Lancaster University
Faculty of Arts and Social Sciences
The Law School

The combined application of force under Article 2(4) and Article 51 of the United Nations Charter for cyber warfare: Examining and learning lessons from the Iranian cyber warfare threat to Saudi Arabia

This thesis is submitted for the degree of the Degree of Doctor of Philosophy

MONIRAH FAHAD ALHAMDAN

LL.B in Law (King Saud University)

LL.M in International Law (University of Westminster)

(March 2023)

ABSTRACT

This thesis is written by MONIRAH FAHAD ALHAMDAN on the combined application of force under Article 2(4) and Article 51 of the United Nations Charter for cyber warfare: Examining and learning lessons from the Iranian cyber warfare threat to Saudi Arabia. In the absence of formal international legal regulation on cyber warfare and cyber-attacks, countries must apply the traditional rules for determining whether an armed conflict exists (*jus ad bellum)* to this new type of conflict. Nonetheless, applying *jus ad bellum* norms to this issue is a very controversial matter. Article 2(4) of the UN Charter prohibits using force between states, whereas Article 51 makes an exception for self-defence against an armed attack. To what extent can these Articles be applied to prevent and punish the source of cyber operations? This and other questions will be discussed in this study. The International Court of Justice (ICJ) clarified the use of force in the *Nicaragua* case. Also, it recognised the right of self-defence in customary international law.

Moreover, the present study is timely and significant because of the increased number of 'cyber operations' influencing other states, such as in the long-lasting regional struggle for power between Saudi Arabia and Iran. That regional struggle will provide the backdrop to this thesis, although global examples will also be examined. Also, to understand its responsibility and scope of cyber-attacks, this research will attempt to assess the lawfulness of the Security Council to authorize the use of cyber weapons as a tool to maintain peace and security in the world. This body of research will furthermore look into the *jus ad bellum* norms in Traditional Islamic Rules in a cyber-context.

Moreover, it will help researchers do further research in applying international law norms to cyber operations. This thesis undertakes a robust doctrinal analysis of the existing exalt in this field and proposes some future developments. This thesis will not use measurements of quantity and amounts as its essential tools but instead a qualitative method.

Keywords: International Law, Jus ad Bellum, Cyber Operations, Use of Force, Self – defence, Saudi Arabia, Iran, Cyber Domain, Cyber Security

TABLE OF CONTENTS

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my supervisors, Prof James Sweeney and Prof Catherine Easton for always being there when I needed their support, reviewing my progress constantly, and guiding me through my PhD studies. I would also like to extend my thanks to Prof Skogly Sigrun for her support and encouragement. Finally, but most importantly, I would like to thank my family, my mother and father for their support and trust. And especial thanks to my husband, who was beside me during my entire PhD journey. I really appreciate all of his sacrifices and understanding.

DECLARATION

I declare that this thesis is my own work and has not been submitted in substantially the same form for the award of a higher degree elsewhere. Any sections of the thesis which have been published, or submitted for a higher degree elsewhere, shall be clearly identified.

CHAPTER 1: INTRODUCTION

1.1. Introduction

With the rapid advancement in computer technology, our lives have become increasingly dependent on it. Sophisticated computer devices, tools, and techniques have been a significant part of our lives. Whilst there are many benefits to the technology, there are many downsides too. Whereas technology, arguably, is helping to make the world a better place, it is also making it riskier and prone to security threats.[1] With the very same technology, people we do not know can look into our data without our consent. The same is true for states that are threatened by hackers that can get access to confidential data and leak or otherwise use this information just by using simple computer code. Such type of unauthorised access and hacking of computer data is referred to as a cyber-attack. With the increased popularity of the internet and technology in general, we can see a drastic increase in the number of cyber-attacks.[2] A cyber-attack can happen to anyone and at any time. Although the most common targets of larger-scale cyber-attacks are banks, governmental organisations, and national security systems, as well as social media.[3] A cyber-attack relevant to the *jus ad bellum* is usually one of three types. One has the objective to destroy the target computer system, the second has the aim to gain access to the target computer data, and the third is a Denial-of-Service attack (DOS), which has the aim to slow down the system itself. [4] Irrespective of the type, all cyber-attacks adversely affect people's lives and are potentially dangerous to states. Cyber-attacks can be prevented using antivirus, data encryption, password protection, firewall security, and other security mechanisms. Nevertheless, it is impossible to be fully secure, mainly because cyber threats continue to evolve. The most significant malware, which constituted a revolution in the cyber realm, is

[1] Pawar, M. V. & Anuradha, J. (2015) Network Security and Types of Attacks in Network. Procedia Computer Science, 48, pp.503–506.

[2] Courtney, M. (2017) States of cyber-warfare. Engineering & Technology, 12 (3), pp.22–25.

[3] National Crime Agency Website, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

[4] Waxman, M.C. (1988) Cyber-attacks as Force under UN Charter Article 2(4). International Law Studies, 87, p.15.

Stuxnet.[5] In 2010, this worm attacked the uranium enrichment plant at Natanz in Iran. Iranian officials accused the United States, Israel, and some scientists at Siemens of the attack.[6] Then, in August 2012, there was a cyber-attack using a virus called 'Shamoon' that destroyed the Saudi Aramco computers and networks.[7] Aramco is the largest oil-producing company in Saudi Arabia, and this attack caused enormous damage to its systems: Around 30,000 computers were infected, and many files and data were deleted.[8] An investigation conducted by Kaspersky Lab[9] found evidence suggesting that the sources responsible for this attack were Iran and Hezbollah.[10]

It is obvious from the incidents above that cyber-attacks become more dangerous and advanced every year.[11] This matter is not just a national concern but also needs to be examined from an international law perspective. Several authors undertook

---

[5] A worm is an unwanted software program secretly planted on a computer that enables (among other things) someone other than the owner to control it. The name "Stuxnet" is an anagram of letters found in parts of its code. Also, it is defined by the U.S. Army Information Assurance Training Center, Malware is an acronym that stands for Malicious Software and it comes in many forms. Generally speaking, malware is software code or snippets of code that is designed with malice in mind and usually performs undesirable actions on a host system.

[6] Fildes (n 4).

[7]'It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable' http://www.symantec.com/connect/blogs/shamoon-attacks.

[8] C Bronk, E Tikk-Ringas, 'The Cyber-Attack on Saudi Aramco', IISS (April 2013), <www.iiss.org/en/publications/survival/sections/201394b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08bronkandtikk-ringas-e272>

[9] One of the world's fastest-growing cybersecurity companies: http://me.kaspersky.com/en/about.

[10]Paganini, P., 'Iran Suspected for the Attack on the Saudi Aramco' (20 Aug. 2012). <www.securityaffairs.co/wordpress/8300/malware/iran-suspected-for-the-attack-on-thesaudi-aramco.html>. Iran is suspected in the attack on the Saudi Aramco.

[11] Panel Julian Jang, JaccardSuryaNepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014, Pages 973-99.

research on cyber-attacks and how to apply international law rules to them, specifically on how to use *jus ad bellum* in cyber operations, which is this thesis' main scope.[12] By reference to primary and secondary legal sources, this thesis will examine how *jus ad bellum* rules can be applied to cyber operations conducted by Saudi Arabia and examine Saudi regulations and its international practice.

1.2 Contours of Current Research into Cyber Warfare

In 2013, twenty law scholars drafted a Manual on the international law applicable to cyber warfare called "Tallinn Manual." It contains ten suggested rules for applying *jus ad bellum* in cyber warfare.[13] This Manual can offer direction both for the UN and individual states alike. Although not all of the rules in the Manual have been universally accepted, it can be considered as a massive step towards united international rules for cyberspace. The Tallinn Manual 1.0 addressed cyber operations in the *jus ad bellum* and jus *in bello* context. Then, in 2017, the same international experts published a second edition, "Tallinn Manual 2.0". Like the first edition, the second one addresses the ability to apply international legal norms to cyber operations in wartime by examining *jus ad bellum* and *jus in bello* rules. However, Tallinn 2.0 also addresses the use of international law norms in the cyber context in peacetime. Consequently, Tallinn 2.0 is more detailed and has more extensive commentary, unlike the first edition. Moreover, it discusses incidents that do not rise to the level of use of force. Furthermore, the Tallinn Manual 2.0 refers to customary international law more than the previous edition.

Due to the importance of the Tallinn Manual, chapter two will primarily use it as a foundation when assessing the use of force and self-defence in cyber space. The chapter will first examine Article 2 (4) of the UN Charter (the prohibition of the use of force) as well as the corresponding customary law principles. It will be first established how these international law principles can be applied to cyber operations. Then, the chapter will continue with analysing four possible approaches

[12] Such as Michael M. Schmitt, Marco Rocsini and Terry Gill.

[13] Michael N Schmitt (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) [hereinafter Tallinn Manual].

to determine the applicability of self-defence to cyber operations: the instrument-based approach, the weapon assessment, the consequence-based approach, and the target-based approach. Furthermore, the chapter will examine the threat of force and the use of force and armed attack relationship in the cyber context. The last part of the chapter deals with Article 51 (self-defence) in cyber space and investigates anticipatory self-defence and then, more broadly generally, self-defence in cyber space. In order to this, subsections will deal with cyber armed attack, the accumulation of events in cyber space, self-defence against cyber-operations conducted by non-state actors, the concept of necessity and proportionality, and lastly immediacy and imminence.

This thesis will then commence with chapter three, which focusses on state responsibility. At first, it will examine the principle of non-intervention and state responsibility in relation to cyber-space. Further, the related subsections will investigate both lawful intervention, and intervention by invitation. The next section will then deal with state sovereignty and cyber space; particularly, the question if and how sovereignty can be applied to cyber-space will be addressed there. The following sections address due diligence, the attribution of state responsibility to cyber-operations, and precluding the wrongfulness of the act. In this context, the author also explores countermeasures and necessity. Lastly, chapter three will examine the obligation of states concerning internationally wrongful acts and due diligence before concluding.

The next chapter, which is chapter four, will apply all of the previously discussed rules studied in chapter two and three to selected major cyber-operations. The first section will be about Estonia DDoS, the second about the Stuxnet attack, and lastly, the third section about the Aramco Attack.

The fifth chapter analyses the UNSC’s role in cyber operations. It discusses the potential possibilities the UNSC has to intervene to maintain international peace and security. Afterwards, the author studies how the UNSC responds to cyber-attacks. Then chapter five closes by examining the UNSC’s ability to use cyber operations as a sanction. Finally, the last chapter will conclude the findings of this thesis and offer some recommendations as well as avenues for future research.

1.3 Key Terms

This section will explain and define some relevant terms for this thesis.

