082728

Prepared under the supervision of

Mr. Allan Mukuki

January 2018

Word count (18,223)

Table of contents

Declaration

I, MAKORY JADE CYNTHIA, 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

Dedication

To all victims of atrocities committed through cyberspace, to whom transgressions have been committed yet no faults found, no recourse made available, no reparations considered due.

Acknowledgments

I am profoundly beholden to Mr. Allan Mukuki, my supervisor, for all the direction he has afforded to me throughout my research. I am also appreciative of the support and encouragement that has been ever-present from my family.

Abstract

This dissertation addresses cyberwarfare regulation through the lens of liability and jurisdiction, seeking to address its three objectives: an analysis of the legal framework regulating cyberwarfare in international law; an analysis as to how liability with regard to cyberwarfare may be addressed; and, a further analysis as to how jurisdiction with regard to cyberwarfare may be established. The methodology used to conduct this research was desk research with the relevant materials being analysed to give relevant insight. It was not possible to carry out field research because of how sensitive matters pertaining to warfare are, and to this regard, most of the information not published is confidential.

Chapter 2 addresses the first objective. It looks at both positive and normative international law as they both constitute important dimensions of international law. It goes a step further to mention the two Tallinn Manuals on cyber operations which constitute soft law. Chapter 3 addresses the second objective. It looks at both individual and state liability. Chapter 4 addressed the third objective. It looks into the principles of establishing jurisdiction under international law. Sovereign immunity and inviolability are also looked into because they provide exceptions to the establishment of jurisdiction. Chapter 5 addresses the recommendations and provides a conclusion to the dissertation. The legal solutions recommended include: there ought to be established an international treaty that will address the issue of cyberwarfare; if it is not possible to have consensus about a treaty, there ought to be an international tribunal for cyberwarfare established by the Security Council drawing its mandate from Chapter VII of the Charter of the United Nations; the mandate of the World Trade Organisation should be expanded to deal with digital industrial espionage; the definition of aggression should be expanded to incorporate cyberwarfare; and, capacity should be built on the international level to address the issue of cyberwarfare.

List of cases

English case law

Daimler Company Limited v Continental Tyre and Rubber Company (1916) 2AC 307.

European Court of Justice (ECJ) case law

Re Wood Pulp Cartel (Ahlström Osakeyhtiö and others v Commission of the European Communities) (1994), ECJ.

Iran-US Claims Tribunal cases

Amoco International Finance Corporation v Iran (1985), Iran-US Claims Tribunal.

International Criminal Court (ICC) case law

Prosecutor v Jean-Pierre Bemba Gombo (Trial Judgment), ICC-01/05-01/08, 21 March 2016.

International Court of Justice (ICJ) case law

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

Corfu Channel Case (UK v Albania), ICJ Reports 1949.

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

Gabcikovo-Nagymaros Project (Hungary v Czechoslovakia), ICJ Reports 1997.

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

The case of the United States Diplomatic and Consular Staff in Tehran (US v Iran) (1980), ICJ Reports 1980.

International Criminal Tribunal for Rwanda (ICTR) case law

Prosecutor v Jean-Paul Akayesu (Trial Judgement), ICTR-96-4-T, ICTR, 2 September 1998.

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

Prosecutor v Radislav Krstic (Appeal Judgement), IT-98-33-A, ICTY, 19 April 2004.

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

Prosecutor v Tihomir Blaskic (Trial Judgement), IT-95-14-T, ICTY, 3 March 2000.

Nuremberg War Crimes Tribunal cases

Ferencz B, USA, *The Nuremberg War Crimes Tribunal* (1945).

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.

Convention on Registration of Objects Launched into Outer Space, 14 January 1975, 1023 UNTS 15.

Convention on the Law of the Sea, 10 December 1982.

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31.

Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention), 12 August 1949, 75 UNTS 85.

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

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

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.

Rome Statute of the International Criminal Court, Elements of Crimes, 011, ISBN No. 92-9227-232-2.

Rome Statute of the International Criminal Court, 17 July 1998, ISBN No. 92-9227-227-6.

Rome Statute of the International Criminal Court, Rules of Procedure and Evidence, ICC-ASP/1/3, at 10, 1 (2002), UN Doc PCNICC/2000/1/Add.1 (2000).

Second Protocol to The Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, 26 March 1999.

Statute of the International Court of Justice, 18 April 1946.

The North Atlantic Treaty, 4 April 1949.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 610 UNTS 205.

Vienna Convention on Diplomatic Relations, 18 April 1961.

List of acronyms and abbreviations

ARISWA	Draft Articles on State Responsibility
ARPANET	Advanced Research Projects Agency Network
Doc	Document
DoD	Department of Defence
DoS	Denial of Service
ECJ	European Court of Justice
GA	General Assembly
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
IAC	International Armed Conflict
IT	Information Technology
JCE	Joint Criminal Enterprise
NIAC	Non- international Armed Conflict
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
OAS	Organisation of American States
Res	Resolution
SC	Security Council

SCO	Shanghai Cooperation Organisation
TCP/IP	Transmission Communication Protocol/ Internet Protocol
UFO	Unidentified flying object
UK	United Kingdom
UN	United Nations
US	United States of America
USSR	Union of Soviet Socialist Republics
WTO	World Trade Organisation

CHAPTER 1

1.1 Introduction

Cyberspace is a global platform within the information environment. It comprises of resident data and networked information technology (IT) infrastructures to the inclusion of: networks in telecommunication, computer systems, embedded controllers and processors and the internet.[34] Cyberspace is therefore a space of virtual reality: a notional environment, within which electronic communication especially via the internet occurs.[35]

Cyberspace is considered to be a contemporary domain where war can be waged and carried out.[36]It can be used entirely during war or partially. Cyberwarfare has thus resulted in situations where physical means of perpetrating attacks can be done away with yet the same outcome reached. At times, the outcome can even be worse.

There is therefore a need to make the international community aware of the necessity of a global response to the urgent and increasing cyber threats that may be considered to constitute cyberwarfare.[37] The preambular declaration of the Charter of the United Nations (UN) provides that the peoples of the UN ought to unite in strength to maintain international peace and security.[38] The Charter of the UN is the founding treaty of the UN, an intergovernmental body that comprises 193 states and thus is easily the most influential intergovernmental body in the world. Given the context surrounding the drafting of the Charter of the UN, it is not far removed to infer that the UN was to be tasked with stepping in to maintain peace and security when a situation arises that necessitates it. It is with this premise that this dissertation seeks to undertake an inquiry as to: what constitutes cyberwarfare in international law; how may liability be attached when cyberwarfare is alleged; and who has jurisdiction to adjudicate over matters that arise as a result of cyberwarfare.

---

[34] United States Department of Defence, *'Cyberspace operations (JP 3-12)', Joint Publication 3-12*, 5 February 2013.
[35] Oxford Dictionaries, 'Cyberspace', https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/ on 6 January 2018.
[36] United States Department of Defense, *'Quadrennial Defense Review Report 37'*, 2010. *See also:* Geiss R, 'Cyber Warfare: Implications for Non- International Armed Conflicts' *International Law Studies, US Naval War College* 89, 627 (2013).
[37] http://www.nalsarpro.org/CL/Modules/Module4/Chapter-5.pdf on 29 December 2017.
[38] Preamble, *Charter of the UN*, 24 October 1945, 1 UNTS XVI.

Critical information infrastructures, both belonging to the government and private enterprises, have been targets of global cyber-attacks over the years.[39] It is rapidly being considered alarming when cyber-attacks are launched against sensitive national information infrastructure. This is becoming an international security threat. Such attacks potentially have an impact on international security, the global economy, and subsequently, the critical information infrastructures of all nations.[40] It is because of this that there is a need to look into cyberwarfare regulation generally at first- then in particular, with respect to liability and jurisdiction.

1.2 Background

Cyberspace is considered to be a contemporary domain that can be manipulated in various ways resulting in devastating outcomes. This was anticipated when it was first coined by William Gibson in 1982, in his infamous work, *'Burning Chrome'*. It was later launched into popular use in 1984 in his other work, *'Neuromancer'*.[41] With ARPANET (Advanced Research Projects Agency Network) adopting TCP/IP (Transmission Control Protocol/Internet Protocol) in January 1, 1983, which in turn resulted in the assembly of a 'network of networks' that later became known as the internet, communications and operations in cyberspace changed.[42] This dissertation posits that the susceptibility of cyberspace to attacks is not improbable. With the dawning of the cyber age, the former US Secretary of Defense, Leone Panetta, averred that, a perpetration in cyberspace by violent extremist groups or states could be as destructive as the terrorist attack on 9/11[43] .[44]

---

[39] http://www.nalsarpro.org/CL/Modules/Module4/Chapter-5.pdf on 29 December 2017.
[40] http://www.nalsarpro.org/CL/Modules/Module4/Chapter-5.pdf on 29 December 2017.
[41] Oxford Dictionaries, 'Cyberspace', https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/ on 6 January 2018.
[42] History, Andrew E, 'Who Invented the Internet', http://www.history.com/news/ask-history/who-invented-the-internet on 6 January 2017.
[43] On 11 September 2001, 19 militants associated with the Islamic extremist group Al-Qaeda hijacked four airliners and carried out suicide attacks against targets in the United States. Two of the planes were flown into the towers of the World Trade Center in New York City, a third plane hit the Pentagon just outside Washington, DC, and the fourth plane crashed in a field in Pennsylvania. Often referred to as 9/11, the attacks resulted in extensive death and destruction, triggering major U.S. initiatives to combat terrorism and defining the presidency of George W. Bush. Over 3,000 people were killed during the attacks in New York City and Washington, DC, including more than 400 police officers and fire fighters. *See also:* History, '9/11 Attacks', http://www.history.com/topics/9-11-attacks on 30 January 2017.
[44] Nato Review Magazine, 'The History of Cyber-attacks: A timeline', http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm on 30 January 2017.

Destructive cyber-attacks, although considered contemporary, have their roots embedded as early as 1988. In 1988, a worm created by Robert Morris, caused havoc never seen before.[45]The worm replicated itself using weakness present in the UNIX system Noun 1 and thus slowed down computers to the point where they were rendered unusable.[46]

Between 2001 and 2002, Gary McKinnon, a North London resident, infiltrated dozens of computers belonging to the US Department of Defense (DoD), the Air Force, the Navy and the Army and about sixteen National Aeronautics and Space Administration (NASA) computers in search of evidence that the US was supressing free energy and covering up unidentified flying object (UFO) activity and other technology that may be considered to be of use to the public. His activities resulted in damaged amounting to $800,000. His extradition from the United Kingdom (UK) failed but he was considered responsible for committing the biggest military computer hack ever seen.[47]

In 2007 during April and May, a series of cyber-attacks were perpetrated against Estonia resulting in the compromise of dozens of business enterprise and government sites. Estonia being considered one of the most wired states in Europe, was left devastated. The cyber-attacks, in the form of denial of service attacks (DoS) were attributed to Russia and it was put forward that in the coordinated attack that ensued, hundreds of thousands of computers were used.[48]

Around mid-2007, the unclassified email account belonging to the US Secretary of Defence's was compromised. It was alleged that this was perpetrated by foreign intruders whose identity remained unknown in order to obtain unauthorised access to the pentagon's network and exploit it as part of a large scheme of things. The Chinese military was suspected to have carried out the hack.[49] Although a military object was being carried out, how would one go

---

[45] Orman H, 'The Morris Worm: a fifteen-year perspective' 99 (5) *IEEE Security and Privacy* (2003).

[46] Nato Review Magazine, 'The History of Cyber-attacks: A timeline', http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm on 30 January 2017.

[47] ANONHQ.COM, Vandita, 'The Biggest Military Hack Ever Exposes NASA Secret 'UFO Files'' http://anonhq.com/biggest-military-hack-exposes-nasa-lie-ufos/ on 30 January 2017.

[48] NBC News.com, Security, 'A look at Estonia's Cyber Attack in 2007', http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WJm_J2997IU on 7 January 2017.

[49] Financial Times, Sevastopulo D, 'Chinese Hacked into Pentagon', https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac on 7 January 2017. *See also*: Fox News, 'Pentagon Source Says China Hacked

about this if the Chinese military and in turn its government decided to use the information attained for other purposes later on that might not constitute a military object? This is the information age. This means information means more to states than it did before. It may be posited that information is one of the most important assets owned by a state. This can be attached to the fact that states want a competitive edge when it comes to how they go about their business. It is therefore more important now more than ever to be able to attach liability for acts of both individuals and states, as well as have jurisdiction to bring actions against perpetrating individuals and states.

This was also brought out in the war that happened in South Ossetia War in 2008 between Russia and Georgia where there were cyber-attacks directed against Georgia before the Russia invasion happened.[50] In August 2008, foreign intruders of unknown identity compromised computer networks in Georgia around the time the state was at war with Russia.[51]It is becoming more important to identify perpetrators of these cyber-attacks so that individual liability can be attached to these individuals. If a state is behind such attacks as well, they ought to be considered liable as well.

In 2009 during the month of January, Israel's internet infrastructure was infiltrated by hackers during the military attack in the Gaza strip. The attack was executed by about five million computers and it targeted government websites. It was suspected by the Israeli officials that the cyber-attack was perpetrated in the Russia by a criminal organisation paid for by Hamas or Hezbollah.[52]

In 2010 during the month of October, suspicion arose that a cyber-weapon had been launched targeting the Iranian nuclear programme. It was a complicated malware modified to interfere

---

Defence Department Computers', http://www.foxnews.com/story/2007/09/04/pentagon-source-says-china-hacked-defense-department-computers.html on 8 January 2017.

[50] The New York Times, Technology, Markoff J, 'Before the Gunfire, Cyber Attacks', http://www.nytimes.com/2008/08/13/technology/13cyber.html on 7 January 2017.

[51] Hollis D, 'Cyber War Case Study: Georgia 2008' *Small Wars Journal (2011)*. *See also:* 'The Russo- Georgian War 2008: The Role of the Cyber Attacks in the Conflict', http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf on 7 January 2017.

[52] HAARETZ, Pfeffer A, 'Israel Suffered Massive Cyber Attack during Gaza Offensive', http://www.haaretz.com/israel-suffered-massive-cyber-attack-during-gaza-offensive-1.278094 on 8 January 2017.

with Siemens industrial control systems and it was called Stuxnet.[53] If a disaster did occur as a result of the malware, would this be classified as a 'cyber war crime'? And if so, to whom would liability be attached?

In 2011 during the month of January, a major cyber-attack came to light. It was brought to light by the Canadian government and it was alleged that it was to target Canadian agencies including Defence Research and Development Canada, the Canadian agency for its Department of National Defence.[54] The Treasury board and the Finance Department were made to disconnect from the internet. This was alarming considering these two are the main economic agencies in Canada and they were very dependent on the internet.[55] In such an instance, to whom would responsibility be attached?

In 2012 during the month of October, a cyber-attack in the form of a virus that had been operating since as early as 2007 was discovered by the Russian firm that goes by the name Kaspersky. This cyber hack was famously known as 'Red October'. Its perpetrators made use of the weaknesses in Microsoft's Word and Excel to collect information. It was aimed at: states in Eastern Europe, Central Asia, the former Union of Soviet Socialist Republics (USSR), Western Europe and North America. The virus collected information from government agencies and nuclear infrastructures of states.[56]

In mid-2014 in Iraq, it was alleged that cyberspace was being used as a domain for hostilities. Perpetrators of the cyber-attacks aspired to collect information, have malwares attack hostile computer networks in order to obtain control over such networks and in turn compromise

[53] BBC News, Technology, Fildes J, 'Stuxnet worm 'targeted high-value Iranian Assets', http://www.bbc.com/news/technology-11388018 on 8 January 2017. *See also:* PCWorld News, McMillan R, 'Was Stuxnet Built to Attack Iran's Nuclear Program?' http://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html on 8 January 2017.