Botnet: “A network of compromised computers, so-called ‘bots’, remotely controlled by an intruder, ‘the bothered’, used to conduct coordinated cyber operations, such as ‘distributed denial of service’ operations (see below). There is no practical limit on the number of bots that can be assimilated into a botnet.”[14]

Cloud Computing: “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing allows for efficient pooling of computer resources and the ability to scale resources to demand”.[15]

Computer Emergency Response Team (CERT): “A team that provides initial emergency response aid and triage services to the victims or potential victims of ‘cyber operations’[16] (see below) or cyber-crimes, usually in a manner that involves coordination between the private sector and government entities. These teams also maintain situational awareness about malicious cyber activities and new developments in the design and use of ‘malware’ (see below), providing defenders of computer networks with advice on how to address security threats and vulnerabilities associated with those activities and malware.”[17]

Computer Network: “An infrastructure of interconnected devices or nodes that enables the exchange of data. The data exchange medium may be wired (e.g., Ethernet over twisted pair, fibre-optic, etc.), wireless (e.g., Wi-Fi, Bluetooth), or a

[14] Hanna KT, Lutkevich B and Wright R, “What Is Botnet?” (SecurityMarch 30, 2021) <https://www.techtarget.com/searchsecurity/definition/botnet > [accessed February 13, 2023].

[15] The National Institute of Standards in Technology, US Department of Commerce, definition of Cloud Computing, Special Publication 800-145, September 2011 563.

[16] Sullivan P, “What Is CERT?” (*WhatIs.com* March 18, 2021) <https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team > [accessed February 13, 2023].

[17] Ibid.

combination of the two. Computer System: One or more interconnected computers with associated software and peripheral devices. It can include sensors and/or (programmable logic) controllers, connected over a computer network. Computer systems can be general purpose (e.g. a laptop) or specialised (e.g. the 'blue force tracking system')."[18]

Critical Infrastructure: "Physical or virtual systems and assets of a state that are so vital that their incapacitation or destruction may debilitate a state's security, economy, public health or safety, or the environment."[19]

Cyber: "Connotes a relationship with information technology."[20]

Cyber-attack: "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[21]

Cyber Espionage: "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information."[22]

Cyber Operation: "The employment of cyber capabilities to achieve objectives in or through cyberspace."[23] (see also 'cyber activity').

Cyberspace: "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[24]

---

[18] Gillis AS, "What Is a Computer Network?" (*Networking*December 20, 2019) <https://www.techtarget.com/searchnetworking/definition/network> accessed February 13, 2023

[19] Editor CSRCC, "Critical Infrastructure - Glossary: CSRC" (*CSRC Content Editor*) <https://csrc.nist.gov/glossary/term/critical_infrastructure> accessed February 14, 2023

[20] Beal V, "What Is Cyber?" (*Webopedia*June 23, 2021) <https://www.webopedia.com/definitions/cyber/> accessed February 14, 2023

[21] Tallinn Manual. Rule 92. 415.

[22] Ibid, Rule 32,168.

[23] Editor CSRCC, "Cyberspace Operations (CO) - Glossary: CSRC" (*CSRC Content Editor*) <https://csrc.nist.gov/glossary/term/cyberspace_operations> accessed February 14, 2023

[24]"Cyberspace"(*Cyberspace-CIPedia*) <https://websites.fraunhofer.de/CIPedia/index.php/Cyberspace> accessed February 14, 2023

Data: “Computer data is information that is stored and processed digitally on a computer. Data on a computer can take many forms, including text, images, audio, or video.”[25]

Database: “A collection of interrelated data stored together in one or more computerized files”.[26]

Denial of Service (DoS): “is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected”.[27]

Distributed Denial of Service (DDoS): “a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.”[28]

Hacktivist: “A private citizen who on his or her own initiative engages in hacking for, inter alia, ideological, political, religious, or patriotic reasons.”[29]

Internet: “A global system of interconnected computer networks that use the Internet Protocol suite and a clearly defined routing policy.”[30]

---

[25] Pickle B and Christensson P, “Data” (*Definition*December 13, 2022) <https://techterms.com/definition/data> accessed February 14, 2023

[26] Software Engineering Technology, Institute of Electrical and Electronics Engineers (IEEE) Std 610.12 (28 September 1990).

[27] read 3min., “What Is a Denial of Service Attack (Dos) ?” (*Palo Alto Networks*) <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos> accessed February 14, 2023

[28] “What Is a Distributed Denial-of-Service (Ddos) Attack? - Cloudflare” <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> accessed February 14, 2023

[29] (*Hacktivismo - CCN-stic 401*) <http://www.dit.upm.es/~pepe/401/4660.htm#!-alone> accessed February 14, 2023

[30] World Telecommunication /ICT Policy Forum 2013, Document WTPF-13/INF/8-E, Defining the Internet, Geneva.

Internet Protocol (IP) Address:" A unique identifier for a device on an IP network, including the Internet."[31]

Phishing:" A type of social engineering attack most commonly executed by the use of email, social networks, or instant messaging. The perpetrator attempts to lure unsuspecting victims into visiting a malicious website, opening an infected document, or executing actions on behalf of the attacker. The purpose of a phishing operation is generally to acquire sensitive information, such as user credentials, personal data, or credit card details."[32]

Server: "is a computer, a device or a program that is dedicated to managing network resources. They are called that because they "serve" another computer, device, or program called "client" to which they provide functionality.".[33]

Software: "Software is a set of programs (sequence of instructions) that allows the users to perform a well-defined function or some specified task."[34]

Spoofing: "is a type of scam in which a criminal disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source.".[35]

Virus: "A type of 'malware' (see above) with self-replicating capability that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence."[36]

---

[31] Internet Assigned Numbers Authority, Glossary of terms available at: www.iana.org/glossary.

[32] "What Is Phishing: Attack Techniques & Scam Examples: Imperva" (*Learning Center*June 17, 2020) <https://www.imperva.com/learn/application-security/phishing-attack-scam/> accessed February 14, 2023

[33] "What Is a Server? - Definition from Techopedia" (*Techopedia.com*) <https://www.techopedia.com/definition/2282/server> accessed February 14, 2023

[34] "What Is Software in Computer? Types and Examples - Javatpoint" (*www.javatpoint.com*) <https://www.javatpoint.com/what-is-software> accessed February 15, 2023

[35] Folger J, "What Is Spoofing? How Scam Works and How to Protect Yourself" (*Investopedia*November 3, 2022) <https://www.investopedia.com/terms/s/spoofing.asp> accessed February 15, 2023

Website: “is a collection of interlinked pages on the internet grouped under a unique name or online address. These pages, known as web pages, contain information or services by a business or organization. The information may be in different formats like text, images, videos, audio, and animation and the services may be like buying or selling products, downloading digital products, etc.”[37]

Wi-Fi: “a wireless networking technology that uses radio waves to provide wireless high-speed Internet access.” [38]

Worm:” A type of ‘malware’ (see above) that is able to self-replicate and autonomously spread across ‘computer networks’ (see above), unlike a virus that relies on embedding in another application in order to propagate to other computer systems.”[39]

1.4 Aims and Objectives

The objective of this thesis is to conduct a detailed study on how to apply the law of on the use of force (*jus ad bellum*) to cyber warfare by studying Articles 2(4) and 51 of the UN Charter, as well as customary international law. The research will focus on how international law addresses, and in the absence of clear rules could address, cyber conflict in the light of the meaning of ‘use of force’ in Article 2(4), and how, based on Article 51, Saudi Arabia could act in self-defence against cyber-attacks. Based on the unfriendly relationship between Iran and Saudi Arabia and the precedent of the Saudi Aramco cyber-attack, there is a threat in cyber domain that

---

[36] “Computer Virus” (*Computer Virus - an overview | ScienceDirect Topics*) <https://www.sciencedirect.com/topics/engineering/computer-virus> accessed February 15, 2023

[37] Editorial SS, “What Is a Website & How Does It Work? (Easy Beginner's Guide)” (*SiteSaga*September 26, 2022) <https://www.sitesaga.com/what-is-a-website/> accessed February 19, 2023

[38] “WIFI Definition and Meaning” (*Washington Technology Solutions*) <https://watech.wa.gov/WiFi-definition-and-meaning> accessed February 19, 2023

[39] Bedell C, Loshin P and Hanna KT, “What Is a Computer Worm and How Does It Work?” (*Security*September 13, 2022) <https://www.techtarget.com/searchsecurity/definition/worm> accessed February 20, 2023

needs to be studied. Moreover, there needs to be a clear legal framework for responding to such attacks in the future. This study aims to achieve this goal by identifying a number of examples of state practice regarding cyber-attacks and by analysing them (as well as opinio juris). Additionally, this thesis will illustrate existing Saudi Arabian regulations in the field of cyber security and how they comply with international rules.

As Saudi Arabia started to work on building a local Command, Control, Communications, Computer and Intelligence System (C4i system), there is an urgent need to study cyber threats and security from a legal perspective. Until now, such threats have mainly been studied from a technical viewpoint. Besides, there are some newly established institutions dealing with cyber security, such as the Saudi Federation for Cyber Security and Programming, the College of Cyber Security Studies, and the Saudi National Cyber Security Centre (NCSC) which was already established in February 2017. Therefore, this research is very important and aims to assist the Saudi Arabian government in their upcoming National Cyber Strategy and cyber development. It is vital to understand the threats in order to plan a good and lawful strategy, which is one of the thesis's aims. Another is studying Iranian threats and offering some perspective for lawful future responses.

This research aims to provide a legal description for and an analysis of the terms and conditions under which self-defence can be used lawfully against cyber-attacks. Furthermore, this research will discuss the legality of anticipatory self-defence against cyber operations, as well as the problems of attribution, especially when the perpetrator is a non-state actor. Cyber sovereignty is another matter which will be addressed in this thesis. It will deal with the state responsibility for cyber-attacks and the complex relationship between states and non-state actors. This research will further attempt to assess the probability of the Security Council to use cyber 'weapons' as a tool to maintain peace and security when exercising their rights under Articles 41 and 42 of the UN charter. Furthermore, the thesis will assess the possibility of using cyber 'weapons' as a sanction by applying the same method used in the nuclear weapons case.

Additionally, this research will contribute to the literature by providing an academic reference addressing the legal aspects of offences against and the right to defend in

cyberspace, specifically in relation to Saudi Arabia. Currently, there is no such research available in the English language. No scholar has so far discussed the Saudi-Irani cyber warfare from an international law perspective – therefore, this is the most significant contribution of this research.

The findings of this study may also be utilised by relevant interested parties, such as Saudi government bodies, non-governmental organisations, cyber law researchers and others in their aim to analyse and study the application of international law in the cyber realm. Moreover, this research will help the Saudi Arabian government to decide how to apply existing international law rules to cyber operations and illustrate where improvements are needed in the national legislations.

This research will encourage Saudi Arabia to engage in international cooperation regarding cyber security both regionally with gulf countries, and with NATO countries. It will make them aware of the threats and the requirement of immediate actions to strengthen its deterrence and be ready for any attacks. This research will also assist in knowing the proper time for using self-defence in the most efficient way.

This area of research is still a grey zone which needs to be studied more, especially in our contemporary world, and that what makes this study valuable for the subject.

There are some scholars who wrote valuable works in the cyber security field, such as Michael Schmitt. He was the first scholar who investigated applying international law rules to cyber operations. He listed seven factors to determine if a 'particular cyber event constitutes force' which are: severity, immediacy, directedness, invasiveness, measurability, presumptive legitimately and responsibility. Schmitt also provides a critical argument regarding the harm caused by a cyber-attack. According to his analysis, the harm must physically manifest to constitute an armed attack.[40]

Roscini noted in his book, Cyber operations and the use of force in international law, that "A cyber operation could go as far as to disable power, generators, cut off the military command, control and communication systems, cause trains to derail and aero planes to crash, nuclear reactors to melt down, pipelines to explode, weapons

[40] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law.

to malfunction banking systems to cripple."[41] He discussed the ability of applying jus in bello and jus ad bellum to cyber operation.

This thesis is significantly different to Schmitt's and Roscini's works because it studies the ability of applying international law norms to cyber operation in Saudi Arabia. Also, unlike those two authors, it will focus on the Iranian threat in the cyber realm. Moreover, it will study the role of the Security Council in cyber warfare and the ability of it to use the cyber operation as a sanction. It also differs from Gray (International law and the use of force)[42] in applying the use of force rules to cyber operations. Therefore, this thesis positions itself in a place between Schmitt, Roscini, and Gray, which will enrich the international law literature in the area of cyber security and cyber warfare.

Saudi Arabia defines in Article 1 of its constitution that "Constitution: The Holy Qur'an and the Prophet's Sunnah (traditions)." As this thesis will refer to Saudi Arabia, it is important to also look into Islamic Legal Traditions. There are many rules in Islam regulating the use of force and permitting the state to use self-defence with conditions and limitations. All of that will be discussed in this thesis in the context of cyber operations, which will contribute to the legal literature in this area.

1.5 Research Methodology

The method that will be used to carry out this research is doctrinal analysis. Doctrinal means 'a research process used to identify, analyse and synthesise the content of law'.[43] This type of method includes the 'doctrinal restatement' and the 'recasting project,' which includes intellectual contributions.[44]

This research will carry out this methodology in three steps. First, it will examine the legal rules and regulations relating to the use of force and cyberwarfare and conduct

[41] Roscini, M., Cyber operations and the use of force in international law. Oxford University Press, 2014.

[42] Gray C, International law and the use of force , Oxford University Press, Third Edition, 2008.

[43] D Watkins, M Burton, Research Methods in Law (Routledge 2013), 10.

[44] Ibid. at 11.

a literature review of the most remarkable writers' works in this field, such as Schmitt[45], Koh[46], Waxman[47], Banisar[48], and Zetter[49].

This will include analysing conference papers, journals Articles, trends, and cyber security strategy, which will provide a comprehensive understanding of how world leaders intend on solving the problem, thus providing guidance for the most practical and efficient solutions. Moreover, ICJ decisions and advisory opinions regarding the 'use of force' and 'self-defence' will be considered. The main source of this study that may be categorised as a black-letter law is the *Tallinn Manual*, which contains many rules and expert commentary on cyberwarfare.

Data collection for this thesis will be widened to also include publications from relevant government institutions as well as information agencies that can provide accurate data and familiarise the researcher with the realities of governments' cyber practices. The thesis will collect data from the Centre of Excellence (COE), NATO Cooperative Cyber Defence (CCD), United Nations specialised agency for information and communication technologies – ICTs, the International

[45] Michael N Schmitt 'Professor of Public International Law at Exeter Law School and a member of Exeter University's Strategy and Security Institute, Professor Schmitt is the Charles H. Stockton Professor and Director of the Stockton Center for the Study of International Law at the United States Naval War College in Newport, Rhode Island. He is also a Fellow at Harvard Law School's Program on International Law and Armed Conflict, Senior Fellow at the NATO Cyber Defence Centre of Excellence, and General Editor of International Law Studies' http://socialsciences.exeter.ac.uk/law/staff/mschmitt/.

[46] Harold Hongju Koh 'is Sterling Professor of International Law at Yale Law School. He returned to Yale Law School in January 2013 after serving for nearly four years as the 22nd Legal Adviser of the U.S. Department of State' https://www.law.yale.edu/harold-hongju-koh.

[47] Matthew Waxman ' is an expert in national security law and international law, including issues related to executive power; international human rights and constitutional rights; military force and armed conflict; and terrorism'
http://www.law.columbia.edu/fac/Matthew_Waxman.

[48] 'He has worked in the field of information policy for nearly 20 years on the intersection of human rights and ICTs including privacy, freedom of expression, cyber-crime and the right to information' http://cyberlaw.stanford.edu/about/people/david-banisar.

[49] Kim Zetter ' is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and security' http://www.wired.com/author/kimzetter/.

Telecommunication Union and the Internet Corporation for Assigned Names and Numbers (ICAAN). Data will also be collected from related Saudi Arabian sectors, for example, King Abdul-Aziz City for Science and Technology, the Interior Ministry, the National Centre of Electronic Security, the Communications and Information Technology Commission, C4i Centre For Advanced System, and the Ministry of Defence. Thus, this research encompasses theoretical as well as practical sources.

Finally, the texts will be interpreted and analysed while observing and assessing state practice. Initially, the main rules in this study, Articles 2(4) and 51, will be analysed in an attempt to close the gap between these Articles and their applicability in the cyber realm. It is necessary to provide an explanation of any difficulties that may arise for governments facing sudden cyber-attacks. Also, the paper will analyse Iranian and US practices in dealing with cyber-attacks and if and how they comply with international law rules. This research will study the Saudi Aramco attack, as the focus of this study is cyber threats to Saudi Arabia. In this part, there is a need to use the deductive logic, inductive reasoning, and analogy.[50]

It is obvious from the steps mentioned above that this thesis will not use measurements of quantity and amounts as its basic tools, but instead a qualitative method.[51]

[50] Ibid.

[51] F Aynalem, K Vibhute, Legal Research Methods (Justice and Legal System Research Institute, 2009), 17.

CHAPTER 2: THE USE OF FORCE AND SELF-DEFENCE IN CYBER SPACE

2.1 Introduction

This chapter is the foundation for all consecutive chapters. It will examine the prohibition of the use of force and its exceptions such as the right to self-defence both in conventional international law and in cyber operations. It will help in getting a full picture of the law on cyber operations, because of that, there is a need to go beyond the jus ad bellum. To achieve this, sections in this chapter will first discuss the general international law rules for kinetic attacks, and then discuss the possibility of applying these laws to the cyber context.

The main source for the cyber analysis in this chapter is the Tallinn Manual, which is the only collection of suggested rules for cyber operations available on the international level. Nevertheless, there are some domestic proposals as well. In the International Strategy for Cyberspace of the United Stated (2011), the White House stated that "…the development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace".[52] This statement clearly is in favour of applying international law to the cyber space, and therefore is an example of state practice in this regard. Moreover, in September 2019, the French Ministry of Defence published a document, describing its views on how international law applies in cyberspace.[53] Additionally, the Dutch Minister of Foreign Affairs, explained the view of the Government on international law's

[52] The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, Washington, (2011), 9.

[53] Roguski, P, France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I, Opinio Juris (24 September 2019).

applicability in cyberspace in a letter to the Dutch Parliament in July 2017.[54] All these documents and declarations indicate that these states are in favour of applying international law, which includes the prohibition on the use of force, in cyber space. However, the Tallinn Manual was the most detailed document in this regard.

The prohibition of the use of force was codified in Article 2 (4) of the UN Charter, which states that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations".[55] However, that principle is not the only one which protects a state's integrity. There is also the exception to this principle, which is the right to use self-defence, which stated in Article 51 of the United Nation Charter.[56] The right of self-defence cannot be used by the victim state without restrictions, there are some conditions and requirements to adhere to. Primarily, self-defence needs to be used proportionately and there needs to be necessity. Alas, these conditions will be assessed in detail in a later section on the exercise of self-defence. Another matter in this regard is 'anticipatory self-defence'[57], which means 'the right to take forcible measures against a threat before the attack is actually launched'. International law allows anticipatory self-defence in one particular instance: if an attack is imminent, "instant, overwhelming, leaving no choice of means, and no moment of deliberation" (Caroline Doctrine). That means that a state may use force to defend itself first if there is clear evidence that an enemy attack is about to happen and there are no other means like negotiations possible. Although international put some strict rules on when anticipatory self-defence is allowed, there are some states who practice it more liberally. For example, the United States recognised the right of "pre-emptive self-defence" after the 9/11 incident.[58] The US's definition recognises self-defence even without "imminence" and is not supported by customary international law or any

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

[55] Charter of the United Nations, Ibid.

[56] Ibid.

[57] Gill TD and Duchene PAL, 'Anticipatory Self-Defence in the Cyber Context' (2013) 89 Int'l L. Stud. 438.

[58] Ibid.

other source of international law.[59] Nevertheless, the question is what the required level of 'imminence' is for cyber which would permit the anticipatory use of self-defence.

In addition, the principle of non-intervention, is a very significant principle which "restricts the ability of outside nations to interfere with the internal affairs of another nation. At its core, the principle is a corollary to the right of territorial sovereignty possessed by each nation"[60]. The non-intervention principle comes into play in the case of acts which do not amount to a use of force or an armed attack. This principle will be useful in examining some cyber operations which do not rise to the use of force level, but who do qualify an internationally wrongful act. An example thereof would be manipulating an election outcome by sending emails to voters.[61] Such an operation would not be considered as a use of force, but it would still be prohibited in international law because such an action would be an intervention in another state's internal matters. Moreover, the victim state would have the option to respond to this act, e.g., by asking the ICJ to adjudicate the matter and protect its territory from these types of operations. However, this principle has not been settled regarding cyber operations. It also not yet settled whether the principle of non-intervention includes just military intervention or also economic, political, and cyber intervention.[62] Furthermore, the non-intervention principle is closely related to the prohibition of the use of force principle. This has been detailed in the United Nations General Assembly Resolutions No. 2625[63] and No. 3314[64] as well as by the

[59] Ibid.

[60] Dubay C. , A Refresher on the Principle of Non-Intervention , International Judicial Monitor , Spring 2014 Issue , <http://www.judicialmonitor.org/archive_spring2014/generalprinciples.html> accessed 09 July 2019.

[61] Tallinn Manual, 45.

[62] Ibid.

[63] See UNGA Res 2625 (XXV) (24 October 1970) 'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations.

[64] See art 3, subparagraph g) of UNGA Res 3314 (XXIX) (14 December 1974) 'Definition of Aggression'.