[54] CBC News, Politics, Weston G, 'Foreign Hackers attack Canadian Government', http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618 on 8 January 2017.

[55] The New York Times, Austen I, 'Canada Hit by Cyber Attack', http://www.nytimes.com/2011/02/18/world/americas/18canada.html on 8 January 2017.

[56] BBC News, Technology, Lee D, ''Red October' Cyber Attack Found by Russian Researchers', http://www.bbc.com/news/technology-21013087 on 8 January 2017.

them. Emails were also booby trapped to spread misleading information. Social medial also came in handy when it came to spreading fear to targeted sections of the population.[57]

Cyber-attacks have had catastrophic effects no matter the context within which they have been employed. This being the case, there is a need to evaluate whether cyberwarfare regulation is adequately provided for under international law and what implications this will have with regard to questions of establishing both liability and jurisdiction.

1.3 Statement of the problem

There is no treaty of international law that forms the *lex specialis* that would regulate the conduct of hostilities in cyberspace. Furthermore, despite there not being positive law on the same, international customary law with regard to cyberwarfare regulation is underdeveloped thus there is no evidence of normative law that presents itself as state practice and *opinio juris*.[58]As it stands as well, there is no international law, either positive or normative, that provides for cyber-weapons that would provide guidance as to whether various forms of cyber-attacks are either banned or restricted in any way (this is without considering the fact that cyber weapons have not been adequately defined in international law, nor provided for).[59]This also leaves problems when it comes to addressing issues in the cyber context as is the case when it comes to defining a distinguishing act (between military objectives and civilian objectives). This obscures the interpretation of military conduct in cyberspace. With this obscurity comes problems when it comes to establishing both liability and jurisdiction.

Questions with regard to liability and jurisdiction in relation to cyberwarfare also go unanswered as there is no aspect of predictability when it comes to the legal framework that would guide the international community as to how they can act when troubled with incidences of cyberwarfare that threaten the peace fabric of the international community.

---

[57] BBC News, Technology, Ward M, *'Iraq Conflict Breeds Cyber-War among Rival Factions',* http://www.bbc.co.uk/news/technology-28418951 on 8 January 2017.

[58] Turns D, 'The First Case of Cyber war in Non- International Armed Conflict? The Matrix in Iraq', https://www.asil.org/insights/volume/19/issue/18/first-case-cyberwar-non-international-armed-conflict-matrix-iraq on 7 January 2017. *See also:* Kodar E, 'Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I', http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf on 8 January 2017.

[59] Kodar E, 'Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I'- <http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf> on 8 January 2017.

An analysis evaluating the legal framework regulating cyberwarfare in international law should therefore be undertaken. In doing so, it would be imperative to consider cyberwarfare regulation with particular interest in liability and jurisdiction.

1.4 Definition of terms

Given the technical aspects that may present themselves in this dissertation, it is prudent to kick of this dissertation with a definition of terms that will provide a better understanding as to the technical concepts that may come up.

Below are the definition of terms:

Attack	A situation that may arise where the integrity of a computer system is compromised or information is accessed that is considered unauthorised thus compromising the computer system.
Critical information infrastructure	Asset and service supportive information systems within the national infrastructure.
Cyber-attack	An attack perpetrated through cyberspace that targets information systems**.**
Cyber infrastructure	Constitutes: the people, the processes and the systems that interact through cyberspace.
DoS attack	A cyber-attack where the perpetrator seeks to render a network unavailable to its legitimate users thus making it useless.
Hack	Acting outside the creator's intention and making modifications and alterations to a computer software or hardware.
Hacker	Someone who perpetrates a hack.
Hacktivism	A hack perpetrated by a hacktivist.
Hacktivist	A person who perpetrates a hack to convey a political message.

Internet	Interconnected computer networks that constitute a worldwide system.
Lone wolf	An individual who perpetrates a cyber-attack outside any command structure.
Operating system	Software that provides a basis for a computer's programs enabling it to perform its basic functions.
Proxy	A person acting on behalf of someone else.
TCP/IP	A suite of communication protocols used to interconnect network devices on the internet.
UNIX System Noun 1	A type of a trademarked operating system.
Worm	A malicious software that self-replicates and distributes copies of itself onto a network causing damage that results in the network being considered inoperable.

1.5 Literature review

This dissertation seeks to make use of certain themes in conducting its literature review. The themes it seeks to cover are: the regulation of cyberwarfare in international law; cyberwarfare with respect to liability; and, cyberwarfare with respect to the establishment of jurisdiction.

1.5.1 The regulation of cyberwarfare in international law

In Robert Geiss' paper, '*Cyber Warfare: Implications for Non- International Armed Conflict'* it is posited that, cyber operations and infrastructure have at times been sought to further strategic aims by states and thus cyberspace is increasingly becoming relevant.[60]

In Jelena Pejic's paper, *'The Protective Scope of Common Article 3, more than meets the eye'*, it is contended that only certain acts in cyberspace may be considered to meet the threshold with regard to non-international armed conflicts (NIACs) as it is relatively high. This thus leaves only certain acts in cyberspace to be considered to be make the cut. Common Article 3 of the Geneva Conventions may therefore be inferred to be applicable when it comes

[60] Geiss R, 'Cyber Warfare: Implications for Non- International Armed Conflicts' *International Law Studies, U.S. Naval War College, 89,627 (2013).*

to cyberwarfare regulation but only is a cyber-attack results in a NIAC. This Article is therefore of fundamental importance in evaluating as to whether a cyber-attack may be classified as a NIAC.[61] Additional Protocol II to the Geneva Conventions adds on to what Common Article 3 provides for. The rules that provide for NIACs are however not as comprehensively provided for as those that provide for international armed conflicts (IACs).[62]

In Kelly A Gable paper, *'Cyber-Apocalypse Now: Securing the Internet Against Cyber terrorism and Using Universal Jurisdiction as a Deterrent',* it is brought out that when it comes to cyberspace, the economy and subsequently the financial markets of states are increasingly dependent on having a functioning, uncompromised cyber infrastructure as with its compromise comes devastating effects.[63]Oona A Hathaway and Rebecca Crootof, writing on *'The Law of Cyber-Attack'* further opine that nuclear infrastructure, air defence systems and also electrical grids may be compromised by cyber-attacks. This poses a serious threat to national security.[64]

With the above being considered, inadequate regulation with regard to cyberwarfare would leave key sectors of states that now carry out operations online vulnerable and thus prone to attack due to the inadequately regulated sphere of cyberwarfare.

1.5.2 Cyberwarfare with respect to liability

1.5.2.1 Individual liability

States by themselves do not commit war crimes, it is individuals that do so. It would therefore be prudent to consider liability with respect to the individual first, thereafter with respect to the state. It is because an individual can be identified as having violated the laws of war, that a state may be questioned as to its liability in the conduct of the individual.

---

[61] Pejic J, 'The Protective Scope of Common Article 3, more than meets the eye', *International Review of the Red Cross, 93, 881, (2011). See also*: International Committee of the Red Cross, Customary International Humanitarian Law, 'Introduction, Purpose of the Study', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_in_puofthst on 7 February 2017.

[62] International Committee of the Red Cross, Customary International Law, 'Introduction, Purpose of the Study', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_in_puofthst on 7th February 2017.

[63] Gable K A, 'Cyber-Apocalypse Now: Securing the Internet against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent 43' *Vanderbilt Journal of Transnational Law 59 (2010).*

[64] Hathaway O A, Crootof R, 'The Law of Cyber- Attack' *Yale Law School Legal Scholarship Repository (2012).*

In Elies van Sliedregt paper, *'Command Responsibility and Cyberattacks'*[65], it is posited that cyber-attacks may be attributed to military commanders under whose command the said cyber-attacks have been perpetrated. In making his assertion, Sliedregt acknowledges that although the law on command responsibility has seen some significant developments in the early case law of the ICTY, its application and practical effect has been quite limited.[66] He further provides that prosecutors have at times decided to charge under other theories of liability, such as aiding and abetting and even Joint Criminal Enterprise (JCE) because of the convenience in doing so. When it comes to convicting perpetrators under these liability theories, it is considered less difficult compared to having one secured under the command responsibility theory. Over the years however, and with developing case law in the ICC such as the ruling in *Bemba*[67], it can be regarded that steps are being made to expand the reach of the command responsibility theory. Command responsibility is said to be triggered when: there is an integration of cyber units into the army and are these cyber units are considered to be part of regular operations; there is outsourcing of cyber operations (even in instances where the hackers remain anonymous); and, where there is proof of a link between a the anonymous hackers and the commander's subordinates (it is a matter of fact that, with no such link, there can be no command responsibility).[68] This problematic nature of establishing criminal liability when it comes to the command responsibility is also brought out by Kai Ambos in his paper, *'Individual Criminal Liability for Cyber Aggression',* where he puts forward that it has been very difficult to assert criminal responsibility under the command responsibility theory due to the complexity that cyberspace presents.[69]

There is therefore a lot to consider when it comes to individual liability. This is also not limited to combatant and military superiors, 'lone wolves' may also be considered when they carry out acts by themselves. It is also important to consider individual liability because this is key in bringing about justice in NIACs where two states may not be in conflict thus state liability cannot be invoked.

---

[65] Sliedregt E, 'Command Responsibility and Cyberattacks' *Journal of Conflict and Security Law (2016).*
[66] Sliedregt E, 'Command Responsibility and Cyberattacks' *Journal of Conflict and Security Law (2016).*
[67] *Prosecutor v Jean-Pierre Bemba Gombo (Trial Judgment),* ICC-01/05-01/08, 21 March 2016.
[68] Sliedregt E, 'Command Responsibility and Cyberattacks' *Journal of Conflict and Security Law (2016).*
[69] Kai A, 'Individual Criminal Responsibility for Cyber Aggression' *Journal of Conflict and Security Law (2016).*

1.5.2.2 State liability

There is a known prohibition in international law that states ought not to resort to armed force. This is contained in Article 2(4) of the Charter of the UN. In addition to this provision, Article 2(7) of the Charter of the UN also provides for the principle of non-intervention which may be inferred to mean that states ought not in any way interfere with the internal affairs of another state: use of force would result in that. This is buttressed by the holding of the International Court of Justice (ICJ), when it stated that in an instance where interference presents itself in the form of a use or a threat of the use of force, the intervention is considered to be in contravention of Article 2(4).[70] Despite this position however, there are exceptional circumstances when the use of armed force may indeed be permitted.[71] This dissertation considers whether a cyber-attack may qualify as an armed attack against another state. But even if this were the case, would another state be justified to act through the use of its physical capabilities if the first blow was ensued in the cyber domain? These are the complicated questions that come up because when considering international customary law, these are not matters that have often come up.

Given the nature of cyber-attacks, it is necessary to re-evaluate the scope of Article 2(4). Stronger states may develop a bias towards having a broadened interpretation of Article 2(4) as this stands to benefit them. The broadened interpretation would interpret Article 2(4) as prohibiting activities that are considered coercive such as cyber-attacks. Despite the ambiguity that has come to be as a result of cyberwarfare, there is however a consensus that Article 2(4) prohibits expressly physical armed force.

In Dana Rubenstein's paper, *'Nation State Espionage and its Impacts'*[72], it is posited that states when launching cyber-attacks seek to disguise their source. This is done through technical means at the disposal of the said state. This therefore makes it all the more difficult if such an occurrence takes place between states that do not have matched cyber capabilities.

[70] *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v US) (1986), ICJ, 14, para 209.
[71] Article 51, *Charter of the UN.*
[72] Rubenstein D, 'Nation State Espionage and its Impacts', http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/ on 22 November 2017.

This view was also brought out in David Turns' paper, *'Cyber Warfare and the Notion of Direct Participation in Hostilities'*[73].

The prohibition of the use of force as provided for under Article 2(4) of the Charter of the UN is subject to two exceptions: the use of force is permissible if it is undertaken as part of collective security operations or as self-defence.[74] The first exception is provided for under Article 39 of the Charter of the UN , where it is provided that the Security Council may determine the existence of any threat to the peace, breach of the peace, or act of aggression, and make recommendations, or decide what measures shall be taken to maintain or restore international peace and security.[75] Reading this together with Article 41 and 42, the Security Council is given leeway to employ other means that may not involve the use of force, unless the use of force becomes inevitable.[76] Collective security operations however can be politically difficult because they require authorisation by the often deadlocked and slow-moving Security Council thus making measures ineffective is they cannot be carried out when there is a need to do so. Moreover, lawful collective security operations are easily identifiable and relatively uncontroversial. This would therefore pose some difficulty if the matter that falls before the Security Council is a cyber-attack as it not clear as to what ought to inform the Security Council to act. The second exception to Article 2(4) is provided for in Article 51 where it provides that nothing in the Charter of the UN ought to impair the inherent right of individual or collective self-defence if an armed attack occurs.[77] This however brings about the problem as to what would constitute a lawful self-defense in the instance of a cyber-attack. However, the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. Many agree that a cyber-attack may rise to the level of an armed attack.[78]

The ICJ has provides that cross-border incursions that are minor in scale and with minimal effect ought to be classified as mere incidents at the frontier rather than being classified as

[73] Turns D, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' *Journal of Conflict and Security Law*, *Volume 17, Issue 2, 1, 279-297 (2012).*
[74] Article 2(4), *Charter of the UN.*
[75] Article 39, *Charter of the UN.*
[76] Article 41 and 42, *Charter of the UN.*
[77] Article 51, *Charter of the UN.*
[78] https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace on 21 August 2017.

armed attacks.[79]It has gone further to provide that armed attacks must be of sufficient gravity to constitute the 'gravest forms of the use of force'.[80]This does not mean that states are forbidden from responding to low-level violations of their sovereignty. Even without the go ahead to resort to defensive force, states may engage in retorsions or non-forceful countermeasures.[81]

In the instance where cyber-attacks do not qualify as armed attacks that warrant self-defense, a state may make use of countermeasures to respond to cyber-attacks (this is provided they do not constitute a use of force in violation of international law and that the need to induce a return to compliance with international law is still possible).[82] It is therefore worth noting from this point that not every cyber-attack constitutes an armed attack. A *jus ad bellum* analysis will be relevant for regulating the use of or response to cyber-attacks by states.

1.5.3 Cyberwarfare with respect to establishment of jurisdiction

IHL is considered the specific body of international law to address cyber-attacks. This being the case, IHL can only be invoked in an instance where the cyber-attack amounts to an armed attack. Trying to establish whether a cyber-attack amounts to an armed attack is difficult as there is no set standard as to what the threshold may be for a cyber-attack to be considered an armed attack. This is inevitably bound to bring about jurisdiction issues.

In order to address this issue of jurisdiction, Oona A Hathaway and other scholars writing on, *'Cyberwarfare and International Law'*, opine that states should extend their extraterritorial reach when it comes to combating cyber-attacks. This could play a vital role in increasing the ability of states to take action against those who initiate cyber-attacks against the said state.[83]Given the transboundary, non-conforming nature of cyber-attacks, this would go a long way. The law should however not overlap other provisions that are provided under domestic and international law, rather, it should only seek to address lacunas in the

[79] *Military and Paramilitary Activities in and Against Nicaragua*, para 195.
[80] *Military and Paramilitary Activities in and Against Nicaragua*, para 191.
[81] Retorsions are lawful unfriendly acts made in response to an international law violation by another state; countermeasures are acts that would be unlawful if not done in response to a prior international law violation. *See*: *Draft articles on state responsibility for internationally wrongful acts*, ILC 53rd Report, 2001, UN Doc A/56/10.
[82] United States Department of Defence, Office of the General Counsel, '*An Assessment of International Legal Issues in Information Operations'*, November 1999.
[83] Hathaway O A *et al*, 'Cyberwarfare and International Law'.

law. An extraterritorial reach is a good place to start but it too is faced with its challenges. How can cooperation be brought about to ensure that different states extradite these cybercriminals? What about situations where a state is considered to be at fault?