International Court of Justice in the Nicaragua case and in the Armed Activities case.[65]

To provide context, it will be considered what type of attack constitutes a use of force and could be considered as an armed attack. In addition, the thesis will propose a framework for jus ad bellum principles, which will later be used in analysing several cyber-attacks incidents in chapter 4. The first part of this chapter will discuss the prohibition of use of force in international law as set out in Art. 2 (4) of the UN Charter. This examination is followed by an analysis of the relevant rules regarding the threat of force, and a discussion on the relationship between the use of force and armed attack. The chapter concludes with a thorough analysis of the right to self-defence and how this can be applied in cyber space.

2.2 Art. 2 (4) - The prohibition of the use of force

Jus ad bellum is defined as "a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception".[66] The examination of the law of conflict is the key point to understand the use of force scope and limitation. This understanding will help in applying the jus ad bellum rules to cyber operations and to know when and how such operations constitute a use of force. The attempt to regulate the use of force has begun at the Peace of Westphalia. More earnestly, the League of Nation, after the First World War, has also tried to do so by adopting it within its Covenant. It included a prohibition to resort to war only against any state that received a judicial decision, arbitral award, or a unanimous award of the council.[67] Consequently, the international community agreed on the Geneva Protocol for the Pacific Settlement of International Disputes in

[65] Nicaragua Case, (para 187 ff).

[66] A Roberts, R Guelff, Documents on the laws of war, 3rd ed., New York: Oxford University Press, (2000). at 2-3.

[67] Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus, The Charter of the United Nation: A commentary,(Nov 2012), 2 OUP, at 110.

1924.[68] In 1928, the Briand-Kellogg pact was adopted. It was an agreement between 15 nation states to regulate the use of force. It stated in Article 1 that "The High Contracting Parties solemnly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies, and renounce it, as an instrument of national policy in their relations with one another."[69] This treaty constituted the first binding rules to regulate the resort to war. Much later, this prohibition became customary international law.[70] Unfortunately, the League of Nations was unsuccessful in the prohibition to resort to war.[71] Largely, because of the ineffective support of the United States, the United Kingdom and France. This was particularly evident in the unsuccessful attempt to terminate Germany's aggression in 1939.[72]

After the United Nation was established in 1945, the Charter of the United Nation forbade the use of force in Article 2(4) by stating that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations"[73]. The ICJ in Armed Activities on the territory of Congo declared that Article 2(4) is a cornerstone of the United Charter.[74]

With regard to the argument on the definition of force according to Article 2(4), during the Cold War many commentators from the United Stated noted that the interpretation of Article 2(4) relied on the effective functioning of the United Nation collective security system.[75] In the case of Corfu Channel[76], The ICJ rejected the UK's broad interpretation of Article 2(4) and claims of self-help. The ICJ stated that:

---

[68] Ibid.

[69] General Treaty on the renunciation of war as an instrument of national policy. Signed at Paris, August 27, 1928.

[70] Simma ,The Charter of the United Nation: A commentary, Ibid at 110-111.

[71] Ibid

[72] Ibid

[73] Charter of the United Nations, (24 October 1945),Ibid.

[74] ICJ Reports (2005) 168, at para 148, 45 ILM (2006) 271.

[75] C Gray, International law and the use of force, Ibid,31.

[76] Corfu Channel Case, Ibid.

"…the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and such as cannot, whatever be the present defects in international organization, find a place in international law. Intervention is perhaps still less admissible in the particular form it would take here; for, from the nature of things, it would be reserved for the most powerful States."[77]

In this regard, Israel as well took a similarly exaggerated interpretation of the Article in Entebbe incident in 1976, but this claim was rejected by many states such as Sweden.[78] In the Grenada case in 1983, the Security Council suggested that "They provide justification for the use of force in pursuit of other values also in this right in the charter, such values as freedom, democracy, peace."[79] Riesman and Baker have noted that:

"Both the Charter, and its reformulations by the Assembly and customary conceptions of international law with regard to the use of the military instrument rested on a set of inherited assumptions about how military conflict is conducted: conflict is territorial, between organized communities. Changes in military technology and political dynamics made many of the key assumptions underlying the basic rules about when and how to use force obsolete."[80]

Also, Schmitt noted in this regard that "because the Charter is the constitutive instrument of an international organization, flexibility in interpretive spirit is apropos."[81] Therefore, this flexibility is demanded in the interpretation because the Charter will be applied in any upcoming cases and issues which need a type of interpretation which be appropriate and applicable in any place and any time. As commented by Schachter "This flexibility does not mean that the rules lack any

[77] ICJ Reports (1949) 4 at 34.

[78] C Gray, International law and the use of force, Ibid32.

[79] Security Council 2491st meeting (1983), para 53, 1983UNYB 211.

[80] W Riesman, J Baker, Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law. Yale University Press, (1992). , at 41.

[81] Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, (1999),3 7 C.J.T L. 885, 904.

content".[82] The reason for the variety of interpretations is because Article 2(4) does not explain what constitutes a "use of force". For example, a blockade is classified as a use of force based on the instrument assessment. On the other side, it only can be a use of force if it has a similar effect of economic sanctions based on the effect-based analysis.[83] The ICJ has adopted an expansive approach with regard to the instrument-based analysis, as it does not refer to specific weapons. E.g., it also considered economic and political coercion as a use of force. In the ICJ advisory opinion on the Threat or Use of Nuclear Weapons,[84] the court stated that "…they apply to any use of force, regardless of the weapons employed ... The Charter neither expressly prohibits, nor permits, the use of any specific weapon."[85]

Moreover, In Nicaragua v. United States, the ICJ has adopted the effect-based analysis when assessing the United States' activities: it held that some of them, such as laying mines in Nicaragua's territorial water, qualified as a use of force.[86] On the other hand, the United States' provision of funds did not rise to the level of use of force.[87] In this case, the ICJ stated that the prohibition of use of force in Article 2(4) has its origin in customary international law.[88] Indeed, customary international law prohibits the use of force based on the instrument analysis.[89] Moreover, the Friendly Relations Declaration has adopted a wider interpretation for Article 2(4). This declaration has prohibited any form of coercion: "Recalling the duty of States to refrain in their international relations from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of

[82] Oscar Schachter, In Defence of International Rules on the Use of Force, 53 U. CHI. L. REV. 113, 127 (1986), 121.

[83] C Gray, Use of Force in International law, Ibid.

[84] Legality of the Threat or Use of Nuclear Weapons, (Advisory Opinion), 8 July 1996, ICJ Reports, 1996 ('Nuclear Weapons'), para 39.

[85] Ibid.

[86] Nicaragua Case, 146.

[87] Ibid 228.

[88] Ibid 147.

[89] A Moore, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law and Potential Models." (2015), Naval L. Rev 64, 9.

any State".[90] This means that coercion could, in some instances, be considered a use of force. Some scholars argue

'[…] under what conditions the intrusion or otherwise uninvited presence of military (or even police organs) on foreign soil without actual fighting amounts to a use of force, and, to mention another example, whether a minimal use of coercion, such as the arrest of a person, the seizure of a foreign fishing vessel, or the opening of a diplomatic bag, could constitute a use of force.'[91]

Consequently, if one uses the Friendly Relations Declaration to make sense of the concept of use of force, as some scholars do, this extended interpretation of Article 2(4), also includes all forms of coercion (from military to political or economic coercion) and therefore even leaves a space for any other form of coercion.[92] As a result, this could include cyber operations which are "aimed against the political independence or territorial integrity". This effect of cyber operations may occur when the operation has been launched from a third state's territory.[93] In this case, the territorial state could be found responsible based on the unable and unwilling assessment. This argument will be further investigated in Chapter Four when examining cyber operations in which non-state actors were involved.

In the context of defining the use of force, there is another aspect to defining and describing what acts could be categorised as force. The "aggressive use of force" has been defined by Sharp as "a shorthand term used to refer to any use of force within the meaning of Article 2(4) that is not justified by a state's right of self-defence or authorized by the Security Council under its coercive Chapter VII powers."[94] Moreover, General Assembly Resolution 3314[95] has defined aggression

---

[90] The United Nations General Assembly Resolution 2625, "The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States" was adopted by the General Assembly on 24 October 1970, during a commemorative session to celebrate the twenty-fifth anniversary of the United Nations.

[91] Kreß, C. 'The International Court of Justice and the principle of non use of force' pp. 574-575, in Weller, Marc, Alexia Solomou, and Jake William Rylatt, eds. *The Oxford Handbook of the use of force in international law*. OUP Oxford, 2015.

[92] Ibid.

[93] Roscini, Ibid, 44.

[94] Sharp, W.G., Cyberspace and the Use of Force, Aegis Research Corporation, (1999)., 33.

in its first Article as "…the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."[96]

It is obvious from this definition that the resolution has linked aggression to armed force. Moreover, Article 3 lists some examples of attacks by armed forces which are considered as a use of force, such as invasion of a state's territory, bombardment and blockade.[97] Yet, the General Assembly has been clearer when explaining what constitutes a use of force.[98] Gray has described the Security Council's role in this regard by saying that :"[t]he Security Council clearly has an important role, but there is controversy as to whether its findings are conclusive as to legality, illegality, and as to the content of the applicable norm."[99] Some scholars such as Sharp suggest that the United Nation Charter provision could be helpful in the interpretation of Article 2(4).[100] For instance, Article 41 of the Charter lists some measures which are not considered a use of force: "These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[101] Also, Article 42 states that "such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."[102]

The post-charter practice proved that the international community has agreed that military invasion is considered a use of force. However, they did not reach unanimous consent on other types of acts. As Professor Schachter states, "No State has ever suggested that violations of Article 2(4) have opened the door to the free

---

[95] Definition of Aggression, G.A. Res. 3314 (XXIX), arts. 1, 3, 4. U.N. Doc. A/3314 (Dec. 14, 1974).

[96] Ibid, Art 1.

[97] Ibid, Art 3.

[98] SHI Jiuyong, Prohibition of Use of Force in International Law, Chinese Journal of International Law (2018) 17(1): 1-14.

[99] Gray C, International law and the use of force, Ibid,17.

[100] Sharp, W.G., Cyberspace and the Use of Force, Aegis Research Corporation, Ibid.

[101] Charter of the United Nations, (24 October 1945),Ibid, Article 41.

[102] Ibid, Art 42.

use of force".[103] This is essential as state practice is one element of customary international law and therefore very important because if it is accompanied by opinio juris, it will become binding customary law.[104] There are other grounds for using force and intervening in another state, such as interventions to reinstate democracy or humanitarian interventions. However, this thesis will not assess them because they are beyond the scope of this thesis.

2.3 Applicability of established international law rules in cyber operations

While the previous sections examined the rules on the use of force in international law, this part, studies these rules in a cyber context and applies them to cyber operations. Further, it will help explain why cyber operations can qualify as use of force. The Tallinn Manual, in Rule 68 identifies the types of cyber operations the Group of Experts considers a threat or use of force: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[105] This rule is a reflection of Article 2 (4) of the United Nation Charter, which is derived from and reflected in customary international law.[106] Even though the Article prohibits the threat or use of force which

[103] Schachter O., Self-Help in International Law: U.S. Action in the Iranian Hostage Crisis, 131.

[104] SHI Jiuyong, Prohibition of Use of Force in International Law, Ibid, 3.

[105] Tallinn Manual, 2017, 329.

[106] "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Art. 2 (4) United Nation Charter.

is against the territorial integrity or political independence of any state, it adds the additional classification “any other manner inconsistent with the purposes of the United Nations” as an act amounting to the use of force to the customary rule. This addition can be interpreted broadly and therefore potentially widens the scope for defining the use of force.

In fact, to interpret the meaning of the term “force” which is stated in the United Nation Charter, one needs to go back to the Vienna Convention on the Law of Treaties which explains how to interpret any international instrument. It states that “in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and scope.”[107] In relation to this, the United Nation Charter preamble states as one aim and objective that “armed forces not be used save in the common interest…”[108] As the Charter preamble reflects, the Article’s textual meaning, uses the term “force” as armed force.[109] This is a restrictive interpretation of “force”. Nevertheless, Article 44 of the Charter also supports this approach. It states that “When the Security Council has decided to use force it shall, […], invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member’s armed forces.”[110]

2.3.1 Instrument-based approach

This section examines the means used to assess cyber operations. This analysis will demonstrate the difference between armed force on the one side and political and economic coercion on the other.[111] The instrument-based approach looks at the means used for the attack. It assesses the attack and analyses if the damaged caused by the cyber-attack is similar to what a kinetic attack would have caused. Usually, this approach is used to separate armed force from political or

[107] Vienna Convention on the Law of Treaties, Article 31(1), 1155 U.N.T.S. 331, (1969).

[108] United Nation Charter, Preamble.

[109] Schmitt M., Schmitt M, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, (2012, Ibid, 18).

[110] Article 44, United Nation Charter.

[111] Roscini, Cyber Operation and The Use of Force in International Law, Ibid, p46-47.

economic sanctions.[112] However, the author holds this approach is not useful in assessing cyber operations because it focuses on the physical tool to conduct force, which is absent in cyber operations. This approach has also been challenged by many scholars such as Schmitt and Roscini in the context of characterising cyber operation as a use of force. Schmitt, for instance, commented that "the instruments do not precisely track the threats to shared values which, ideally, the international community would seek to deter."[113] Silver agreed with that statement and described the instrument approach as “not entirely satisfying”.[114] Additionally, the Group of Experts in Tallinn Manual does not agree this approach should be used on cyber operations. They conclude that “A use of force need not involve the employment of military or other armed forces by the State in question”[115]. Roscini as well, rejected this approach because following it would mean cyber operations can never amount to a use of force, even when they cause damage. The instrument-based approach will not serve the aim and objective of this thesis because it requires a physical means to amount to force, and therefore it ignores many consequences of cyber operations and the huge impact these operations can have on the state’s infrastructure.

2.3.2 Weapon Assessment

In the context of the instrument-based approach, it comes into question whether cyber malware or viruses could be classified or defined as a weapon in international law. To answer that question, the thesis will look at chemical and biological weapons as well as neutron bombs. Using them is considered a use of force and, as Brownlie described, they are “forms of warfare”. This is the case

---

[112] Gosnell Handler, Stephanie, (2012), The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, pp. 226-227.

[113]Schmitt M., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 37, 885-937, 26 .

[114] Silver D. , Computer Network Attack as a Use of Force under Article 2(4), in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell, International Law Studies , Vol.76, (2002).

[115] Tallinn Manual (2017), ibid, 331.

besides the fact that chemical or biological weapons are different in use from traditional weapons such as guns, missiles and bombs. Similarly, one can apply the same logic to cyber means, which are new and have a different nature to traditional weapons. Rossini, like many other scholars, has agreed on considering cyber means as a "weapon".[116] He noted that "the use of certain dual-use non-kinetic weapons, such as biological or chemical agents, against a state would undoubtedly be treated by the victim state as a use of force".[117] Furthermore, the ICJ made it clear in its Advisory Opinion on The Legality of the Threat or Use of Nuclear Weapons that "…in the light of the provisions of the Charter relating to the threat or use of force. It observed, *inter alia*, that those provisions applied to any use of force, regardless of the weapons employed."[118] Moreover, the ICJ stated in the same Advisory Opinion that it "…permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[119] Therefore, following this broad interpretation of the ICJ, one can obviously include cyber operations in the meaning of "weapons". The court intentionally used the formulation "all kinds of weapons" and "those of the future" to prevent gaps in the law resulting from new technology. Moreover, in the Tallinn Manual, the International Group of Experts agrees with the court's statement and describes it as a reflection of customary international law.[120] This argument indicates that malware or any type of worm or botnet code could be characterised as a weapon. Consequently, they could be used in attacks amounting to a use of force.

However, regardless of the weapon that has been used to attack, the core point is the act itself and whether it can be considered as a use of force, or not. This means one needs to assess other aspects such as the target or the consequences of the act and not solely the type of weapon used in the act. The Group of Experts

---

[116] Dinstein Y., Computer Network Attack as a Use of Force under Article 2(4), in Computer Network Attack and International Law ,(2002),76 ILS,99, 280; Schmitt M., Computer Network Attack: The Normative Software", Yearbook of International Humanitarian Law, vol.4, (2001), 56.

[117] Roscini, Cyber Operation and The Use of Force in International Law, Ibid, p50

[118] Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) (1996) 35 ILM 809.

[119] Ibid.

[120] Tallinn Manual, 2017, 328.

noted further that the consequences of the operation and circumstances are the core in determining the act as a use of force, regardless of the instrument used.[121] The author agrees with this assessment because this view is concurrent with the ICJ's assessment regarding new forms of weapons in its nuclear weapons decision. In this case, the Court pointed out that all future weapons, including chemical biological weapons, would be assessed based on the consequences of their use.

2.3.3 Consequences-based approach

The consequences-based approach is a method to evaluate if there is a threat or coercive action. This approach looks at the direct-action effect and the result of the act, such as the physical effect or damage to property or persons.[122] Silver commented on it, stating, "physical injury or property damage must arise as a direct and foreseeable consequence of the CNA and must resemble the injury or damage associated with what, at the time, are generally recognized as military weapons". This indicates that Silver agrees with assessing cyber force by its effect. Roscini and Dinstein have similar opinions on this approach.[123] The Tallinn Manual follows this approach, albeit not exclusively. It suggests the "scale and effect" assessment to determine the use of force in the cyber realm.[124] They are assessing the consequences of the cyber operation along with some other indications. This assessment is based on the Schmitt assessment, which he suggested in 1999.[125] This approach has seven factors (severity, immediacy, directedness, invasiveness, measurability, military character and presumptive legitimately).[126] The Tallinn Manual

[121] Ibid.

[122] Roscini, Cyber Operation and The Use of Force in International Law, Ibid.47-49

[123] Roscini M., Cyber Operation and The Use of Force in International Law, Ibid, 47-49; Yoram Dinstein, Computer Network Attacks and Self-Defence, International law studies. Vol.76, Iss:1 (2002),103

[124] Tallinn Manual (2017), 331-333.

[125] Schmitt M, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' ,Ibid, 18-19

[126] Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare,p 48-52.

supports this view and adds one more factor to it, which is state involvement. To illustrate:

- Severity: the harm of the cyber-attack. Has it a physical effect, or does it cause property damage? If so, it will meet the severity criterion and amount to a use of force.[127] Other than that, any mere effect or consequences of the cyber operation such as a mere disturbance of the mobile network does not meet the severity criteria.
- Immediacy: The quick consequences of the cyber-attack, which does not leave any time for negotiations or for terminating the attack before it given its effect.[128]
- Directedness: Whereas immediacy is related to the time assessment, directedness is about the related causation between the act and the consequences. The more they are related, the more likely they amount to a use of force.[129]
- Invasiveness: The more secure the target, the higher the likelihood it fulfils this criterion. For instance, the attack on a military system, which requires a credential to access, amounts to the use of force, unlike an attack on a non-secure or open website of a university. Moreover, to assess this factor, the domain name would help to determine the level of invasiveness. If the cyber-attack targets a domain name such as (…moi.sa) it will be more likely considered as a use of force because it belongs to the state, rather than a non-state domain name such as (...com).[130]
- Measurability: It means the ability to evaluate the effects with quantitative methods. In a case of an attack carried out by the military, the people killed, and the property damaged can be measured easily. However, in the cyber domain when an attack occurs, it is more likely to qualify as use of force if the amount of data corrupted or the number of destructed servers can be measured.[131]

[127] Tallinn Manual, 2017, 344.

[128] Tallinn Manual, 2017, 334.

[129] Ibid.

[130] Ibid.

[131] Ibid.

- Military character: Whenever a cyber operation is carried out against a military target or when it possesses military conduct, a cyber operation will amount to a use of force.[132]
- Presumptive legitimately: The cyber operation should qualify as an illegal act under international law. The rule is, any act that is not prohibited by international law is presumptively legal. This is because the nature of international law is prohibitive in general.[133]
- State involvement: The more state involvement is present in launching the cyber-attack against another state, the more likely the cyber-attack is considered a use of force.[134]

The Group of Experts in the Tallinn Manual[135] have agreed on additional factors that need to be considered when assessing a cyber-attack. These are, for example, the dominant political environment, connection to any military operation, the attacker's cyber record and the target's nature.[136] Because of that, they describe these factors as "not exhaustive" and "operate in concert" which means it depends on surrounding circumstances.[137] Moreover, the Tallinn Manual Experts have agreed unanimously that any cyber operation rises to the level of use of force when the damage is greater than de minimis suffices. That was the case in the Stuxnet attack in 2010 which damaged an Iranian nuclear facility.[138]

Schmitt has predicted that states will consider data destruction and damage as just as severe as physical injuries from conventional use of force, irrespective of whether the destruction affects the societal, economic or governmental functions.[139] To illustrate, the author will apply the Schmitt criteria to a hypothetical cyber operation against the Air Traffic Control (ATC) which then disables it. The attack results in an airliner crash and the death of passengers - arguably amounting to a

[132] Ibid.

[133] Ibid.

[134] Ibid.

[135] Hereinafter The Group of Experts.

[136] Tallinn Manual, 47.

[137] Ibid, 337.

[138] Ibid.