According to the Department of Defence of the US, cyberspace is a network of networks that includes thousands of internet service providers across the globe. Based off this premise, in ensuring effective cyber defense, no single state is considered capable on its own.[84] This being the case, it can be inferred that a treaty with binding obligations would be able to accomplish what individual state cannot do on their own. This will also bring about cooperation between states.

As part of its mandate under Article 39 of the UN Charter, the Security Council, having established that there is an international threat to peace in the form of unprecedented cyber-attacks, can establish an 'International Tribunal for Cyberwarfare'. This will encompass the adjudication of matters that pertain to both cyberwarfare and cyber-attacks which are yet to reach this magnitude but still pose a threat to peace.

It is important that jurisdiction is established in order to enable cyberwarfare regulation.

1.6 Theoretical framework

This dissertation is guided by Emile Durkheim's theory of unity of a perpetrator's online presence and his physical self. This is contrasted with the theories of John Rawls and Immanuel Kant that posit that there is a duality when it comes to a perpetrator's online presence and his physical self. This dissertation shall take the perpetrator to mean either the individual or the state.

Ari Ezra Waldman, writing on, *'Durkheim's Internet: Social and Political Theory in Online Society'* posits that it is false to imagine the online works as being free and anonymous. According to him, our online selves may be considered traceable and increasingly identifiable as being extensions of our physical selves.[85] In the view of Waldman, having the internet perceived as somehow different, separate, apart, ephemeral, or just plain fake has encouraged

[84] United States Department of Defence, *'Department of Defence Strategy for Operating in Cyberspace*, July 2011.
[85] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society' *New York University Journal of Law & Liberty (2013)*, 358.

us to devalue the effect of online actions. This is in line with Emile Durkheim's theory of the individual online.[86] Considering that this dissertation approaches liability as pertaining to both the individual and the state, it may be inferred from Emile Durkheim's theory that both the individual and the state's presence is increasingly identifiable as an extension of physical realities.

In contrast to this theory is the theory posited by John Rawls, the *'ideal self'* as an extension of Immanuel Kant's construct of *'separate worlds'*.[87] According to Rawls, a person acting online in an anonymous capacity is to be considered by everyone else as being behind the 'veil of ignorance' and thus an autonomous agent of choice, not weighed down by prejudice, limitations, and other encumbrances.[88] Kant additionally provides that, in the real world, people are not considered free- only when they step away into a purely intelligible world such as cyberspace can they be free. According to him, freedom derives from stepping outside the physical world, breaking loose from the constraints imposed by one's body, needs, and entering a world governed by pure reason, where a person can decide what they want on their own terms.[89] The virtual world according to Rawls and Kant is therefore what he calls 'a bastion of freedom'.[90] It is against such a belief that ideas as to the lawlessness of cyberspace have come to be, having restrictions of the physical world rendered meaningless. Considering that the subject of this dissertation is both the individual and the state, John Rawls' and Immanuel Kant's theories may be deduced to mean that there is either a duality between an individual's online self and their physical self or with regard to a state, a duality between a state's online presence and its physical reality.

This dissertation seeks to contend that Durkheim's view is applicable when trying to establish liability, both individual and state. Durkheim adamantly asserts that the online presence is an extension of physical reality. Individual liability can therefore be attached to an individual despite his actions having been committed in cyberspace. This too can be said about the state. This is enlightening in a world where individuals and states perceive themselves in a dual sense, and at times even view their virtual reality as being even more real than what happens

[86] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society', 358.
[87] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society', 371.
[88] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society', 372.
[89] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society', 371.
[90] Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society', 373.

in the physical dimension. This shall be contrasted with Rawls' and Kant's view that brings about a duality.

1.7 Research objectives

The main objective of this dissertation was to investigate whether cyberwarfare is adequately regulated in international law.

The specific objectives of this dissertation were:

(a) To investigate how the aforementioned legal framework regulating cyberwarfare provides for cyberwarfare in terms of addressing the issue of liability
(b) To investigate how the aforementioned legal framework regulating cyberwarfare addresses the issue of jurisdiction.

1.8 Research questions

(a) What is the legal framework regulating cyberwarfare in international law?
(b) How does the legal framework regulating cyberwarfare provide for cyberwarfare in terms of addressing the issue of liability?
(c) How does the legal framework regulating cyberwarfare address the issue of jurisdiction?

1.9 Justification and scope of the study

It was been expressed by the ICRC that when it comes to means and methods of warfare, despite cyber technology having not being provided for expressly in IHL, weapons of these nature through *lex generalis* are subject to IHL in the same way any weapon or strategy is. However, this view does not represent a settled view on the international platform.[91]

The existing body of IHL applies in the same manner when it comes to cyberspace as it would with regard to armed conflict in the classical sense. However, since no law can be said to be the primary source of law when it comes to cyberwarfare specifically, commentaries made by scholars have been of great assistance in establishing how IHL is to apply to hostilities in

[91] International Committee of the Red Cross, International Conference of the Red Cross and Red Crescent, *'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', 31, 36–38,* November 28–December 1, 2011.

the cyber domain.[92] Also, with the publication of the two Tallinn Manuals[93], there is a general development in the form of 'soft law' with regard to what constitutes war in cyberspace and how IHL ought to apply. But nevertheless, there is uncertainty with regards to the application of IHL when it comes to hostilities conducted in the cyber context. Cyberwarfare shall however be examined in relation to the above and in doing so NIACs and IACs shall both be considered within the context of acts perpetrated through cyberspace.

When international law fails to provide solutions that are to be considered binding when disputes arise and domestic sanctions are considered ineffective as to warrant domestic jurisdiction, it has been commonplace to have states act on the justification that a matter in one of international concern. Cyberwarfare is such a matter.[94] A matter becomes one of international concern when it meets one of two criteria: there is a present threat to the peace; or, there is a potential threat to the peace. This shall also be evaluated in this dissertation.

1.10 Hypothesis

There is a need to ameliorate the legal framework that regulates cyberwarfare as it is inadequately provided for, thus posing challenges when it comes to attaching liability or asserting jurisdiction.

1.11 Assumptions

(a) The legal framework regulating cyberwarfare is inadequate as it does not provide for the *sui generis* nature of cyberwarfare;

(b) When it comes to the legal framework regulating cyberwarfare, it is not clear as to what the definition of cyberwarfare is, this bringing problems as to establishing liability; and

(c) Flowing from the same vein as the above assumption, there is also a problem when it comes to establishing jurisdiction.

---

[92] Schmitt M N, *'Wired warfare: Computer Network Attack and Jus in Bello' International Review of the Red Cross 84, 365 (2002).*

[93] 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).

[94] Howell JM, 'A Matter of International Concern' *The American Journal of International Law, Volume 63, 4 (1969).*

1.12 Research design and methodology

This dissertation approached the subject matter through a qualitative research. In doing so, it made use of secondary sources of literature such as books and journal articles by renowned authors on: the legal framework regulating cyberwarfare in international law; and in relation to this, the issues that arise when it comes to liability and establishing jurisdiction.

Given the technical dimension of cyberspace and to better understand the unique nature of cyberwarfare, books and journal articles pertaining to cyberspace came in handy. Case law was key in carrying out comparative evaluations of pertinent issues that this dissertation sought to tackle. Internet sources were also be used.

1.13 Limitations of the study

The limitations of this dissertation are therefore the following: gathering information from primary sources proved near impossible due to the sensitive nature of information pertaining to cyberwarfare that is yet to be out in the public yet; and also, given the technical dimension that cyberspace presents, this dissertation sought to focus mainly on the legal aspects and very little of the technical matters at play (and in doing so, with simplicity).

This dissertation did not involve field activities for example, collection of data. This is due to the nature of the area of research of this dissertation and the fact that warfare entails sensitive information that is never disclosed as it is confidentially held by the involved stakeholders.

1.14 Outline of the dissertation and its flow

This dissertation is centered around cyberwarfare with a specific focus on liability and jurisdiction. In order to understand what cyberwarfare entails in international law, it will be prudent to first analyse how different laws provide for cyberwarfare without expressly providing for it as there is no international law that expressly binds states when it comes to the cyberwarfare, either positively or normatively. Thereafter, this dissertation shall address the issue of liability as without establishing liability, there is no reason to have a cause of action in the first place. Exceptions when it comes to liability shall also be raised so as to fully appreciate liability. It is also worth noting that the occurrence of an act is a matter of fact, but liability is a creature of the law. Thereafter, this dissertation shall delve into jurisdiction. This is because, as international law is as of now, there is no certainty as to

which forum has jurisdiction when it comes to cyberwarfare. This problem is magnified because both individuals and states participate in cyberwarfare. This dissertation is incomplete without a recommendations and a conclusion. Recommendations provide viable solutions that may be sought to remedy the 'chaos' that is when we address cyberwarfare with particular focus on liability and jurisdiction. The conclusion brings about an end to this dissertation.

1.15 Summary of overall results and conclusions

Subject to the methodology used, as well as the limitations posed, this dissertation was able to analyse cyberwarfare with respect to liability and jurisdiction. In doing so, some matters that arose were disproved, whereas others were affirmed. It was hypothetically posited that there is a need to ameliorate the legal framework that regulates cyberwarfare as it is inadequately provided for, thus posing challenges when it comes to attaching liability or asserting jurisdiction. In chapter 2 of the dissertation, various international laws were put to test to see how they provide for cyberwarfare. 'International' is used very loosely as regional laws were also analysed to provide a wholesome view on the matter. The laws however informative, did not expressly provide for cyberwarfare. The Tallinn manual, also analysed, came close, but without binding force, it leaves cyberwarfare in limbo. There is a need to ameliorate the legal framework regulating cyberwarfare. Chapter 3 of this dissertation analysed liability with regard to cyberwarfare in detail. Different players in cyberwarfare were considered and how liability may be attached to them was also looked into. Individuals and states were both the subject of this dissertation's analysis. What came to light is that there are legal regimes in international law that can result in the establishment of liability. This may prove satisfactory but this dissertation posits that a lot can be done to demystify liability further by having an international law that is express when it comes to this. This conclusion was also reached when analysing jurisdiction in chapter 4. Chapter 5 provides recommendations based on the results obtained. In conclusion, a lot needs to be done when it comes to cyberwarfare regulation with respect to liability and jurisdiction. The recommendations put forward may lay the foundation to these solutions.

1.16 Chapter breakdown

1.16.1 Chapter 1

This chapter provides the introduction and background to this dissertation, the problem this dissertation seeks to solve, the justification and the intended scope of this dissertation, the hypothesis of this dissertation, the assumptions to be made when carrying out research, the research objectives, the research questions, the theoretical framework, the literature review, and the limitations of this dissertation.

1.16.2 Chapter 2

This chapter provides a breakdown of the existing legal framework regulating cyberwarfare as is provided in international law and how this legal framework provides for the *sui generis* aspects that come with cyberspace.

1.16.3 Chapter 3

This chapter looks into how cyberwarfare is provided for within the context of the existing legal framework with the aim of addressing the issue of liability.

1.16.4 Chapter 4

This chapter looks into the issue of establishing jurisdiction within the context of the existing legal framework regulating cyberwarfare.

1.16.5 Chapter 5

This chapter provides recommendations made in response to the issues tackled by the dissertation as well as provides a conclusion to the dissertation.

CHAPTER 2

The legal framework regulating cyberwarfare in international Law

2.1 Introduction

This chapter seeks to answer the first research question as espoused upon in Chapter 1 and shed light to the truth or fallaciousness of the hypothesis made to the extent where it was hypothetically provided that there is a need to ameliorate the regulatory framework that deals with cyberwarfare as it is inadequately provided for. With regard to the legal framework regulating cyberwarfare in international law, laws regulating the state and the individual shall both be looked into.

This chapter therefore looks into: cyber-attacks and *jus ad bellum*; cyber-attacks and *jus in bello*; cyber-attacks and the Statute of the ICC; cyber-attacks and the customary international law of countermeasures and in particular, what the Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARISWA) provides on the matter; the UN and its take on regulating cyberspace; NATO and its take on regulating cyberspace; the Council of Europe and its take on regulating cyberspace; the Organisation of American States (OAS) and its take on regulating cyberspace; the Shanghai Cooperation Organisation (SCO) and its take on regulating cyberspace; and finally, the Tallinn Manuals and what they have to say about regulating cyberspace.

2.2 Cyber-attacks and *jus ad bellum*

There is a known prohibition in international law that states ought not to resort to armed force. This is contained in Article 2(4) of the Charter of the UN. In addition to this provision, Article 2(7) of the Charter of the UN also provides for the principle of non-intervention which may be inferred to mean that states ought not in any way interfere with the internal affairs of another state: use of force would result in that. This is buttressed by the holding of the International Court of Justice (ICJ), when it stated that in an instance where interference presents itself in the form of a use or a threat of the use of force, the intervention is considered to be in contravention of Article 2(4).[95] Despite this position however, there are exceptional circumstances when the use of armed force may indeed be permitted.[96] This dissertation

[95] *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v US) (1986), ICJ, 14, para 209.
[96] Article 51, *Charter of the UN.*

considers whether a cyber-attack may qualify as an armed attack against another state. But even if this were the case, would another state be justified to act through the use of its physical capabilities if the first blow was ensued in the cyber domain? These are the complicated questions that come up because when considering international customary law, these are not matters that have often come up.

Given the nature of cyber-attacks, it is necessary to re-evaluate the scope of Article 2(4). Stronger states may develop a bias towards having a broadened interpretation of Article 2(4) as this stands to benefit them. The broadened interpretation would interpret Article 2(4) as prohibiting activities that are considered coercive such as cyber-attacks. Despite the ambiguity that has come to be as a result of cyberwarfare, there is however a consensus that Article 2(4) prohibits expressly physical armed force.

In Dana Rubenstein's paper, *'Nation State Espionage and its Impacts'*[97], it is posited that states when launching cyber-attacks seek to disguise their source. This is done through technical means at the disposal of the said state. This therefore makes it all the more difficult if such an occurrence takes place between states that do not have matched cyber capabilities. This view was also brought out in David Turns' paper, *'Cyber Warfare and the Notion of Direct Participation in Hostilities'*[98].