[139] M Schmitt, The Law of Cyber Conflict: Quo Vadis? , (2014), 25 (2) SLP, 281.

use of force. The author believes it does qualify as a use of force because it has a severe consequence, which is crashing the plane and death. Moreover, the result of the attack happened immediately, which does not leave any time for negotiations or other means to prevent this attack. Also, the cyber operation was directed against the ATC, a part of a state infrastructure, which was the reason for the crash and death. Regarding the measurable factor, the consequences of this attack and all property and human losses can be measured easily.[140] Furthermore, the attack crossed the state's boarders by transmitting the electrons from the place of origin to the ATC, which meets the invasiveness factor. The cyber operation here is presumed illegitimate because this act of force has been criminalised by domestic law and international law alike. There are also no legitimate reasons like self-defence which would allow the use of force.

On the other hand, the cyber operation against a university computer system which disrupts military research conducted in campus laboratories could not constitute a use of force, as there is no physical damage or death it will be below the severity level. Moreover, the damage could not be measured. Also, the goal of this cyber-attack, diminishing the military capability in cyber-attacks, will only be achieved indirectly. While the act could meet the invasiveness criteria, it does not rise to the level of use of force.

However, these factors faced a lot of criticism. For example, Silver commented on the severity criteria, saying that "severity, as defined for this purpose, seems applicable only to physical injury and property damage, compelling the conclusion that CNA will be considered within the force category only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion".[141]

Silver argued that the severity criteria will have a limited role in assessing cyber acts because it is just applicable when the result of the attack "cause physical injury or property damage" while the cyber operation may not have a physical harmful

[140] Ibid, 27.

[141] Silver D. , Computer Network Attack as a Use of Force under Article 2(4), in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, 76 ILS, (2002).91-92.

effect on people or property. The author argues that the cyber operation could have a very harmful effect, which is described as a non-destructive cyber operation. This type of attack still could be considered a use of force because of its severe effect on the state. Therefore, the severity criterium is still desirable in assessing the cyber operation and cannot be limited to the physical injury or property damage.

Ziolkowski commented on the measurability criterion by saying that "effects of malicious cyber-activities will not always be measurable".[142] He adopted this opinion because most cyber infrastructure is owned by private companies, which makes it hard to obtain all the required information to meet the measurable criteria.[143] His view is reflective of the situation in 2012. However, nowadays, there are many developments in that field since the states started adopting cyber security strategies and having agreements with private sectors and regulating the information which owned by private companies. Another criterion which has been criticised by Ziolkowski is the presumptive legitimacy. He noted that "legitimacy" (described an ethically justifiable act) is rather a term of political and ethical discourse; law deals with legality and illegality of actions"[144]. He argued that this assessment cannot help in investigating cyber acts and determining their legality. The author agrees with that assessment. Not only does this open a path to uncertainty, it also is a backwards approach – one should first establish legitimacy (and not assume it) and then apply the law accordingly.

Roscini as well commented in a similar way. He called what Judge Simma described as presumptive legitimacy an "old, tiered view".[145] This thesis also is in favour of that view because it will not play a big role in classifying the cyber operations since there are much stronger criteria such as the severity criterion which can be used to assess whether an act amounts to the use of force. Regarding the directness, Roscini did not agree on directness as a criterion to characterise the cyber act. He based his view on the definition of aggression and on the ICJ

[142] Ziolkowski K., Jus ad bellum in Cyberspace – Some Thoughts on the Schmitt-Criteria for Use of Force, in Czossek C., Ottis R. and Ziolkowski K. (eds),4th International Conference on Cyber Conflict Proceedings (NATO CCD COE Publications: Tallinn, (2012), 295–309.

[143] Ibid.

[144] Ibid.

[145] Roscini M., Cyber Operation and the Use of Force in International Law, Ibid, 49.

judgement in the Nicaragua case, which considered the not direct destructive armed force as a use of force.[146] Therefore, the operation does not need to have a direct effect on the target to amount to a use of force which is contrary to Schmitt's criteria. Moreover, Roscini has noted that the nature of the cyber operation effect is indirect,[147] because the intended harmful consequences do not happen directly.[148] The thesis agrees with that for the same reasons. Take as an example the Aramco cyber-attack, where the virus effect went beyond Aramco to other companies such as Santa Fe, Ocean and Schlumberger and the Exploration and Petroleum Engineering Centre.[149] The direct target was Aramco, but the cyber-attack affected indirectly other companies.

In the context of the consequences-based approach, the big question is what are the possible consequences of a cyber-attack? The harm of a cyber-attack could be shutting down an infrastructure network, physical destruction, burst oil pipelines, opening of a dam, or shutting down a hospital's power. All that could result in death or human injury, either directly or indirectly.[150] Therefore, cyber-attacks have a variety of consequences, some of them could be severe, others not.

Which cyber-attack harm can meet the consequences-based criterion and rise to the level of use of force? The answer to this question is simple when one takes the narrow path. When the cyber-attack causes injury or death to humans or physical damage to property, it will violate the prohibition of the use of force.[151] For example, shutting down the power of a hospital will be characterised as a use of force because it could result in death or severe injury. The International Group of Experts in the Tallinn Manual agreed on the non-destructive cyber phycological operation or

[146] Roscini M., Cyber Operation and the Use of Force in International Law, Ibid, 48.

[147] Ibid.

[148] Ibid.

[149] Bronk, Christopher and Tikk-Ringas, Eneken. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict." (2013) James A. Baker III Institute for Public Policy of Rice University, p20

[150] Ibid.

[151] Ibid

prohibition e-commence with another state or even any negative economic impact will not amount to a use of force.[152]

In the Nicaragua case, the ICJ has rejected the narrow interpretation of "use of force" either in kinetic activities or non-kinetic activities.[153] The ICJ held that the training and arming of guerrilla forces by a state against another one qualified as a use of force.[154] Therefore, non-destructive cyber operations could be considered a use of force. For instance, if a state provided malware to some rebel group and also provided the required training to use it in destructive manners, it will amount to a use of force. That has been asserted by the International Group of Experts in Tallinn Manual who consider providing training to any group to carry out cyber operations against another state, which involves hostilities as rising to a use of force.[155] On the other hand, the ICJ in the Nicaragua case stated that financing guerrillas does not rise to the level of use of force. As a result, financing a rebel group for their cyber activities or using cyber means to coerce another state economically does not amount to a use of force.[156]

While the consequence-based approach is favoured both by the Tallinn Manual and Roscini, it alone is not enough to suitably address cyber operations. Indeed, often even the attacker can't know what the consequences might be. Even more so, the consequence-based approach does not allow for quick changes in the attack, even an innocent looking cyber-operation might quickly transform from something looking like mere coercion into an armed attack. Yet, the consequence-based approach does not offer sufficient guidance on how to deal with such potential scenarios. States might be forced to wait until they can react because the assessment of the consequences takes time.[157] The author attempted to explain why

[152] Tallinn Manual, (2017), 331

[153] Nicaragua case, 228.

[154] Ibid

[155] Tallinn Manual,(2017), 331

[156] M Schmitt, The Law of Cyber Conflict: Quo Vadis?, Ibid, 280

[157] Sklerov, M. Solving the dilemma of state responses to cyberattacks: A justification for the use of active for the use of active defences against states who neglect their duty to prevent. (2009), (Master's Thesis, The Judge Advocate General's School, USA).

this approach alone is not suitable. She proposes that it should be used together with the target-based approach, which is discussed in the next part.

2.3.4 Target-based approach

There is another approach to qualify the act as a use of force, which is known as the "target-based approach". This approach looks at the target of the attack and assesses whether it is part of the national critical infrastructure or not.[158] Stevens explains very well why taking the target into consideration is so very important:

"A cyber attack that shuts down any part of a nation's critical infrastructure may have an effect that is much more debilitating than a traditional military attack. The threat in such a situation may be more terrorizing and harmful than a traditional military attack. Certainly, a country that is unable to use its banking system, or whose power grid has gone off-line due to a cyber attack, possesses legitimate claims for reparation, justice, and security. Because the consequentiality approach focuses on the same type of physical damage caused by a kinetic attack, it does not sufficiently protect critical infrastructure."[159]

However, in order for the target-based approach to function properly, national critical infrastructure needs to be identified clearly to use this approach. There is no universal consensus on how to define the national cyber infrastructure.[160] However, every state has its own definition. For example, Saudi Arabia defines it as "system and assets, whether physical or virtual, so vital to KSA that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of

---

[158] Talbot Jensen, E., Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of self-defence, (2002), SJIL, 234.

[159] Stevens, Internet War Crimes Tribunals and Security in an Interconnected World, (2009). http://www.uiowa.edu/~tlcp/TLCP%20Articles/18-3/stevens.finalfinal.me.mlb.100109.pdf.

[160] Roscini M., Cyber Operation and the Use of Force in International Law, Ibid, 56

those matters."[161] This definition illustrates that the cyber structure and facilities are considered a part of the national infrastructure because any attacks against them or destruction of them will have a harmful effect on security, safety, the economy or public health. This definition uses also the target-based approach, which indicates that Saudi Arabia will follow this approach in assessing cyber operations. Also, Qatar defined the National Critical Infrastructure as "Physical assets, systems or installations, which if disrupted, compromised, or destroyed, would have a serious impact on the health, safety, security, or economic well-being of Qatar or the effective functioning of the Qatari government."[162] This definition is very close to the Saudi one, but it is more detailed. It adds "installation" and provides more examples of harmful acts like "disrupted, compromised".

Roscini describes this approach as "overinclusive" because, in his opinion, this approach will "qualify as a use of force those cyber operation that only cause inconvenience and or merely aim to collect information whenever they target NCI."[163] Back to Saudi Arabia's definition, it limits the meaning of critical infrastructure to the type of effect. It states that it needs to have an impact on security, economy or public health, which means that "merely aim[ing] to collect information" is excluded from the Saudi definition. This underlines the necessity to combine the consequence-based approach with the target-based approach. With these limitations, as included in the Saudi definition, this joint approach would balance the consequences-based approach. Even though, every state has its own definition for National Critical infrastructure, it is still a very useful approach to apply when assessing cyber operations in the meantime. This approach is clear and easy to apply on a state-by-state basis, and it protects the most significant things that any state will be concerned about for maintaining its safety and security in the cyber realm. Moreover, this approach has been used in assessing what an "armed attack" occurred to

---

[161] Developing National Information Security Strategy for the Kingdom of Saudi Arabia NISS draft 7. Available at : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf

[162] QATAR National Cyber Security Strategy (May 2014).Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf

[163] Roscini M, Cyber Operation and The Use of Force in International Law, Ibid,45-62.

determine if there's a right to self-defence by evaluating the severity of the effect on the critical infrastructure function and how that could characterise it as a destructive attack.

The author believes that the target-based approach combined with the consequence-based approach is easy to apply to cyber operations because states will look first at the target of an operation. Moreover, every state has a clear definition of what critical infrastructure is, which is especially true for Saudi Arabia. However, as stated previously, this approach must not be separated from the effect-based approach, rather it should be used together. This is because when one qualifies the cyber operation as a use of force following the target-based approach, one will also have to look at the severity of the consequences for the critical infrastructure. This ensures maximum usability while keeping a high standard to not potentially escalate the situation.

All of these approaches qualify cyber acts as a use of force. The instrument-based approach relies on the type of means which have been used without considering the effects of the attack. The core difference between that approach and the consequences-based approach is that one looks mainly at the effect and result of the cyber operation. This would enable a combination with the target-based approach, which requires the target to be part of the National Critical Infrastructure. The thesis will argue in favour of the target-based approach, as it follows the Saudi approach. The author makes this policy choice because the thesis focusses on Saudi Arabia, and moreover, believes this is the approach that should be taken because there is a clear definition of it. This clear definition leaves no room for misunderstanding and ensures that every state can apply this approach in the same way. This approach distinguishes a cyber operation which targets, for example, a ministry for internal affairs, from an operation which targets a university. It ensures proportionality and predictability of legal decisions. A state's priority is the National Critical infrastructure. Therefore, any cyber operation targeting it qualifies as a use of force.

2.4 Threat of force

Going back to Article 2(4) of the UN Charter, it prohibits not just the use of force but also the threat of it.[164] The United Nation Charter does not define what a threat is. However, some scholars, such as Roscini, tried to come up with a definition. He defines it as "an explicit or implicit promise, through statements or actions, of a future and unlawful use of armed force against one or more states, the realization of which depends on the threatener's will,"[165] Furthermore, Professor Wingfield of the U.S. Army Command and General Staff College has named some acts that could constitute a threat of force which are "verbal threats, initial troop movements, initial movement of ballistic missiles, massing of troops on a border, use of fire control radars, and interference with early warning or command and control systems."[166]

Additionally, the Tallinn Manual examined the term "threat" in cyber operations. It states in the Rule 12: "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."[167] The International Group of Experts proposes two situations for applying this rule. First is when a cyber operation has been used to communicate a threat. Second is when the threat of a cyber operation is conveyed to another state.[168] For example, Iran has developed very sophisticated cyber capabilities which makes Iran capable of using it against another state in general or Saudi Arabia in particular, as it is the case study of this thesis. Having these capabilities alone cannot be considered a threat of force until there is an announcement from the government or one of their representatives. Ultimately, the Tallinn Manual does not settle this matter. Similarly, there is no consensus on the state intention to carry out any cyber operation against another state. A "threat of the use of force" in the cyber realm can be deduced from any political announcements or

[164] The Charter of United Nation, Ibid.

[165] Roscini M., Cyber Operation and The Use of Force in International Law, Ibid, 67.

[166] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council, (2009).51

[167] Ibid, p 52.

[168] Tallinn Manual (2017), Ibid, 338.

action from a state, it can include intelligence gathering or a precedent attack which indicates a harmful cyber-attack will be launched against a state.

Another significant question is: What happens if the cyber-attack does not complete or does not achieve its goal? Is an error in the cyber operation also included? Can these situations still be considered a use of force? Is it enough to consider a state's intention to commit a use of force (or threat thereof)? To answer this question, there is a need to clarify some points. First, the cyber operation in this hypothetical scenario has been prepared and is ready to be launched - which means there is no doubt on the use of force intention. However, the act here transfers to another stage, which is "attempted use of force" regardless of the outcome. The intention to use force has been obvious. Therefore, there is no need to examine whether the state succeeded. The question is whether the state has taken steps to act, which means it is not just an intention or a threat, but indeed an attempt. In the basic rule of law, an illegal "attempt" is an act violating the law. Applying that to the use of force rules, an "attempted use of force" is part of the prohibition of the use of force. As a result, this type of act will also be considered as prohibited in international law and consequently violates the jus ad bellum rules. Therefore, the analysis here depends entirely on the impact of the act on peace and security. In the Nicaragua case, the court refers to Article 18 of the Organization of American States Charter, which provides that "The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic and cultural elements."[169] This statement indicates that an "attempted threat "is prohibited by the non-intervention principle. This leads us to the "attempted use of force" which is of a higher degree than the attempted threat. However, this area of concern has neither been discussed in Tallinn Manuals nor among Scholars. Therefore, this needs to be elaborated on.

2.5 Use of force and armed attack relationship

Another important point is to explain the relationship between the use of force and armed attack. The ICJ in the Nicaragua case made clear what the difference

[169] Nicaragua case, judgement, para 27.

between the use of force and an armed attack is. It stated that the “most grave” forms of use of force can be considered as an armed attack.[170] However, the less grave forms cannot rise to the level of an armed attack.

The question here is: What is grave enough to constitute an armed attack in international law? This is a substantial question for not only the current discussion, but also for evaluating the cyber operation. To answer the main question, there is a need to go back to Nicaragua case.[171] In that case, the ICJ referred to the General Assembly Definition of Aggression 1974, which describes an armed attack as "regular armed force" and added "the sending by or on behalf of a State of an armed band, groups, irregulars or mercenaries, which carry out acts of armed force against another State".[172]

Furthermore, in the Wall Advisory Opinion, the ICJ noted that an armed attack should be "imputable" to a state.[173] The court limited the definition of armed attack in two parts. First, is the actor committing or authorising it needs to be a state. Second, the court connected armed attacks with armed forces, which means the military needs to be involved. With regard to the required severity of the attack, the ICJ noted in the Oil Platform case (Iran vs US) that "the single ship striking a naval mine could potentially constitute an armed attack".[174] However, the ICJ in the same case noted that “it is necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.”[175] In this part, the court gave a restricted approach when determining the armed attack in question. Nevertheless, this distinction is not helpful to answering what constitutes an armed

[170] Nicaragua case, judgement, para 228.

[171] Nicaragua Case, Para 176.

[172] See Art 3, subparagraph g) of UNGA Res 3314 (XXIX) (14 December 1974) ‘Definition of Aggression’.

[173] Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 July 2004, available at: https://www.refworld.org/cases,ICJ,414ad9a719.html [accessed 20 August 2019].

[174] Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), 6 November 2003, available at: https://www.refworld.org/cases,ICJ,414b00604.html [accessed 20 August 2019].

[175] Nicaragua Case, para 191.

attack, as it raises a new question regarding what is considered a grave form of attack and what is not.[176] On the other hand, a comment by Judge Greenwood expands the meaning of armed attack by saying that: "since population is one of the attributes of statehood, an attack upon a state's population would seem to be just as much an attack upon that state as would an attack upon its territory."[177] This statement focuses on the loss of life or harm to persons on the state's territory. However, an attack could also target the state infrastructure, e.g., by targeting a state network or telecommunication system during a cyber operation. Still, in that case, the attack would be considered an "armed attack" as long as there was a harmful effect on the state. The US has a broad view of the definition of self-defence, and explained that "a lower threshold for triggering the right of self-defence can deter aggressors from acting in the first place."[178] This statement indicates that the US is considering any type of threat or coercion, including cyber operations, as an armed attack.

It appears that every situation must be viewed and measured on a case-by-case basis. An armed attack must be grave enough. But what would be grave enough in a cyber context? The International Group of Experts in Tallinn Manual has agreed on that concept and considers any cyber operation that amounts to an armed attack must by default be a use of force.[179] The armed attack assessment triggers self-defence. Therefore, any act or use of force that does not rise to the level of an armed attack cannot give the victim state the right of self-defence. Self-defence against a cyber-attack will be discussed in detail in the following part below.

[176] Gray C,International law and the use of force, Ibid, 147.

[177] Greenwood C, International Law and United States Air Operations against Libya, 89 West Virginia LR (1986), 933, at 941.

[178] Ryan Goodman, Cyber Operations and the U.S. Definition of "Armed Attack", (2018), https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/.

[179] Tallinn Manual, (2017), Ibid, 332.

2.6 Art. 51 – The right to self-defence

The right of self-defence is a significant exception to the prohibition of the use of force. It needs to be discussed here to show the requirements to invoke this right and how it has been regulated in international law. The right of self-defence is enshrined in Article 51 of the United Nations Charter: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council, and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary to maintain or restore international peace and security."[180]

This right, as described in the article, is an "inherent right", which indicates that it has existed before the drafting of the Charter. Indeed, the right of self-defence has its originality in customary international law, which was acknowledged in the Nicaragua case.[181] Although the right of self-defence is an inherent one, there are some conditions that need to be met to legitimise the usage of this right. Moreover, there is a limitation to exercising this right. The first and most important condition is that there needs to be an "armed attack", as was discussed in the previous section.[182]

The previous assessment of the “armed attack” assumed that the act can be attributed to a state. However, Article 51 does not clearly require the attacker to be a state. Therefore, when an attack is launched by a non-state actor (NSA) such as an armed groups based on another state’s territory, states could also have the right to use self-defence against the NSA. Bethlehem has noted that it is “reasonably clear and accepted that states have a right of self-defence against attacks by non-state actors—as reflected, for example, in UN Security Council Resolutions 1368 and 1373

[180] Charter of the United Nations, (24 October 1945),Ibid.

[181] Nicaragua Case, Para 176

[182] SHI Jiuyong, Prohibition of Use of Force in International Law, Ibid, Ibid, 5.

of 2001, adopted following the 9/11 attacks in the United States."[183] This statement indicates international acceptance of using self-defence against non-state actors after the 9/11 attacks, and is further supported by the "war against terrorism". Yet, the United States' position has been the same even before 9/11. In 1998, the United States justified its airstrikes against al-Qaida targets in Afghanistan and Sudan as self-defence measures taken in response to terrorist attacks against its embassies in Kenya and Tanzania.[184] After 9/11, the position of many states has taken the same turn and supports self-defence against non-state actors. For example, the legal advisor to the British Foreign Office, Sir Wood, has stated that "The action against Al-Qaeda in Afghanistan in October 2001 (which was widely supported and scarcely opposed by states) was action in self-defence of anticipated imminent terrorist attacks."[185] Moreover, after France has been attacked by Daesh (ISIS) in 2015, France justified its military actions in Syria and Iraq as self-defence. That has been re-affirmed by the Permanent Representative of France to the UN, who stated in the UN Security Council that "The attacks of 13 November [2015] constitute an armed attack against France. Our military actions, of which we have informed the Security Council from the very beginning, and which were justified as collective self-defence, can from now on be based on the individual self-defence in accordance with Article 51 of the United Nations Charter".[186]

Recently, during the conflict in Yemen, Saudi Arabia has been targeted by Houthi missile attacks several times. Besides the war in Yemen, which must be considered an armed attack in its own right, missile attacks threaten the peace and

[183] Bethlehem D, 'Principles Relevant to the Scope of a State's Right of Self-Defence Against an Imminent or Actual Armed Attack by Non-State Actors', (2012), 106 AJIL 5.