The prohibition of the use of force as provided for under Article 2(4) of the Charter of the UN is subject to two exceptions: the use of force is permissible if it is undertaken as part of collective security operations or as self-defence.[99] The first exception is provided for under Article 39 of the Charter of the UN , where it is provided that the Security Council may determine the existence of any threat to the peace, breach of the peace, or act of aggression, and make recommendations, or decide what measures shall be taken to maintain or restore international peace and security.[100] Reading this together with Article 41 and 42, the Security Council is given leeway to employ other means that may not involve the use of force, unless

[97] Rubenstein D, 'Nation State Espionage and its Impacts', http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/ on 22 November 2017.
[98] Turns D, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' *Journal of Conflict and Security Law*, *Volume 17, Issue 2, 1, 279-297 (2012).*
[99] Article 2(4), *Charter of the UN.*
[100] Article 39, *Charter of the UN.*

the use of force becomes inevitable.[101] Collective security operations however can be politically difficult because they require authorisation by the often deadlocked and slow-moving Security Council thus making measures ineffective is they cannot be carried out when there is a need to do so. Moreover, lawful collective security operations are easily identifiable and relatively controversial. This would therefore pose some difficulty if the matter that falls before the Security Council is a cyber-attack as it not clear as to what ought to inform the Security Council to act. The second exception to Article 2(4) is provided for in Article 51 where it provides that nothing in the Charter of the UN ought to impair the inherent right of individual or collective self-defence if an armed attack occurs.[102] This however brings about the problem as to what would constitute a lawful self-defense in the instance of a cyber-attack. However, the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. Many agree that a cyber-attack may rise to the level of an armed attack.[103]

The ICJ has provides that cross-border incursions that are minor in scale and with minimal effect ought to be classified as mere incidents at the frontier rather than being classified as armed attacks.[104]It has gone further to provide that armed attacks must be of sufficient gravity to constitute the 'gravest forms of the use of force'.[105]This does not mean that states are forbidden from responding to low-level violations of their sovereignty. Even without the go ahead to resort to defensive force, states may engage in retorsions or non-forceful countermeasures.[106]

In the instance where cyber-attacks do not qualify as armed attacks that warrant self-defense, a state may make use of countermeasures to respond to cyber-attacks (this is provided they do not constitute a use of force in violation of international law and that the need to induce a

[101] Article 41 and 42, *Charter of the UN.*
[102] Article 51, *Charter of the UN.*
[103] https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace on 21 August 2017.
[104] *Military and Paramilitary Activities in and Against Nicaragua*, para 195.
[105] *Military and Paramilitary Activities in and Against Nicaragua*, para 191.
[106] Retorsions are lawful unfriendly acts made in response to an international law violation by another state; countermeasures are acts that would be unlawful if not done in response to a prior international law violation. *See*: *Draft articles on state responsibility for internationally wrongful acts*, ILC 53rd Report, 2001, UN Doc A/56/10.

return to compliance with international law is still possible).[107] It is therefore worth noting from this point that not every cyber-attack constitutes an armed attack.

A *jus ad bellum* analysis will be relevant for regulating the use of or response to only cyber-attacks addressed by Security Council resolutions and which meet the standard for an armed attack giving rise to a right of self-defence.

2.3 *Jus in bello* and its respective principles vis-à-vis cyber-attacks

To date, there is yet to be a cyber-attack that has resulted in an armed conflict. Cyber-attacks have however been employed to respond to what is considered 'traditional provocations' (this is when traditional triggers to war are employed and thus result in war). It is therefore paramount to pointy out the relationship and similarities between what is considered traditional *jus in bello* and cyber-attacks as may be employed in armed conflicts. The novel conditions of cyber-warfare pose 'never seen before' challenges to applying *jus in bello* principles such as proportionality, distinction, and neutrality. Because cyber-attacks are often not immediately lethal or destructive and may cause only temporary incapacity of network systems or have its effects felt later on, it may be hard to evaluate whether a cyber-attack is proportional in the traditional sense.[108] It can also be near impossible to distinguish between combatants, civilians directly participating in hostilities, civilians engaged in a continuous combat function, and protected civilians in the context of cyber-attacks. Finally, the ease of masking the source of a cyber-attack makes enforcement of neutrality duties complicated and expensive.[109] It is for this very reason that cyber-attacks pose a problem to *jus in bello* in general.

The *in bello* proportionality requirement prohibits attacks that may by excessive when compared to the expected military advantage thus resulting in unwarranted incidental loss of civilian life, injury to civilians, damage to civilian objects, or at times a combination of the aforementioned. In conducting a proportionality assessment, one must estimate potential civilian casualties and destruction of their property and weigh this against the benefit of

[107] United States Department of Defence, Office of the General Counsel, '*An Assessment of International Legal Issues in Information Operations'*, November 1999.
[108] Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*
[109] Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*

achieving a military objective.[110] This might however not be possible as the nature of harm that cyber-attacks inflict, proportionality with respect to cyber-attacks poses unique challenges. It is difficult to evaluate whether an attack would be proportional as the usual and anticipated direct effects of cyber-attacks may be non-lethal or temporary, yet severe.[111] Furthermore, how should the temporary incapacity of critical systems be evaluated?[112]

The distinction requirement presents another large challenge in evaluating the *in bello* lawfulness of a cyber-attack.[113] This principle requires distinguishing between civilian and military persons and limiting attacks to military objectives.[114] Additionally, military commanders must employ weapons that may be targeted accurately and must use this capability to distinguish between civilian and military objectives.[115] By extension, the law of war prohibits *in bello* cyber-attacks that are uncontrollable, unpredictable, or do not discriminate between civilian and military objectives as it usually near impossible when it comes to cyber-attacks. Furthermore, Additional Protocol I prohibits attacks that deny the civilian population indispensable objects, such as food or water supplies.[116]

At times, it is also difficult to carry out an evaluation as to whether civilian involvement in a cyber-attack violates the law of war by encouraging the use of force by non-combatants as well.[117]

2.4 Cyber-attacks and the Statute of the ICC

With the adoption of the Statute of the ICC (Rome Statute) on 17 July 1998, the ICC was established.[118] This is considered the first time in history where states decided to accept the

---

[110] Articles 51(5) (b), 54, 57(2) (a) (iii)*, 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; Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*

[111] Art. 57(2) (a) (iii), *Additional Protocol I*.

[112] Fry J D, 'Gas smalls awful: UN forces, riot-control agents, and the chemical weapons convention' *Michigan journal of international law 475 (2010)*; Sossai M, 'Drugs as Weapons: Disarmament Treaties Facing the Advances in Biochemistry and Non-Lethal Weapons Technology' *Journal of Conflict and Security Law 5, 1 (2010).*

[113] Delibasis D, 'The Right to National Self-Defense in Information Warfare Operations' 268 (2007), 274.

[114] Doswald-Beck L, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' *Computer Network Attack and International Law, 163, 166 (2002).*

[115] Kanuck S P, 'Recent Development, Information Warfare: New Challenges for Public International Law', *Harvard International Law Journal, 37, 272, 282 (1996).*

[116] Article 54(2), *Additional Protocol I*.

[117] Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*

[118]'Understanding the International Criminal Court', https://www.icccpi.int/iccdocs/pids/publications/uicceng.pdf on 29 January 2018.

jurisdiction of a permanent international court to prosecute crimes that were considered to 'shock the conscience of humanity'.[119] It entered into force on 1 July 2002. Despite the fact that the ICC has jurisdiction over member states pursuant to Article 12(1), this does not mean that the court is a substitute of national courts[120]. The ICC can only intervene where a state is unable or unwilling genuinely to carry out the investigation and prosecute the perpetrators.[121]

With regard to cyberwarfare, Article 5 and Article 8 of the Statute of the ICC would be particularly relevant. Article 5 provides that war crimes shall fall under the jurisdiction of the court with Article 8 specifically providing for war crimes. Article 8(2) (a) provides that grave breaches to the Geneva Conventions of 12 August 1949 constitute war crimes. In this particular Sub-Article, extensive destruction not justified by military necessity stands out as this would particularly be relevant when addressing cyber-attacks.[122]When would a cyber-attack be considered to cause extensive destruction? The Elements of Crimes to the Statute of the ICC does not shed light into this as it only provides that the context of the crime ought to be an IAC.[123] Article 8(2) (b) (i) to (iv) may also be deemed relevant with regard to international customary law as they provide for the principle of distinction in IHL which is a contested matter when it comes to cyber-attacks as there have been questions as to whether attacks perpetrated through cyberspace are capable of discriminating between civilian objects and military objects.[124]Article 8(e) (i) and (ii) also provide for the principle of distinction when it comes to NIACs.[125]

2.5 Cyber-attacks and the customary international law of countermeasures

For international law violations that do not meet the threshold of an armed attack, the customary international law of countermeasures applies, and thus, cyber-attacks may be inferred to fall under this category thus subject to it. Countermeasures, as is provided in ARISWA are the measures that would otherwise be considered to be violations of

[119] Preamble, *Statute of the ICC.*
[120] Article 17 and 53, *Statute of the ICC;* Rule 48, *Rules of Procedure and Evidence to the Statute of the ICC.*
[121] Article 17(1), *Statute of the ICC.*
[122] Article 8(2) (a) (iv), *Statute of the ICC.*
[123] Article 8(2) (a) (iv), Element 6, *Elements of Crimes to the Statute of the ICC.*
[124] Article 8(2) (b) (i) - (iv), *Statute of the ICC.*
[125] Article 8(2) (e) (i) and (ii), *Statute of the ICC.*

international law but are not because a state has been injured and are thus expected to retaliate to bring about an end to the injury and to guarantee reparation.[126]

There is however ambiguity as the international law of countermeasures does not define when a cyber-attack may be considered unlawful, rather, it provides that when a state commits an international law violation, an injured state may respond with a reciprocal act.[127] It therefore stands to question as to whether this refers to a similar nature of attack, thus: a cyber-attack is only justified if it is in response to a corresponding cyber-attack. Despite the fact that cyber-attacks may not be considered as having attained the threshold to be considered armed attacks, these attacks do violate the customary international law principle of non-intervention and the injured state may therefore use countermeasures to bring the responsible state into compliance with the law as laid down in ARISWA. However, countermeasures cannot be justified in a situation where the international law violation that resulted in the countermeasure has ceased. It is important to note that human rights violations, humanitarian prohibitions on reprisals, or acts contrary to *jus cogens* as well cannot be justified as a countermeasure.[128]

In the context of cyberspace, a state perpetrating a cyber-attack may violate its obligation not to intervene in another sovereign state through the perpetration, and so the state that has been attacked may make use of lawful countermeasures. When a state is considering countermeasures, the most indispensable countermeasures in this context are so-called 'active defenses', which are made use of to disable the source of an attack (they however require the state in question to have the capability to do so); 'passive defenses', on the other hand, such as firewalls, merely attempt to keep cyber-attacks at bay.[129] States are however plagued with the difficulty of identifying the state responsible for a cyber-attack. The customary law of countermeasures therefore only offers a partial answer to the problem of cyber-attacks.

---

[126] ILC, *Draft articles on state responsibility for internationally wrongful acts*, 31, 80.
[127] Article 49, para 3, ILC, *Draft articles on state responsibility for internationally wrongful acts*; Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*
[128] Gervais M, 'Cyber Attacks and the Laws of War' *Berkeley Journal of International Law 525 (2012).*
[129] United States Department of Defence, *'Department of Defence Strategy for Operating in Cyberspace*, July 2011.

2.6 The UN's regulation of cyberspace

The UN General Assembly has passed a few resolutions that relate to the regulation of cyberspace.[130] These resolutions however may be opined to be vague and also do not require any specific action by UN members thus ineffective when it comes to dealing with cyber-attacks.[131]In 1999 during the month of August, a meeting of cyber-experts was held in Geneva (sponsored by the UN) to better understand emerging information technologies. A resolution soon followed when the General Assembly passed a resolution it 2002 encouraging there to be further discussions around information security.[132] There was also a World Summit (also sponsored by the UN) that encouraged the further consideration of issues pertaining to information security. But this was with little consequence as it was not fruitful. [133] In 2010 during July, the UN did manage to guarantee progress when cyber-experts from fifteen states (with the inclusion of major cyber-powers like the US, China, and Russia) put forward a set of recommendations to the UN Secretary-General as part of a first step towards stability and security for the international community.[134]This was highly commendable.

Though small in terms of impact and ambiguous, these recommendations represent progress as states such as the US and Russia were able to come together to address issues that pertain to cyberspace and security with regard to it. This may even make possible a future multilateral treaty under the auspices of the UN (Russia has been advocating for this).[135] At the present, however, the role of the UN with respect to cyberspace and in turn cyber-security remains largely limited.

---

[130] UNGA, *Report of the Committee of Conferences,* UN A/Res/58/32 (22 September 2003); UNGA, *Report of the Economic and Social Council - Letter dated 17 February 2004 from the Permanent Representative of Switzerland to the United Nations addressed to the Secretary-General*, UN A/Res/59/61 (24 February 2004).
[131] UNGA, *Creation of a Global Culture of Cybersecurity,* UN A/Res/57/239 (31 January 2003); UNGA, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Informational Infrastructures*, UN A/Res/58/199 (30 January 2004); and, UNGA, *Creation of a Global Culture of Cyber security and Taking Stock of National Efforts to Protect Critical Information Infrastructures*, UN A/Res/64/211 (17 March 2010).
[132] UNGA, *Developments in the field of information and telecommunications in the context of international security*, UN A/Res/57/53 (30 December 2002).
[133] UNGA, *World Summit on the Information Society,* UN A/Res60/252 (27 April 2006).
[134] UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN A/Res/65/201 (30 July 2010).
[135] Markoff J, 'Step Taken to End Impasse over Cybersecurity Talks', New York Times, July 16, 2010, http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1 on 19 August 2017.

2.7 NATO's regulation of cyberspace

During the cyber-attack perpetrated against Estonia, little was done by NATO. NATO posited that it did not have a doctrine to use to go about tackling what had happened, nor did it have a strategy.[136] NATO could however not let things continue as they were. It therefore held its first meeting with regard to cyber-security a year later Bucharest in form of a summit where cyber-attacks were to be addressed. This summit resulted in the creation of two new NATO divisions focused on cyber-attacks. These were: the Cooperative Cyber Defence Centre of Excellence and, the Cyber Defence Management Authority.[137]

These two divisions aimed to centralise cyber defense capabilities across NATO members. Although little information is publicly available, the Authority is believed to possess monitoring capabilities that enable it to share critical cyber intelligence in real-time. Its aim is to eventually become an operational forefront for cyber-defense.[138] The two divisions also aspire to ensure the development of a long-term cyber doctrine and strategy.[139]The control of the NATO cyber-policy and defense however still resides with the North Atlantic Council.[140] According to Article 4 of the NATO treaty, members ought to consult each other in the event of a cyber-attack. This in itself is not binding on the member states when it comes to providing assistance in accordance with Article 5 of the NATO treaty. There is therefore a lack of implementation even with pressure from Eastern European states.[141]

2.8 The Council of Europe's regulation of cyberspace

Under the auspices of the Council of Europe in 2001, an international treaty came to be that was to provide for crimes committed through the internet as well as other computer networks (Cybercrime Convention). This treaty provided for a common policy that was to be aimed at providing protection to society against cybercrime. This was to be ensured through legislation

---

[136] Hughes R B, 'NATO and Cyber Defence: Mission Accomplished?' April 2009, at 1, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , on 19 August 2017.
[137] Hughes R B, 'NATO and Cyber Defence: Mission Accomplished?' April 2009, at 1, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , on 19 August 2017.
[138] Hughes R B, 'NATO and Cyber Defence: Mission Accomplished?' April 2009, at 1, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , on 19 August 2017.
[139] Hughes R B, 'NATO and Cyber Defence: Mission Accomplished?' April 2009, at 1, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , on 19 August 2017.
[140] http://www.nato.int/issues/cyber_defence/index.html on 18 August 2017.
[141] Article 4 and 5, *The North Atlantic Treaty*, 4 April 1949.

and international cooperation.[142] The US ratified the Convention in 2006. Cyber-attacks may be inferred to fall under the regulation on the Cybercrime Convention as the offenses it outlines relate to unauthorised access as well as interference of systems and information.[143] It is however questionable as to whether the rules laid down in the Convention apply to government actions when a governments in trying to enforce the law or ensure national security.[144]

Nonetheless, the Cybercrime Convention may be considered to impose limitations on the execution of cyber-attack operations by ratifying states. Parties to the Convention are taken to have agreed to cooperate with one another for the purposes of investigations or proceeding relating to criminal offenses.[145] Although implied, such an agreement to cooperate could also be inferred as placing a limitation on the conduct of ratifying states who cannot act contrary to the object of the Convention. It is however not clear as to what the consequences would be in the event of a breach by a member state to the Convention.

2.9 The OAS' regulation of cyberspace

The OAS approved a resolution in 2004 during April that provides that member states should consider implementing the principles of the Cybercrime Convention and should also consider making steps to accede to the said Convention.[146] This was followed by a 'Comprehensive Inter-American Cybersecurity Strategy' whose goal is to adopt policies that will provide protection to internet users and at the same time ensuring that the privacy and the individual rights of internet users is respected.[147] Subsequently, the OAS deployed experts as to be of technical assistance in the drafting and enacting of laws by member states to ensure that

[142] Preamble, *Convention on Cybercrime*, 23 November 2001, ETS No. 185; AlMahroos R, 'Privacy on the Internet and in Organizational Database: Phishing for the Answer: Recent Developments in Combating Phishing', J*ournal of Law and Policy for the Information Society, 595, 613 (2008).*
[143] Articles 2, 4 and 5, *Convention on Cybercrime*.
[144] Schaap A J, 'Cyberwarfare Operations: Development and Use under International Law' *121, 171 (2009).*
[145] Article 23, *Convention on Cybercrime*.
[146] OAS, *Meeting of ministers of justice or ministers or attorney generals of the Americas,* AG/Res/2040/XXXIV-O/04 (8 June 2004).
[147] OAS, *A Comprehensive Inter-American Cybersecurity Strategy: A Multi-Dimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, AG/Res/2004/XXXIV-O/04 (8 June 2004).

law.[148] Guidance is the only mandate of these experts as the OAS does not intend to bring about the promulgation of uniform laws.

In 2010 during January, a meeting convened by the OAS Working Group on Cybercrime put forward a recommendation that member starts ought to establish state bodies that will investigate and prosecute cybercrimes. There also ought to be domestic legislation criminalising cybercrime and enabling international cooperation on the same.[149] As it stands now, the OAS is working on useful regional joint strategies for combatting cyber-attacks that constitute cybercrimes. This is however not an active program that is to address cyber-attacks generally.

2.10 The SCO's regulation of cyberspace

In 2009 during June, a declaration was made known as the Yekaterinburg Declaration. In this declaration, it was provided by the SCO that one of the key elements of the common system when it comes to regional security is that information security should be guaranteed as well.[150] The SCO declaration presents what could one day be considered a model for other regional and international institutions that would want to provide for cyber-attacks. SCO anticipates that cyber-attacks do have the capability to undermine political stability.

2.11 Cyber-attacks and the Tallinn manual

The focus of the original manual was on the most severe cyber operations- that is, those that violate the prohibition of the use of force in international relations.[151] The new version of the manual however adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that those that fall below the threshold of the use of force or armed conflict.[152]The first Tallinn manual is the one that is relevant when it comes to this dissertation as it is the one that regulates cyberwarfare.

---

[148] OAS, *A Comprehensive Inter-American Cybersecurity Strategy: A Multi-Dimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, AG/Res/2004/XXXIV-O/04 (8 June 2004).
[149] Sixth Meeting of the Working Group on Cybercrime, 21-22 January 2010, Washington DC.
[150] SCO, *Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City* (9 July 2009).
[151] 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).*
[152] 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).*

In providing for how international law ought to regulate cyberwarfare, the Tallinn manual outlines ninety-five 'black letter rules' that may come in handy in regulating cyber-attacks. It also provides specific focus on areas such as sovereignty, state responsibility, *jus ad bellum, jus in bello,* and the law of neutrality and their implications in cyberspace.[153] As there is no explicit treaty under international law that regulates cyberwarfare, nor is there normative customary law on the same, this manual and commentaries made shed light when it come to the regulation of cyberwarfare as it looks at the different occurrences that may happen in cyberspace.

2.12 Conclusion

The legal framework regulating cyberwarfare may be drawn from various sources. Despite this being the case, there is yet to be binding obligations on states to adhere to some of these sources. For example, since the Tallinn manual, the only comprehensive work on cyberwarfare is just scholarly work. It does not present itself in as a treaty and thus problems may arise when it comes to implementing it. With this being the case, problems are evidently going to arise as to how liability ought to be attached when it comes to cyber-attacks perpetrated. Also, there are diverse views as to whether liability may be attached to states or to individuals. If there is difficulty in establishing liability, problems as to jurisdiction will arise as well.

[153] 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).*

CHAPTER 3

Cyberwarfare with respect to liability

3.1 Introduction

This chapter seeks to address the second research question which pertains to whether the legal framework regulating cyberwarfare can aid in establishing liability when it comes to cyberwarfare. When it comes to cyberwarfare, war has to be waged. War can only be waged between states, and with this being said, states should be considered liable for cyber-attacks they have orchestrated that have resulted in international wrongful acts. Despite states being the primary subject of war, individuals are the ones who carry out the cyber-attacks. When IHL violations occur, someone ought to be considered liable. Issues presented when it comes to both individual liability as well as state liability is what this chapter seeks to address.

3.2 Individual liability

Cyber-attacks are committed by individuals. With this being the case, it is important to determine who the perpetrator of a cyber-attack is in order to assist in a determination of liability. When it comes to cyberwarfare, it being warfare means that the law of armed conflict is applicable, and with that being the case, the participants remain the same. There will be combatants, civilians and at times, other parties may participate in the hostilities even if it is in the instance of isolated cases of having 'lone wolves'. When violations are committed in the context of cyberwarfare, determining the role played by different individuals enables an adjudicating forum to establish who to attach liability to and who is exempt from such liability.[154] The command responsibility doctrine also comes in handy in trying to establish individual liability.

3.2.1 Combatants in cyberwarfare

In IHL, there are certain individuals who are afforded a different status that flows from their participation or lack thereof during war. Combatant status is one of such statuses and it results in bringing to rest some legal questions that may arise such as immunity that is granted to combatants from prosecution for warlike acts, their susceptibility to intentional targeting as they may be legally views as objects of attacks, and, in part, their treatment when they are

[154] Rule 25, 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).*

captured.[155] This status has come in handy since the late nineteenth century where it was considered key in ensuring humanity in war.[156]

In this day and age, if there is to be a war, combatants intermingle often with civilians. When deliberating as to whether to provide a warning to civilians in the event of an impending attack, having civilians warned may compromise the military mission entirely. Civilians therefore end up being caught up when military attacks ensue.[157] Although unfortunate, this is a reality. In the cyber context, it is not far removed that, given the transboundary nature of cyberspace and the fact that actions in this space can affect many people at the same time, it is very hard to distinguish between a combatant and a civilian.

A combatant therefore, trying to adhere to the laws of war may find himself or herself in a dilemma when deciding when and how to act in cyberspace. His actions, although in pursuit of a military objective may intertwine with civilian matters thus complicating the entire matter altogether. There is therefore a need to better provide for what ought to constitute lawful combatant conduct during cyberwarfare and by doing so, combatants may be able to execute their military functions in a way that does not put civilians in jeopardy.[158]

3.2.2 Liability of commanders and superiors

The Tallinn manual in Rule 24 provides that commanders and other superiors do not escape criminal responsibility in the instance where they did not personally participate in the carrying out of an attack.[159] It is however not clear as to whether their liability would be established as a JCE or as a command responsibility. This position has been brought out in

[155] Watts S, 'The Notion of Combatancy in Cyberwarfare', *4th International Conference on Cyber Conflict (2012);* Rule 25, 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).*
[156] Watts S, 'The Notion of Combatancy in Cyberwarfare', *4th International Conference on Cyber Conflict (2012).*
[157] Watts S, 'The Notion of Combatancy in Cyberwarfare', *4th International Conference on Cyber Conflict (2012).*
[158] Rule 26, 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).*
[159] Rule 24, 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).*

various treaties.[160] Rule 24 is applicable in both a NIAC and an IAC and it is a reflection of normative customary law.[161]

Such responsibility extends down the chain of command or control. For example, orders to comply by a subordinate commander to his or her troops issued from a superior would still result in the subordinate commander being considered responsible as well for ordering the said war crime.[162] This would also be the position taken when it comes to cyber-attacks that constitute cyberwarfare. Such responsibility is manifest in the command responsibility doctrine. But even with that being said, what of a JCE? And if a JCE is to be considered, would combatants be considered liable regardless of the chain of command?

3.3 State liability

The ARISWA provides for state responsibility, and although it is soft law, it is the foremost reference point when it comes to the same. Article 1 posits that when it comes to internationally wrongful acts, they ought to be attributed to the responsible state and international responsibility is required.[163] This notion of state responsibility is supported by

[160] Article 49, *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention)*, 12 August 1949, 75 UNTS 31; *See also*: Article 50, *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention)*, 12 August 1949, 75 UNTS 85; Article 129, *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention)*, 12 August 1949, 75 UNTS 135; Article 146, *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*, 12 August 1949, 75 UNTS 287; Article 15(2), *Second Protocol to The Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict*, 26 March 1999; Article 86 and 87, *Additional Protocol I*; and, Article 25 (3) (b) and 28, *Rome Statute of the International Criminal Court*, 17 July 1998, ISBN No. 92-9227-227-6.

[161] *Prosecutor v Tihomir Blaskic (Trial Judgement)*, IT-95-14-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 3 March 2000; *See also: Prosecutor v Radislav Krstic (Appeal Judgement)*, IT-98-33-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 19 April 2004; *Prosecutor v Jean-Paul Akayesu (Trial Judgement)*, ICTR-96-4-T, International Criminal Tribunal for Rwanda (ICTR), 2 September 1998.

[161] Rule 24, 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).*

[162] Rule 24, 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).*

[163] Article 1, ILC, *Draft articles on state responsibility for internationally wrongful acts.*

state practice as well as *opinio juris*.[164] It is also brought out in Rule 6 of the Tallinn Manual where it is posited that a state is legally responsible for cyber operations attributed to it.[165]

In the *Corfu Channel Case*, the ICJ examined the threshold to attribute responsibility for actions within a state's borders.[166] It was held that territorial sovereignty is not only an essential foundation of international relations, but also that under customary international law, every state also has an obligation to not allow knowingly its territory to be used for acts contrary to the rights of other states.[167] This formulation, however, does not answer all the questions that come up that involve state responsibility. It therefore worth investigating the issue of state responsibility in closer detail. Difficult questions however arise such as whether a state should be held internationally responsible for a single soldier or hacker acting in the interests of the state that uses a cyber-attack to destroy critical infrastructure of an adversary. These questions merit further exploration.[168]

3.3.1 State actors

There is little controversy that, if a state's agent attacks another state, then the hostile conduct is attributable to the state. Article 4 of the ARISWA posits that the conduct of any state entity shall be attributed to that state under international law.[169] A state organ is to be understood as all the persons and entities that make up the organisation or government of the state and act on its behalf.[170]This view is further cemented in Rule 6 of the Tallinn Manual.[171]

This principle is a codification of customary international law. It reflects the assumption that a state is fully responsible for its agents (even in the instance when those agents act outside the scope of their duties). In *Armed Activities on the Territory of the Congo*, the ICJ held that

---

[164] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[165] 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).*
[166] *Corfu Channel Case* (UK v Albania) (1949), ICJ.
[167] *Corfu Channel Case* (UK v Albania).
[168] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[169] Article 4, ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[170] Article 2, commentary, ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[171] 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).*

in the instance of the occurrence of an armed conflict, a party to an armed conflict shall be considered responsible for all the acts of the members of its armed forces. This was considered a well-established rule under international customary law.[172] This rule is also considered applicable when a person or entity is not an organ of the state but exercises elements of governmental authority to the extension of both private and public entities.[173] Gervais gives the example that, say a country such Britain decides to employ private defence companies. In the event that the companies perform an act as they discharge their duties to Britain, such acts will be attributed to Britain.[174] As the ARISWA notes, if an entity, whether private or public concerns itself with government activity, no matter its acts, they shall be attributed to the said state.[175]

Similarly, if a state makes another state act on its behalf, these acts will be attributed to the state for whose behalf the state acts. Article 17 of the ARISWA considers a state internationally responsible for wrongful acts that it exercises control over knowingly.[176] This test echoes what was brought out in the *Corfu Channel Case* where a state is equally responsible for acts that is permits within its territory that result in internationally wrongful acts. This is of importance when it comes to cyberwarfare as given the transboundary nature of cyber-attacks, perpetrators of these cyber-attacks may be doing so on behalf of a state yet they are not perpetrating them from the said state.[177]

As mentioned, many states have already begun developing cyber units within their military or intelligence apparatuses. States have also delegated some elements of their cyber-attack capabilities to the private sector. One state might even consider using another state to launch an attack on its behalf. Although tracing a cyber-attack is a formidable technical challenge, if the targeted state successfully traces a cyber-attack to source state's cyber unit or to an

[172] *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda) (2005), ICJ.
[173] Article 5, ILC, *Draft articles on state responsibility for internationally wrongful acts*; *Amoco International Finance Corporation v Iran* (1985), Iran-US Claims Tribunal.
[174] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[175] Article 5, ILC, *Draft articles on state responsibility for internationally wrongful acts.*
[176] Article 17, ILC, *Draft articles on state responsibility for internationally wrongful acts;* Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[177] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*

entity acting with the authority or under the control of the source state, the latter ought to be held responsible.[178]

3.3.2 Non-state actors

A harder question, in both the realm of cyberspace and traditional warfare, is determining whether it is appropriate to attribute state responsibility when non-state actors perpetrate an attack. Article 51 of the Charter does not provide instruction on whether a state may respond with force to a non-state actor.[179] Non-state actors, usually hacktivists, present a complicated issue for targeted states. Hacktivists are usually private citizens motivated by mostly by their ideological feelings which may be nationalistic and who possess sufficient skill to perpetrate a cyber-attack.[180] The nature of cyberspace permits hacktivists to launch attacks on another state from anywhere without them having government direction. This freedom to engage in cyber-attacks from anywhere in the world gives them the leeway to operate from the territory of a third party that may not the engaged in hostilities nor at times be aware of what is going on. There are however questions as to whether action can be taken against such individuals considering the fact that they are carrying out acts, although not commanded by a state, but are done for a state anyway. Is any action against them a violation of state sovereignty?[181] The Charter of the UN does not explicitly address this, leaving a legal loophole that hacktivists may exploit.

Through custom and practice, it has been demonstrated that states do respond with force to non-state actors as states view them as threats given their actions. To their detriment however, they do not enjoy benefits that perhaps combatants would enjoy. To illustrate using an example, following the 9/11 attacks perpetrated against the US, US sought to respond to this using force which was considered acceptable by the international community.[182] This is further buttressed by the passing of resolution 1368 by the Security Council after 9/11 which

---

[178] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012)*.
[179] Article 51, *Charter of the UN*.
[180] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012)*.
[181] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012)*.
[182] Nato Review Magazine, 'The History of Cyber-attacks: A timeline', http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm on 30 January 2017.

endorsed US's response in self-defence in accordance with Article 51 of the Charter of the UN.[183]This was still universally supported even after it was later brought to light that non-state actors were the perpetrators.[184]

On what basis do we attribute responsibility to a state for the actions of its non-state actors? If the state directs or controls the non-state actors, regardless of whether the non-state actors are within its jurisdiction, there are several bases for which to hold the state responsible. However, lone wolf hacktivists present a more complicated dilemma. Under the original *Corfu Channel* formulation, it was posited that if a state did not know that its territory was being used, nor did it allow it, then *mutatis mutandis* the stat may not be considered responsible for acts perpetrated on its territory by another state.[185]

According to the ARISWA, following the decision reached in *Corfu Channel,* responsibility may be attributed to a state if a person or persons act in accordance with the instructions of a state.[186] The ARISWA also mirrors what was decided in the *Nicaragua case*. In *Nicaragua*, the issue was whether the US was responsible thus attributable for the actions of the contras in their rebellion. The ICJ posited that in order to establish if the US responsible, it was to be required to prove 'effective control' over the non-state actor group.[187] Such a finding would imply that state control extends beyond its immediate territory. Thus, if it was found that a state is in 'effective control' of non-state actors operating in another state, the controlling state would be considered responsible for their wrongful acts.[188] This is further brought out in the Declaration on the Strengthening of International Security that provides that every state has the duty to refrain from interfering in the activities of another state in any way.[189] Therefore, if a state provided assistance and thus interfered with the affairs of another state,

[183] UNSC S/Res/1368 (12 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.
[184] UNSC S/Res/1373 (28 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.
[185] *Corfu Channel Case.*
[186] Article 8, ILC, *Draft articles on state responsibility for internationally wrongful acts*; Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[187] *Military and Paramilitary Activities in and Against Nicaragua*, para 209.
[188] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[189] UNGA, *Declaration on the Strengthening of International Security,* UN A/Res/2734 (16 December 1970).

responsibility for their actions shall be attributed to the state that offered such assistance and thus consequently, interference.

Different forums have decided differently when it comes to 'overall control'. In the ICTY, the standard held is much lower and this was brought out in *Prosecutor vs. Tadić*.[190] In this case, the tribunal opined that interference results in an equation of the interfering state to a state organ.[191] This standard was to be applied only to participants in an organised and hierarchically structured group such as the military. An example that may be given to illustrate this is the Russian Business Network that has an association with the elite members of Russia, some of whom form the government.[192] This network of persons was alleged to have been involved in various attacks that were attributed to Russia such as those perpetrated against Estonia and Georgia, a fact that Russia denied. Following the 'overall control' test as laid down in the ICTY, such a relationship as the aforementioned one would be sufficient to consider a state responsible.[193]

When it comes to unorganised groups as well as individuals, the *Tadić* tribunal echoed the 'effective control' as was laid down in *Nicaragua*. For effective control to be established according to *Tadić,* there must be express instructions aimed at the commission of specific actions. In the instance that this is lacking, there ought to at least be a public backing of the same.[194]

Article 11 of the ARISWA posits that if a state adopts a conduct that had not been previously attributed to the state, it is considered to be attributable to the said state.[195] *The case of the US Diplomatic and Consular Staff in Tehran*[196] provides for this. In this given the case, when

---

[190] *Prosecutor v Tadic (Sentencing Judgment)*, Case No. IT-94-1-T, ICTY, 14 July 2007; The lower standard used in this case was criticised by the ICJ as being unsuitable because of the major drawback of broadening the scope of state responsibility beyond the fundamental law of international responsibility- *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro) (2007), Judgment, ICJ, 43; Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*

[191] *Prosecutor v Tadic*, 120.

[192] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*

[193] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*

[194] *Prosecutor v Tadic*, 120.

[195] Article 11, ILC, *Draft articles on state responsibility for internationally wrongful acts*.

[196] *The case of the United States Diplomatic and Consular Staff in Tehran* (US v Iran) (1980), 1980 ICJ, 3.

the militants who seized the US embassy were endorsed by the Iranian state, their actions were consequently attributable to Iran. The ICJ posited that when Iran approved the said conduct by the militants, tis was considered acceptable conduct for Iran and thus wrongful acts that were committed were to be attributed to Iran. With this case in mind, an example may be illustrated: if unorganised groups or individuals use a cyber-attack to destroy a power plant in another state and their host approved of their actions, these wrongful acts committed will be attributed to the said state hosting them.[197] The most difficult question however is what is to be made of lone wolf hacktivists? These individuals operate without active encouragement or instructions from a state. In this scenario, international law requires states to take reasonable preventive measures.[198]

The Convention on Cybercrime, for instance, requires signatories to adopt domestic laws that criminalise cyber-attacks.[199] How far a state's duty extends to prevent lone wolf hacktivists remains undetermined. For instance, must a state adapt its technology in some way, for example by removing online anonymity? Such a requirement raises serious questions about the liberty and privacy interests of individuals.[200] But this is an issue that is more clear within the context of domestic law, rather than the laws of war, and thus outside the scope of this dissertation.

What if a state were required by international law to take reasonable measures to protect other states from foreseeable cyber-attacks? In this situation, the said state knows of the cyber attackers launching of attacks and should therefore take the necessary steps to stop the attack from happening. This is not because of duty to the targeted state but rather a responsibility owed to the international community, failure to uphold resulting in an act being considered an internationally wrongful act. Also, if the host state fails to take any measures, the state that is being targeted may have no choice but to act in self-defence with the legitimisation of

[197] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[198] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[199] Preamble, *Convention on Cybercrime.*
[200] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*

Article 51 of the Charter of the UN.[201] This flows from the international obligation that requires a state to supress any acts by non-state actors as a failure to do so will result in a state being considered liable.[202] It is however not expected that the state goes over and beyond to prevent an attack by a non-state actor, rather, it is enough for the state to prove that it undertook sufficient measures that were unsuccessful. In such an instance, a state shall not be considered to be liable. There has arguably been a shift in the way state responsibility is viewed post the 9/11 attacks.[203] It has been opined by some scholars that, pre-9/11, a state may have been held responsible for the actions of non-state actors carrying out activities within its territory. The state alleging however has to prove that the state hosting the non-state actors exercised effective control over them. Knowing alone was therefore not considered sufficient devoid effective control. After 9/11 however this view was heavily contested. This may to a large extent be attributed to the campaign carried out by the US against Al-Qaeda.[204] This can be inferred to have resulted in the adoption of Resolutions 1368 and 1373 by the Security Council.[205]

It was expressly provided for in Resolution 1368 that those who aided, supported, or harboured the perpetrators of the 9/11 attacks would be considered responsible for their perpetration.[206] This is a very controversial path that the Security Council chose to attribute state responsibility. It may be considered a shift from the positions taken by the ICJ and the ICTY respectively in *Nicaragua* and *Tadić*. There are those who are in strong opposition of the shift opining that the Security Council resolutions were taken in favour of the US but not as a result of a consensus in the international community- something that is highly frowned

[201] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[202] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012).*
[203] 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?' *Australian International Law Journal, 201 (2007).*
[204] 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?' *Australian International Law Journal, 201 (2007).*
[205] UNSC S/Res/1368 (12 September 2001) Threats to International Peace and Security Caused by Terrorist Acts; UNSC S/Res/1373 (28 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.
[206] UNSC S/Res/1368 (12 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.

upon.[207] Some may however be of the view that this somewhat novel view is a reflection of how things were as those considered to be harbouring the perpetrators of 9/11 may be considered to in fact be endorsing their actions. This therefore consequently puts a higher burden on states in the realm of cyberspace without any direction as to compliance.

Given the transboundary nature of cyber-attacks and their ability to be perpetrated from anywhere in the globe, every state at some point may end up being considered liable eve if the only connection a state has to the perpetrators of the cyber-attack is only territory. And with that being said, how many states have the cyber capacity to ensure that their territory is not being used to carry out cyber-attacks directed at other states?[208] But with states comes diplomacy. States should therefore act according to their station and in the instance of a cyber-attack, a state ought not respond immediately with force. Compliance should first be sought from the state that is being accused of wrongful acts.[209] Only in the instance where there is no compliance is the victim state to attribute state responsibility.

3.4 Conclusion

Liability is an issue that cannot be ignored. When it comes to cyberwarfare, liability may present itself in both the individual level as well as at the state level. These two aspects of liability may both be looked at in the instance of cyberwarfare as they are not mutually exclusive. For example, if a state is found in violation of a cyberwarfare regulation that does not mean that the individual perpetrators of the cyber-attack carried out under the guise of the state will not be pursued for the particular violations perpetrated. In doing so however, there should be rules used to determine who may be charged for such violations. Not all perpetrators should be charged, rather those who exercise authority over others in a cyber-attack. This chapter is crucial in laying a foundational stone for the next chapter this dissertation will address which will be on jurisdiction. Without addressing the issue of

---

[207] Gervais M, 'Cyber-Attacks and the Laws of War' *Berkeley Journal of International Law, Volume 30, Issue 2 (2012)*.

[208] Gervais M, 'Cyber-Attacks and the Laws of War', *Berkeley Journal of International Law, Volume 30, Issue 2 (2012)*.

[209] *Gabcikovo-Nagymaros Project* (Hungary v Czechoslovakia) (1997), ICJ, 55-56 (In the first place countermeasures must be taken in response to a previous international wrongful act of another State and must be directed against that State. Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it. Third, the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question).

liability, establishing jurisdiction would be futile as there would be no part to bring before an appropriate forum.

CHAPTER 4

Cyberwarfare with respect to jurisdiction

4.1 Introduction

When we talk about jurisdiction, what it means is that a forum has the requisite authority to prescribe, enforce and adjudicate. The basis through which a state opts to exercise jurisdiction, and rightly so is when a person is physically or legally present in its territory (*in personam*) or an object in on its territory (*in rem*). In pursuant to its *in personam* jurisdiction a state may promulgate laws and regulations governing the cyber activities of individuals on its territory as well as its nationals. This is not only limited to physical persons but rather extends also to legal persons such as business entities. Their place of registration in this case would determine which state enjoys jurisdiction over it. This would also extend to internet service providers. *In rem* jurisdiction would come in handy when considering the location of cyber infrastructure.

4.2 Cyberwarfare and jurisdiction in international law

When it comes to international customary law, a state is considered to enjoy jurisdiction when it comes to: its nationals; persons in its territory perpetrating cyber-attacks; presence of cyber infrastructure within its territory and matters considered to trigger universal jurisdiction as provided for in international law.[210]

Difficulties arise when it comes to attributing jurisdiction in cyberspace given the nature of content in cyberspace as cloud systems for example replicate data that may be considered available across jurisdictions thus making it difficult to pinpoint exactly who has jurisdiction over such information to begin with. Such information may be accessed from different states thus amplifying this dilemma.[211] But despite the aforementioned assertions, a state may not

[210] Rule 2, 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).*

[211] Rule 2, 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).*

be deterred from exercising jurisdiction over individuals and objects present within its territory.[212]

When it comes to jurisdiction, there are various principles that come into play. The very first principle that shall be considered is the principle of territoriality. According to Attorney General of the European Court of Justice, this principle has two dimensions: a subjective dimension and an objective dimension. The subjective dimension provides that a state has jurisdiction over an act that originates from its territory. The objective principle however provides that a state has jurisdiction over an act that concludes on its territory. This therefore results in a number of different states having jurisdiction over the same conduct.[213]With regard to jurisdiction based upon territoriality, it must be noted that although individuals using information technology have a specific location where they are physically present, the location of mobile devices can change during a computing session thus resulting in an act perpetrated through a mobile device having different locations that may be attributed to the act. For instance, a person with a computing device, be it a phone or a tablet, can start a number or transactions for processing by a cloud-based service. As the transactions being undertaken take place, the user may keep changing locations. All these locations comprise where the said person carried out his/her transactions.[214]

Subjective territorial jurisdiction is considered applicable even in instances where the originating state does not feel the effects of the conduct undertaken. When it comes to objective territorial jurisdiction however, emphasis is not on where the conduct originated from, but where it was concluded thus where its effects are felt.[215] The objective territorial principle is therefore also known as the effects principle as well.[216]

---

[212] Rule 2, 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).*

[213] Opinion of Mr. Advocate General Darmon, *Re Wood Pulp Cartel* (Ahlström Osakeyhtiö and others v Commission of the European Communities) (1994), paras, European Court of Justice.

[214] Rule 2, 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).*

[215] Opinion of Mr. Advocate General Darmon*, Re Wood Pulp Cartel* (Ahlström Osakeyhtiö and others v Commission of the European Communities) (1994), paras, European Court of Justice.

[216] https://home.heinonline.org/titles/American-Law-Institute-Library/Restatement-Third-Foreign-Relations-Law-of-the-United-States-Revised/?letter=R on 27 January 2018.

With regard to cyberwarfare, the objective territorial jurisdiction is very important to consider as the jurisdiction of the place where the effects of the conduct in question are felt is brought to question. In the Estonia cyber-attack in 2007, half of the attacks originated from abroad. Invoking the objective territorial principle would thus grant jurisdiction to Estonia over all individuals, wherever located who instigated the cyber-attack.[217] Similarly, in the cyber-attack perpetrated against Georgia in 2008, given the fact that its perpetrators were considered to be located outside Georgia, through the objective territorial principle, Georgia would have been considered to have jurisdiction over the perpetrators of the cyber-attacks no matter where they were.[218]

Other recognised bases for extraterritorial jurisdiction, include: nationality of the perpetrator of the cyber-attack (active personality); nationality of the victim of the cyber-attack (passive personality); national security threat to the state in the form of the cyber-attack (protective principle); and, violation of a universal norm of international law through the perpetration of the cyber-attack such as a war crime (universal jurisdiction).[219]

In light of the variety of jurisdictional bases in international law, two or more states often enjoy jurisdiction over the same person or object in respect of the same event. This was brought out in the Tallinn manual where it was considered because of the nationality of the perpetrator, the nationality of the victims as well as where a cyber-attack originates and concludes, various people end up having jurisdiction over the same event.[220]

---

[217] NBC News.com, Security, 'A look at Estonia's Cyber Attack in 2007', http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WJm_J2997IU on 7 January 2017.

[218] Rule 2, 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)* -Civilians are not entitled to combatant immunity under the law of armed conflict and therefore are fully susceptible to the traditional bases of jurisdiction dealt with here- para 9.

[219] Rule 2, 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).*

[220] Rule 2, 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).*

In some instances, although an act may by fact be attributed to a person, by law liability and thus jurisdiction cannot be attached to them.[221] Examples of such instances include where individuals enjoy certain immunities and also where there is a grant of primary jurisdiction to one of the states enjoying jurisdiction over a person or a particular offence (through the application of a Status of Forces Agreement).[222]

4.3 Jurisdiction of flag states and states of registration

Under international law, cyber infrastructure located on aircraft, ships, or other platforms in international airspace, on the high seas, or in outer space is subject to the jurisdiction of the flag state or state of registration.[223] On the aforementioned vessels, cyber infrastructure may be present in the form of offshore installations or even satellites. A good example of cyber infrastructure on a ship is when an Automatic Identification System is used to always have the location of the ship known.[224]

In the instance mentioned above for example, the jurisdiction over the cyber infrastructure shall be the flag state and thus in the event of it being compromised through a cyber-attack, it shall be taken that the attack is being perpetrated against the flag state regardless of whether this is at the high seas[225] and in the instance of aircraft and space objects, their state of registration.[226]When it comes to ships, they may only sail under one flag thus only one flag state is permitted per ship. This is except it is permitted somewhere in international law that a ship may perhaps have more than one flag state. Different vessels have different rules when

[221] Rule 2, 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).*
[222] Rule 2, 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).*
[223] Rule 3, 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).*
[224] Rule 3, 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).*
[225] Article 92 (1), *Convention on the Law of the Sea.*
[226] Article II, *Convention on Registration of Objects Launched into Outer Space*, 14 January 1975, 1023 UNTS 15; Article VIII, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205.

it comes to who may have jurisdiction over the vessel. In the case of offshore installation, coastal states are considered to have the sovereign rights over such.[227]

It must be borne in mind that although objects and persons abroad platforms are subject to the jurisdiction of the flag state or state of registration, they may also be subject to the jurisdiction of other states.[228]In the instance where an individual belongs to a different state yet the flag state is also different, both states would exercise jurisdiction over the individual but on different grounds, for one it will be based of the nationality of the individual whereas the other based off the flag state.[229]

With respect to flag state or state of registration, a state that has control over the vessel may not exercise jurisdiction over it despite the vessel being in its territory and thus tis control. This is also posited in the Tallinn Manual.[230] It may therefore be inferred that there is an absence of a specific international law basis for having things as they have been brought out above such as is the case where there is a vessel that is in the exclusive economic zone of a coastal state. There is therefore a lot that ought to be considered when deliberating on the assertion of jurisdiction. It may also furthermore be brought out that in accordance with Article IV and IX of the Outer Space Treaty, if flag state and registration of vessel as grounds for establishing jurisdiction is not respected, this would result in a violation of Article 2(4) of the Charter of the UN.[231]

There are therefore procedures that have to be adhered to when it comes to even registering vessels. These include the fact that if one is a national of a particular state, if they wish to register their vessel, it will acquire the same place of registration as its owner's nationality. Companies however usually acquire their nationality based on where the company ware

---

[227] Rule 3, 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)*.
[228] Rule 3, 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)*.
[229] Rule 3, 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)*.
[230] Rule 3, 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)*.
[231] Article IV and IX, *Outer Space Treaty*; Article 2(4), *Charter of the UN*.

incorporated but also have other links to places such as where registration of the company was done.[232]In the event of war, what is to constitute the nationality of a corporation is established through a 'control-test' to determine who has decision making capabilities in the company, is it enemy nationals or one's own nationals.[233]

With technological advancements, even submarines may be said to constitute cyber infrastructure. With respect to them, jurisdiction is derived from their ownership as well as other laws that may be considered applicable such as Article 54 of The Hague Regulations and the laws of the sea.

4.4 Sovereign immunity and inviolability

Sovereign immunity entails that if an object or a person is used or works for the government in a non-commercial way, they are considered to enjoy sovereign immunity. Despite this being of importance even in the advent of cyberwarfare, the Tallinn manual does not consider immunity bestowed on government officials nor diplomatic immunity.[234]

If a platform or vessel enjoys sovereign immunity, any interference with regard to its cyber infrastructure is considered to be in violation of its sovereignty.[235] In international law, warships and government ships are considered to enjoy state immunity. If they do have cyber infrastructure and is compromised, this is considered to violate the sovereignty of the state that the warship or the government ship belongs to.[236]This also applies when it comes to state aircraft[237]as well as space objects of non-commercial government purpose as was opined by the International Group of Experts.[238]

---

[232] Brownlie I, Principles of Public International Law 420 (7th ed. 2008).
[233] *Daimler Company Limited v Continental Tyre and Rubber Company* (1916) 2AC 307.
[234] Rule 4, 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)*.
[235] Rule 4, 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)*.
[236] Articles 95 and 96, *Convention on the Law of the Sea*; United States Commander's Handbook on the Law of Naval Operations, 2007, para 2(1).
[237] Rule 4, 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)*.
[238] Article 3(3), UNGA, *United Nations Convention on Jurisdictional Immunities of States and Their Property*, UN A/Res/59/38 (2 December 2004).

Sovereign immunity may only be invoked in the instance where the platform considered is used exclusively for government purposes. With this being the case, if a government institution partly works for the government but also participates in the economy to make profit, it cannot enjoy state immunity and thus it cannot be considered to be inviolable. This is the same as satellites that are partly owned by the government and partly by individuals pursuing commercial gain. This was the stance taken by the International Group of Experts.[239]

When an object enjoys immunity, any interference of it constitutes a violation go international law as it also considered to be inviolable.[240] Interference may be in the form of damage to the property as well as unauthorised access to the same. This therefore speaks into what is to be concluded if cyber infrastructure is compromised when the platform it is on is inviolable. This was brought out in the British military communications satellite case in 2007 where reprogramming was the carried out having the act considered a violation of sovereignty.[241]

It is also not enough for a state to claim that it enjoys sovereignty. It also ought to respect the sovereignty of the vessels of other states that enjoy the same immunity. A warship therefore ought not use force against another countries ship unwarrantedly. Airspace is one such thing that is not taken likely. Regardless of whatever immunity is enjoyed by an aircraft, if it crosses over to another state's airspace, it ought to be prepared for the consequences of doing so. Cyber infrastructure is no exception to this rule.[242] Legally recognised interests thus require for states to have some respect for each other and thus in turn act accordingly.[243]

---

[239] Rule 4, 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)*.

[240] Rule 4, 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)*.

[241] Rule 4, 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)*.

[242] Article 19. 25(1), 32, *Convention on the Law of the Sea*.

[243] Rule 4, 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)*.

Despite having no rule in international law that authoritatively provides for vessels and objects that are made use of for non-commercial purposes, the Convention on Jurisdictional Immunities in Article 5 provides that a state is to enjoy immunity from the courts of another state when it comes to matters that touch on its property.[244]It could therefore be put forward that this provision, as well as the points made above, there is a general principle which is against the interference of objects, vessels and platforms owned or used by a state for non-commercial governmental purposes as they are covered by the state's sovereignty. They are therefore subject to a state's exclusive jurisdiction irrespective of their location. There is however no consensus on this in the international platform.[245]

In war, things are very different. As states fight each other, it ceases to matter that certain people, objects, platforms and vessels enjoy immunity and are thus to be considered inviolable. This is however subject to specific rules such as Article 45 of the Vienna Convention on Diplomatic Relations. This is because, as war ensues, these objects and vessels may at times be considered military objects and thus become targets of attacks.[246] Cyber infrastructures are seen no differently.[247]Status of Forces Agreements may however afford objects and platforms immunity during war. Diplomatic archives pursuant to the Vienna Convention on Diplomatic Relations also enjoy immunity at all times, even during war.[248]

4.5 Conclusion

When it comes to jurisdiction, different platforms are affected differently. Within the territories of states, even when it comes to cyberspace, the presence of physical cyber infrastructure can still be regulated. The biggest problem faced on the international level is how to go about matters that already prove difficult to regulate despite being provided for

[244] Article 5, *Convention on Jurisdictional Immunities*.
[245] Rule 4, 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)*.
[246] Rule 4, 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)*.
[247] Rule 4, 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)*.
[248] Article 24 and 27, *Vienna Convention on Diplomatic Relations,* 18 April 1961.

under international law. These are areas that concern the high seas and outer space. But even when it comes to asserting jurisdiction, there are exceptions under international law that ought to be adhered to. These to pose unique challenges when it comes to asserting jurisdiction within the context of cyberwarfare.

CHAPTER 5

Recommendations and conclusion

5.1 Introduction

States now have the capacity to make use of modern information technology to inflict grave harm on other states and their economies. This has been demonstrated by the events that have happened throughout the years where states have had their critical infrastructures compromised through cyber-attacks perpetrated through cyberwarfare.[249] This cannot continue to go unaddressed. Solutions ought to be sought.

This dissertation looks into cyberwarfare regulation with particular focus on liability and jurisdiction with respect to the same. The first chapter provided an introduction to this dissertation, and by doing so, outlined the need to pursue this dissertation with the aim that as the research objectives and questions are addressed, this will make clear the problems that are faced in the purview of international law when it comes to cyberwarfare regulation in general, and in particular, how liability can be established and jurisdiction determined.

This chapter marks the final chapter of this dissertation. It will address various recommendations and succinctly conclude this dissertation.

5.2 Recommendations

5.2.1 A cyberwarfare treaty

After World War II, so much changed. Nuclear weapons became the 'must have' if a state was establish itself as a super-power. With this being the case, a lot of concern arose as to the implications of unchecked nuclear power. This therefore resulted in arms control agreements that brought to an end the anxiety sparked by this new form of technology then. Despite the fact that there are still nuclear threats, having agreements that have binding effects on members who are party to the agreement has its benefits which outweigh a situation where the said agreements do not exist entirely.

With cyberspace being a novel domain that poses many possibilities as well as threats, there is a need to regulate this space. For purposes of this dissertation, there is a need to specifically

[249] Philosophy and Technology, Eilstrup- Sangiovanni M, 'Why the World Needs an International Cyberwar Convention', 21 July 2017, https://link.springer.com/article/10.1007/s13347-017-0271-5> on 29 January 2018.

regulate cyberwarfare as its consequences have been devastating so far and if it remains unchecked, things will only continue to get worse. This is especially the case as states develop cyber offensive weapons in anticipation of their use against their enemies.[250]

Benjamin Mueller, writing on 'Why we need a Cyberwar Treaty' posits that the international community ought to take the prospect of cyberwarfare seriously and by doing so, there needs to be a new agreed standard that should outline its parameters.[251] Peace and justice in cyberspace should be protected by international law through a treaty or a set of treaties under the UN preferably as the UN is arguably the most influential organisation in the world due to its numbers when it comes to membership.[252] In order to establish consensus and have obligations bind states and individuals, a comprehensive treaty would go a long way. It would also bring about a uniform standard to which each state may be held, and it would also result in certainty and predictability as to how international law applies when it comes to cyberwarfare.

According to Mueller, the 'weaponisation' of cyberspace should no longer be taken to entail science fiction.[253] Gone are the days of 'Neuromancer'[254]: militaries have the capacity to carry out attacks on communications networks and critical infrastructures of states just by making use of cyberspace.[255] With the cyber capacity of states growing yet remaining unchecked, the more probable that the world will soon face a catastrophe like none ever seen before because as it stands today, cyberspace connects everything we all hold dear in one way or another.[256]

There is no regulation whatsoever of war in cyberspace -unlike conventional forms of battle, which are subject to an extensive set of international treaty laws signed and respected by the

[250] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[251] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[252] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[253] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[254] Gibson W, Neuromancer, 1984.
[255] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[256] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.

vast majority of the world's states.[257] IHL regulates when a nation state may legally use military force against another state, and what means it may make use of to do so. Also a line may be extrapolated to have cyberspace and consequently cyberwarfare regulated by IHL. But even with that being the case, *lex generalis* will never be as effective as *lex specialis* and cyberwarfare is no exception.[258]

But even when comparing the physical domain to cyberspace, the differences that are brought out in cyberspace ought to be emphasised. Cyberspace makes it in such a way that an attack can take place in one removed location and have its effects felt many miles away easily. What is to be understood as a cyber-attack is also not clearly provided for anywhere in international law except for its mention in the Tallinn Manuals which constitute soft law and thus are only persuasive as they are now. Also, ought a cyber-attack to cause devastating effects to be considered cyberwarfare?[259]What light a treaty would shed to questions such as this!

If an international treaty is indeed to be drafted, there are certain key things it ought to provide for. First and foremost, the treaty should unequivocally clarify what is meant by a cyber-attack. Secondly, what is permissible behaviour between states should also be considered. Third, sanctions should be meted to states that act contrary to their obligations in the treaty in the form of reparations and cessation of injury that is being caused. It is also imperative that many states are party to the treaty as this would give the treaty a large backing and thus also ensure that there is little impetus as to its functions as most states will be party to the treaty.

A cyberwarfare treaty will bring about three main advantages. First, militaries will know to what standard their conduct ought to conform thus resulting in obligations by states as well as duties. Second, with sanctions being meted for wrongful acts committed in cyberspace, states may be deterred from carrying out certain acts. This also applies to individuals. Third,

---

[257] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[258] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[259] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.

having a treaty may bring about cooperation that would be indispensable considering the transboundary nature of cyberspace and in turn cyber-attacks.[260]

5.2.2 Establishing an international tribunal for cyberwarfare

Judge Schjolberg considered that under Chapter 7 of the Charter of the UN, the UN Security Council could establish an international criminal tribunal for cyberwarfare for the investigation prosecution and sentencing of cyber-attacks within the context of cyberwarfare. He also considered that the framework of the Charter of the UN was the most effective means for this, given that it would be binding on all members of the UN.[261]

There are precedents for such activity. The Security Council asserted its rights, authority and jurisdiction based on the Charter when it established the ICTR and the ICTY.[262] In the case of the international criminal tribunal for cyberwarfare, the UN Security Council would have the authority to refer cases to it and could request an investigation.

Judge Scholberg considers cyberspace the fifth common space after land, sea, air, and outer space. There is a great need for operation among all nations. Given the nature of cyberspace, states by themselves with no cooperation are ill-matched. Such a matter as cyberwarfare should not be constrained to domestic law, thus domestic action. It should be considered a latter that should be of international concern and thus addressed on the international platform.[263]

An international criminal tribunal for cyberwarfare would be fully independent and would be established to ensure that the gravest global cyber-attacks in cyberspace do not go unpunished. According to Judge Scholberg, the chamber of an international criminal tribunal for cyberwarfare should consist of 16 permanent Judges all appointed by the UN. These Judges could be divided between 3 trial chambers and 1 appeals chamber. Judges would be appointed for a period of less than 4 years.[264]This tribunal would therefore be modelled from those that came before it. Its necessity however is another matter and this dissertations

---

[260] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[261] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[262] Article 39, *Charter of the UN.*
[263] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[264] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.

assertion is that there is need to have a forum before which matters that constitute cyberwarfare may be heard and adjudged.

5.2.3 Expanding the mandate of the World Trade Organisation (WTO)

Digital industrial espionage falls under the WTO, which ought to take steps to outlaw what is an anti-competitive tactic, and expand the scope of its dispute settlement mechanism to include such behaviour.[265] The WTO would therefore be tasked with being involved in cases where there have been cyber-attacks that have in turn resulted in digital industrial espionage. But in order to do so, there is a need to expressly have this provided for under the WTO Treaty Regime.

5.2.4 Expanding the definition of aggression to incorporate cyberwarfare

The General Assembly of the UN has in one of its resolutions provided a definition for aggression which has not been defined in the Statute of the ICC.[266] Under this resolution, aggression is defined as a situation where the territorial integrity or political independence of a state is threatened by the use of armed force by another state in a way that is considered inconsistent with the Charter of the UN. Article 3 of the resolution, looking into the particulars of events that would constitute aggression despite a declaration of war provides that the bombardment by the armed forces of a state against the territory of another State or the use of any weapons by a state against the territory of another State may constitute aggression. This is a very wide provision and it may be argued that cyber-attacks would constitute such a bombardment. But in the instance of cyber-attacks, they are not necessarily felt, only when they manifest themselves physically. The international legal system must adapt to this battleground and provide workable mechanisms to hold aggressive actors accountable for their actions.[267] The complexity of cyberspace thus pre-empts that the definition of aggression ought to spell out the particulars that would constitute aggression in cyberspace.

---

[265] The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.
[266] UNGA, *Definition of Aggression*, UN A/Res/3314 (14 December 14 1974).
[267] Ophardt J A, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law & Technology Review 1-28 (2010).*

The Assembly of State Parties should construct the definition of aggression to include these emerging challenges. The definition should also include the challenged posed by different actors in cyberspace (specifically non-state actors).[268]

5.2.5 Building capacity on the international level to address cyberwarfare

5.2.5.1 The ICC

As the Nuremberg trials ensued, it was stated that peace is nothing without justice and justice can only be sought trough law, which is meaningless without a court to decide what is just and lawful.[269] An independent Criminal Court for Cyberspace is urgently needed to enable global justice. The court would enforce measures on cyber-attacks that constitute cyberwarfare thus posing great threats to the critical infrastructures of states. To date, we have had many serious cyber-attacks that had devastating effects. Despite this being the case, nearly none of the perpetrators of these cyber-attacks has been prosecuted let alone investigated. Such acts need to be included in a global treaty or a set of treaties, and investigated and prosecuted before an international criminal court or tribunal.[270]

The international community took in 1998 during July, a great step when it sought to establish a permanent International Criminal Court, when 120 States adopted the Rome Statute of the ICC. 160 States were present in Rome and it is understood that launching the Rome Statute was based on complete consensus among all present States.[271]

The ICC is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court does not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a state, party to the Statute of the ICC, is unwilling or unable to prosecute.[272] Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.[273]

---

[268] Ophardt J A, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law & Technology Review 1-28 (2010).*
[269] Ferencz B, USA, *The Nuremberg War Crimes Tribunal* (1945).
[270] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[271] Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.
[272] Article 17, *Rome Statute.*
[273] Article 5, *Rome Statute.*

There is therefore a need under international law to have a Court that is mandated to prosecute cyber-attacks. This has to start by having it set out in a treaty or a set of treaty granting a court jurisdiction to adjudicate over such matters or have this mandate included in the Rome Statute to expressly provide for cyber-attacks and their prosecution as a separate crime that can sometimes have elements that lack in the already defined crimes.

5.2.5.2 The ICJ

An international criminal court cannot have matters between states brought before it. There is therefore a need to inquire as to what forum states may bring matters that arise between them with regard to the question of cyberwarfare and generally cyber-attacks. This is both a question of jurisdiction and capacity and expertise to entertain a matter.

The ICJ was established by the Charter of the UN, which provides that all members of the UN are parties to the Courts Statute.[274] The Court is the principal judicial organisation for the UN and started working in 1946.[275]

The ICJ functions as a world court. The Court consists of 15 judges elected for a 9 year period by the UN General Assembly and the Security Council sitting independently of each other. No nations may have more than one judge, and elections are held every three years for one third of the judges.[276] A State party to the case may appoint a judge *ad hoc* for the purpose of the case. With the prevalence of cyber-attacks, this dissertation proposes that expert judges who serve permanently ought to be brought on board to build capacity to address issues between states when it comes to cyberwarfare. States have over the years chosen to address this matter by themselves, but if capacity is built by the ICJ, many matters may now be brought forth before the Court.

When it comes to jurisdiction currently, the Court decides cases in accordance with international law, disputes of a legal nature that are submitted to the Court by agreement between the States parties to the case.[277] The Court give advisory opinions on legal questions only at the request of the organs of the UN and 16 specialised agencies authorised to make

[274] Article 7(1), *Charter of the UN*.
[275] Article 92, *Charter of the UN*; Article 1, *Statute of the ICJ*, 18 April 1946.
[276] Article 2 and 3, *Statute of the ICJ*.
[277] Article 36, 38 *Statute of the ICJ*.

such a request.[278] If any doubts occur on the jurisdiction, it is the Court itself which decides. The judgments are final and without appeal. Perhaps a special agency that is tasked with cyberwarfare and cyber-attacks may be given the authority to approach the Court as well and request for an advisory opinion.

5.3 Conclusion

This dissertation has addressed issues as to what constitutes the legal framework regulating cyberwarfare on the international platform. In doing so, it has looked at both positive and normative obligations as they both shape what is expected of individuals and states.

When addressing the issue of liability with regard to cyberwarfare which was tackled in Chapter 3, it was argued that liability can be attached to both the state and the individual. The reason as to why liability may be attached to both is because both are subjects of international law and different legal regimes regulate their conduct. State liability and individual liability were also argued to be independent determinations. This means that for a single cyber-attack that brings about the question of liability, both the state and individuals may be considered liable.

With respect to individual liability, different actors when it comes to warfare are considered. In trying to establish liability, the status of the individual was deemed to be of importance. If an individual is a combatant or a civilian taking part in hostilities, the implications under international law vary. Questions as to anonymity and its implications when it comes to liability were also addressed. In answering these questions, the legal theories posited by scholars such as Emile Durkheim, Immanuel Kant and John Rawls helped to shape the flow of the argument. Their different views with regard to the online person kicked off the dissertation in the literature review, and it is based off these views that individual liability was addressed in Chapter 3.

With respect to state liability, positive international law and normative international law were analysed in detail. The reason why it was essential to do both was because under Article 38 of the Statute of the ICJ, Conventions and normative customary international law are brought out as both being of foremost importance in determining disputes between states.

[278] Article 65, *Statute of the ICJ.*

Chapter 4 of this dissertation addresses the question of establishing jurisdiction. Jurisdiction is important to determine because without jurisdiction asserting liability would be useless. Principles if jurisdiction such as the nationality principle, the territorial principle, the protective principle, the passive personality principle and the universal principle are analysed. Given the transboundary nature of cyber-attacks, it was necessary to look into all of these principles as some would be applicable when the other principles are not.

Chapter 5 of this dissertation gave recommendations and it concludes this dissertation. In giving recommendations, this dissertation argues that there is a lot that may be done when it comes to regulating cyberwarfare on the international platform. The recommendations provided include: the establishment of an international treaty that will address the issue of cyberwarfare and cyber-attacks that may not necessarily constitute cyberwarfare but constitute threats to international peace under Chapter 7 of the Charter of the UN; establishing an international tribunal for cyberspace; expanding the mandate of the WTO; expanding the definition of aggression to incorporate cyberwarfare; and, building capacity on the international platform to address the issue of cyberwarfare through an analysis of the mandate of the ICC and the ICJ.

This dissertation hopes that the recommendations its makes will pave the way when it comes to addressing the issue of cyberwarfare regulation and in particular with specific focus on the issues of liability and jurisdiction.

BIBLIOGRAPHY

Books

Brownlie I, Principles of Public International Law, *Oxford Publishers (2008).*

Gibson W, Neuromancer, *Ace Books (1984).*

Journal articles

AlMahroos R, 'Privacy on the Internet and in Organizational Database: Phishing for the Answer: Recent Developments in Combating Phishing', J*ournal of Law and Policy for the Information Society, 595, 613 (2008)*

Brown B L, 'The Proportionality Principle in the Humanitarian Law of Warfare: Recent Efforts at Codification' *Cornell International Law Journal 10(1) (1976).*

Cannizzaro E, 'Contextualizing Proportionality: *jus ad bellum* and *jus in bello* in the Lebanese war' *International Review of the Red Cross, 88(4) (2006).*

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?' *Australian International Law Journal, 201 (2007).*

Delibasis D, 'The Right to National Self-Defense in Information Warfare Operations' 268 (2007), 274.

Doswald-Beck L, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' *Computer Network Attack and International Law, 163, 166 (2002).*

Fry J D, 'Gas smalls awful: UN forces, riot-control agents, and the chemical weapons convention' *Michigan journal of international law 475 (2010).*

Gable K A, 'Cyber-Apocalypse Now: Securing the Internet against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent 43' *Vanderbilt Journal of Transnational Law 59 (2010).*

Geiss R, 'Cyber Warfare: Implications for Non- International Armed Conflicts', *International Law Studies, US Naval War College, 89, 627 (2013).*

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

Glanville L, 'The Responsibility to Protect Beyond Borders' *Human Rights Law Review 12(1), (2012).*

Hathaway O A, Crootof R, 'The Law of Cyber- Attack' *Yale Law School Legal Scholarship Repository (2012).*

Hathaway O A *et al*, 'Cyberwarfare and International Law'.

Hollis D, 'Cyber War Case Study: Georgia 2008' *Small Wars Journal (2011)*.

Howell JM, 'A Matter of International Concern' *The American Journal of International Law, Volume 63, 4 (1969).*

Kai A, 'Individual Criminal Responsibility for Cyber Aggression' *Journal of Conflict and Security Law (2016).*

Kanuck S P, 'Recent Development, Information Warfare: New Challenges for Public International Law', *Harvard International Law Journal, 37, 272, 282 (1996).*

Melzer N, 'Targeted Killing in International Law' *Oxford Scholarship Online (2009).*

Ocran T M, 'The Doctrine of Humanitarian Intervention in Light of Robust Peacekeeping' *Boston College International and Comparative Law Review 25(1) (2002).*

Ophardt J A, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law & Technology Review 1-28 (2010).*

Orman H, 'The Morris Worm: a fifteen-year perspective' 99 (5) *IEEE Security and Privacy (2003).*

Pejic J, 'The Protective Scope of Common Article 3, more than meets the eye', *International Review of the Red Cross*, *93, 881 (2011).*

Queguiner J F, 'Precautions under the Law Governing the Conduct of *Hostilities' International Review of the Red Cross 88,864 (2006).*

Ramsey P, 'The Just War, Force and Political Responsibility' *Rowman & Littlefield (2002).*

Schaap A J, 'Cyberwarfare Operations: Development and Use under International Law' *121, 171 (2009).*

Schjolberg S, 'An International Criminal Tribunal for Cyberspace'.

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).*

Schmitt M N, 'Wired warfare: Computer Network Attack and Jus in Bello' *International Review of the Red Cross 84, 365 (2002).*

Sliedregt E, 'Command Responsibility and Cyberattacks' *Journal of Conflict and Security Law (2016).*

Sossai M, 'Drugs as Weapons: Disarmament Treaties Facing the Advances in Biochemistry and Non-Lethal Weapons Technology' *Journal of Conflict and Security Law 5, 1 (2010).*

Turns D, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' *Journal of Conflict and Security Law*, *Volume 17, Issue 2, 1, 279-297 (2012).*

Waldman A E, 'Durkheim's Internet: Social and Political Theory in Online Society' *New York University Journal of Law & Liberty (2013).*

Walzer M, 'Just and Unjust Wars: A Moral Argument with Historical Illustrations' *New York, Basic Books (1977).*

Watts S, 'The Notion of Combatancy in Cyberwarfare', *4th International Conference on Cyber Conflict (2012).*

Wong J, 'Non-intervention: Restricting Electronic Surveillance against Cyber terrorism'.

Internet sources

ANONHQ.COM, Vandita, 'The Biggest Military Hack Ever Exposes NASA Secret 'UFO Files'' http://anonhq.com/biggest-military-hack-exposes-nasa-lie-ufos/ on 30 January 2017.

BBC News, Technology, Fildes J, 'Stuxnet worm 'targeted high-value Iranian Assets', http://www.bbc.com/news/technology-11388018 on 8 January 2017.

BBC News, Technology, Lee D, ''Red October' Cyber Attack Found by Russian Researchers', http://www.bbc.com/news/technology-21013087 on 8 January 2017.

BBC News, Technology, Ward M, *'Iraq Conflict Breeds Cyber-War among Rival Factions',* http://www.bbc.co.uk/news/technology-28418951 on 8 January 2017.

CBC News, Politics, Weston G, 'Foreign Hackers attack Canadian Government', http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618 on 8 January 2017.

Financial Times, Sevastopulo D, 'Chinese Hacked into Pentagon', https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac on 7 January 2017.

Fox News, 'Pentagon Source Says China Hacked Defence Department Computers', http://www.foxnews.com/story/2007/09/04/pentagon-source-says-china-hacked-defense-department-computers.html on 8 January 2017.

HAARETZ, Pfeffer A, 'Israel Suffered Massive Cyber Attack during Gaza Offensive', http://www.haaretz.com/israel-suffered-massive-cyber-attack-during-gaza-offensive-1.278094 on 8 January 2017.

History, Andrew E, 'Who Invented the Internet', http://www.history.com/news/ask-history/who-invented-the-internet on 6 January 2017.

History, '9/11 Attacks', http://www.history.com/topics/9-11-attacks on 30 January 2017.

https://home.heinonline.org/titles/American-Law-Institute-Library/Restatement-Third-Foreign-Relations-Law-of-the-United-States-Revised/?letter=R on 27 January 2018.

http://www.nalsarpro.org/CL/Modules/Module4/Chapter-5.pdf on 29 December 2017.

http://www.nato.int/issues/cyber_defence/index.html on 18 August 2017.

https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space on 21 August 2017.

Hughes R B, 'NATO and Cyber Defence: Mission Accomplished?' April 2009, at 1, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , on 19 August 2017.

International Committee of the Red Cross, Customary International Humanitarian Law, 'Introduction, Purpose of the Study', https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_in_puofthst on 7 February 2017.

Kodar E, 'Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I', http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf on 8 January 2017.

Markoff J, 'Step Taken to End Impasse over Cybersecurity Talks', New York Times, July 16, 2010, http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1 on 19 August 2017.

Nato Review Magazine, 'The History of Cyber-attacks: A timeline', http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm on 30 January 2017.

NBC News.com, Security, 'A look at Estonia's Cyber Attack in 2007', http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WJm_J2997IU on 7 January 2017.

Oxford Dictionaries, 'Cyberspace', https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/ on 6 January 2018.

PCWorld News, McMillan R, 'Was Stuxnet Built to Attack Iran's Nuclear Program?' http://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html on 8 January 2017.

Philosophy and Technology, Eilstrup- Sangiovanni M, 'Why the World Needs an International Cyberwar Convention', 21 July 2017, https://link.springer.com/article/10.1007/s13347-017-0271-5> on 29 January 2018.

Rubenstein D, 'Nation State Espionage and its Impacts', http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/ on 22 November 2017.

Stanford Encyclopedia, Lazar S, 'War', https://plato.stanford.edu/entries/war/ on 6th February 2017.

The Guardian, Mueller B, 'Why we need a Cyberwar Treaty' https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty on 29 January 2018.

The New York Times, Austen I, 'Canada Hit by Cyber Attack', http://www.nytimes.com/2011/02/18/world/americas/18canada.html on 8 January 2017.

The New York Times, Technology, Markoff J, 'Before the Gunfire, Cyber Attacks', http://www.nytimes.com/2008/08/13/technology/13cyber.html on 7 January 2017.

'The Russo- Georgian War 2008: The Role of the Cyber Attacks in the Conflict', http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf on 7 January 2017.

Turns D, 'The First Case of Cyber war in Non- International Armed Conflict? The Matrix in Iraq', https://www.asil.org/insights/volume/19/issue/18/first-case-cyberwar-non-international-armed-conflict-matrix-iraq on 7 January 2017.

Understanding the International Criminal Court', https://www.icccpi.int/iccdocs/pids/publications/uicceng.pdf on 29 January 2018.

OAS General Assembly

OAS, *Meeting of ministers of justice or ministers or attorney generals of the Americas,* AG/Res/2040/XXXIV-O/04 (8 June 2004).

OAS, *A Comprehensive Inter-American Cybersecurity Strategy: A Multi-Dimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, AG/Res/2004/XXXIV-O/04 (8 June 2004).

Other UN documents

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

Reports

International Committee of the Red Cross, International Conference of the Red Cross and Red Crescent, *'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', 31, 36–38,* November 28–December 1, 2011.

Sixth Meeting of the Working Group on Cybercrime, 21-22 January 2010, Washington DC.

United States Commander's Handbook on the Law of Naval Operations, 2007.

United States Department of Defence, *'Cyberspace operations (JP 3-12)', Joint Publication 3-12*, 5 February 2013.

United States Department of Defence, *'Department of Defence Strategy for Operating in Cyberspace*, July 2011.

United States Department of Defence, Office of the General Counsel, '*An Assessment of International Legal Issues in Information Operations'*, November 1999.

United States Department of Defense, *'Quadrennial Defense Review Report 37'*, 2010.

SCO General Assembly

SCO, *Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City* (9 July 2009).

UN General Assembly

UNGA, *Creation of a Global Culture of Cybersecurity,* UN A/Res/57/239 (31 January 2003).

UNGA, *Creation of a Global Culture of Cyber security and Taking Stock of National Efforts to Protect Critical Information Infrastructures*, UN A/Res/64/211 (17 March 2010).

UNGA, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Informational Infrastructures*, UN A/Res/58/199 (30 January 2004).

UNGA, *Declaration on the Strengthening of International Security,* UN A/Res/2734 (16 December 1970).

UNGA, *Definition of Aggression*, UN A/Res/3314 (14 December 14 1974).

UNGA, *Developments in the field of information and telecommunications in the context of international security*, UN A/Res/57/53 (30 December 2002).

UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN A/Res/65/201 (30 July 2010).

UNGA, *Report of the Committee of Conferences,* UN A/Res/58/32 (22 September 2003).

UNGA, *Report of the Economic and Social Council - Letter dated 17 February 2004 from the Permanent Representative of Switzerland to the United Nations addressed to the Secretary-General*, UN A/Res/59/61 (24 February 2004).

UNGA, *United Nations Convention on Jurisdictional Immunities of States and Their Property*, UN A/Res/59/38 (2 December 2004).

UNGA, *World Summit on the Information Society,* UN A/Res60/252 (27 April 2006).s

UN Security Council

UNSC S/Res/1368 (12 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.

UNSC S/Res/1373 (28 September 2001) Threats to International Peace and Security Caused by Terrorist Acts.