[184] Permanent Rep. of the United States of America to the U.N., Letter dated August 20, 1998 from the Permanent Rep. of the United States of America to the United Nations addressed to the President of the Security Council, U.N. Doc. S/1998/780 (Aug. 20, 1998); see also Terry D. Gill & Kinga Tibori-Szabó, Twelve Key Questions on Self-Defence against Non-State Actors, (2019), 95 INT'L L. STUD. 467, 219.

[185] Elizabeth Wilmshurst, Principles of International Law on the Use of Force by States in Self-Defence (2005), ILP WP 05/01 Chatham House, 31.

[186] United Nations. S/PV.7565. Security Council. Seventieth year. 7565th meeting. (20 November 2015).

security of the Saudi-Yemeni borders, and Saudi territory. Therefore, Saudi Arabia has the right of self-defence against this threat. As the foreign minister of Britain declared: “Britain supports Saudi Arabia's right to defend its national security against missile attacks from Yemen, many of which have targeted the Kingdom’s cities, including Riyadh."[187]

In this context, there is an obligation on the state to ensure its territory is not used illegally for measures against another state. This obligation is known as the “due diligence” obligation. This principle has been acknowledged since 1928 and was discussed on the island of Palmas arbitral award.[188] Additionally, the ICJ has recognised this principle both in the Corfu Channel case and the Nicaragua Case.[189] This obligation cannot be considered a burden on the state because it is only triggered if the state has knowledge of the armed group’s activity. As noted by Gill and Tibori-Szabó “It is unlikely that a NSAG can conduct armed attacks against another State from a base of operations in a territorial State without either State being aware of such activity. Where there is such knowledge, the duty to take effective action is indisputable.”[190] However, the due diligence obligation does not automatically trigger the right of self-defence in itself. The defending state should consider the necessity and proportionality conditions.[191]

Moreover, when deciding the territorial state’s role in dealing with this NSA group, there will be two situations after the NSA launched an armed attack. Option one: the territorial state will be “unable” to face the non-state actor and stop them. Option two: the territorial state will be “unwilling” to deal with this armed group. In the first situation, the state can be “unable” for various reasons. An example would be the situation in Somalia, where the governmental power of the state effectively ceased to

[187] UK says it supports Saudi Arabia's 'self-defence ' in Yemen, The New Arab , (2018) , UK says it supports Saudi Arabia's 'self-defence ' in Yemen (alaraby.co.uk).

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

[189] Corfu Channel Case, 22; Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica), ICJ. Reports [2015], para.104

[190] Terry D. Gill & Kinga Tibori-Szabó, Twelve Key Questions on Self-Defence against Non-State Actors, Ibid, 494

[191] These conditions will be discussed in the upcoming part.

exist. In cases like these, the victim state could invoke self-defence as there is no alternative means available. However, Mullerson requires the victim state to seek the territorial state's consent, as "there is still government in place".[192] Moreover, the Chatham House Principles state that the territorial state's consent is required when it could be obtained.[193] However, this requirement could weaken the exercise of self-defence against NSA, especially in the case of the "unwilling" state. On the other hand, Gill and Tibori-Szabó argued that consent is not a requirement where necessity occurred.[194] This view is supported by the Bethlehem Principles, which noted that "The requirement for consent does not operate in circumstances in which there is a reasonable and objective basis."[195] The thesis agrees with the last view. There is no need to ask for permission to use self-defence. In reality, there will be no time available to seek the territorial state's consent - especially if it refuses to co-operate. In that event, the "unable" state will be an "unwilling" one.[196] This argument relates to weak or powerless governments. Separate from that, in some circumstances, a state will not hold authority over its entire territory because, e.g., a non-state actor has effective control over parts of the state's territory. That example would authorise the use of self-defence without consent, as there is no government to ask for consent. It is worth mentioning that, when a state invokes the right of self-defence and uses force against the threat coming from another state's territory, this latter state cannot respond to that force in any manner because "there is no self-defence against self-defence."[197]

---

[192] Mullerson R.,Self-defence against Armed Attacks by Non-State Actors, Chinese Journal of International Law (2019), 751–775.

[193] Elizabeth Wilmshurst, Chatham House Principles of International Law on the Use of Force by States in Self-Defence , (2006) 55 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 963, 963.

[194] Terry D. Gill & Kinga Tibori-Szabó, Twelve Key Questions on Self-Defence against Non-State Actors, Ibid, 500-501.

[195] Bethlehem D, 'Principles Relevant to the Scope of a State's Right of Self-Defence Against an Imminent or Actual Armed Attack by Non-State Actors' ,Ibid, 776 (Principle 11).

[196] Mullerson R.,Self-defence against Armed Attacks by Non-State Actors, Ibid, 771.

[197] Terry D. Gill & Kinga Tibori-Szabó, Twelve Key Questions on Self-Defence against Non-State Actors, Ibid, 495.

There are two more significant conditions that need to be met when exercising individual or collective self-defence: necessity and proportionality of the use of force are required in customary international law.[198] Sharp has explained that: "a state's use of force proportional in intensity and magnitude to what is reasonably necessary to promptly secure the permissible objectives of self-defence."[199] Moreover, the two conditions are interconnected.[200] This means if exercising self-defence is not necessary, it is not proportionate and therefore not available in a lawful manner.[201] The ICJ elaborated this point in the Nicaragua case: "there is a specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law".[202]

Furthermore, the ICJ noted in its *Advisory Opinion Concerning the Legality of the Threat or Use of Nuclear Weapons* in 1996 that: "The entitlement to resort to self-defence under Article 51 is subject to the conditions of necessity and proportionality".[203] Regarding the relation between these two conditions, Gray commented that “if a use of force is not necessary, it cannot be proportionate and, if it is not proportionate, it is difficult to see how it can be necessary.”[204] While they are connected, the thesis will now examine each one individually to ensure more clarity, before looking further into the interconnectedness and possible applications to cyber operations.

---

[198] Moore, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law and Potential Models." ,Ibid,156; Gray C., International law and the use of force, Ibid, 140.

[199] Sharp, W.G., Cyberspace and the Use of Force, Aegis Research Corporation, Ibid, 38.

[200] Pank.S.. “What is the scope of legal self-defence in International Law? Jus ad bellum with a special view to new frontiers for self-defence.” (2014).

[201] Ibid.

[202] Nicaragua Case, para. 176, 94.

[203] Advisory Opinion Concerning the Legality of the Threat or Use of Nuclear Weapons (Request for Advisory Opinion by the General Assembly of the United Nations), (8 July 1996) ICJ, available at: https://www.refworld.org/cases,ICJ,3ae6b67f14.html [accessed 21 August 2019].

[204] Gray C, International law and the use of force, Ibid, 150.

Necessity of a use of force is defined as “a degree and kind of force not otherwise prohibited by the law of armed conflict, requires for the partial or complete submission of the enemy with minimum expenditure of time, life, and physical resources …".[205] This means must not be an alternative defence method that can be applied.[206] This is what the ICJ stated in the Nuclear Weapons Advisory opinion: “the Court cannot lose sight of the fundamental right of every state to survival, and thus its right to resort to self-defence . . . when its survival is at stake.”[207] Once the state’s existence is threatened, necessity is clearly present. However, this restricted meaning of necessity is not the only significant criterion in determining the lawful exercise of the right of self-defence. As the ICJ made clear in its judgement in the Nicaragua Case: “‘it was possible to eliminate the main danger to the Salvadorian Government without the United States embarking on activities in and against Nicaragua”.[208] The court indicates that as long as there are alternative actions, the use of force would be unnecessary. In a similar way, the ICJ rejected the Ugandan claim in the Armed Activities on territory of the Congo case because of the absence of the necessity ground.[209] Another rejection of the claimed self-defence occurred in the Oil Platform Case in 2003. The court noted that “there is no evidence that the United States complained to Iran of the military activities of the platforms, in the same way as it complained repeatedly of minelaying and attacks on neutral shipping, which does not suggest that the targeting of the platforms was seen as a necessary act.”[210]

In some precedents, there was room for seeking peaceful means before using armed force in self-defence, but in others not. For example, in the Tehran hostages’ case in 1980, the United States exhausted all peaceful means to rescue the hostages, however all attempts failed. Therefore, using armed force for the rescue was

[205] Ibid, 39.

[206] Gray C, International law and the use of force,Ibid, 150.

[207] Advisory Opinion Concerning the Legality of the Threat or Use of Nuclear Weapons, Ibid, para 96.

[208] Nicaragua Case, para 237.

[209] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits, [2005],ICJ Judgment, para 147.

[210] Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), (6 November 2003), para 76.

“necessary” to achieve the mission.[211] While this is an example of a case where there were many attempts at peaceful means before using armed force, there is no agreement on when situations meet the “last resort” criteria.[212] The bottom line here is that acting in self-defence is the only way to defend itself when all the other means have either been used or are unavailable. It is worth to mention that in some circumstances there is a need to act immediately to defend the state. As Green noted, “There may not be the time for negotiation or even complaint on the part of a defending state”.[213] This is the case with cyber-attacks, as they happen immediately, which leaves no time to use peaceful means.

Regarding the maximum duration of self-defence, Schachter commented that "defensive retaliation" may be justified when a state has good reason to expect a series of attacks from the same source and such retaliation serves as a deterrent or protective action.”[214] Which indicates that the defensive actions may continue until the danger has been terminated. Also, if the attack launched in parts, necessity would continue to exist. Cyber operations are an appropriate example of this type of attack. Indeed, when a cyber operation has been launched against a target, the attack could happen in stages. That has been discussed by the Group of Experts in Tallinn Manual, and they describe this situation as “composite armed attack”.[215] However, the ICJ does not have a clear position regarding the “accumulation of events” and if it is possible to considered them as an armed attack. Nevertheless, neither has the ICJ rejected it as an armed attack.[216] The court chose to remain silent on that issue in many cases, such as Nicaragua case, Iranian Oil Platforms, and DRC v Uganda.[217]

---

[211] Schachter O., Self-Help in International Law: U.S. Action in the Iranian Hostage Crisis, 37 J. INTL. AFF. 231 (1984).241-246

[212] Green, J A., The International Court of Justice and Self-Defence in International Law, Ibid, 80-84.

[213] Ibid, 84; Oscar Schachter, 'The Right of States to Use Armed Force' (1984) 82 Mich L Rev 1620.

[214] Oscar Schachter, 'The Right of States to Use Armed Force' (1984) 82 Mich L Rev 1620, p 1630.

[215] Tallinn Manual (2017), 342.

[216] Gray C, International law and the use of force, Ibid, 155-156.

[217] Ibid.

The author's position regarding this matter depends on the timeframe between the acts and the severity of the attack. In situations where the attacks happen in short sequence and have a severe impact on the state, the author argues these attacks amount collectively to an armed attack.

As mentioned previously, exercising the right of self-defence must be necessary and proportionate to the attack. Proportionality is defined as "the level of force required to destroy a military objective, but which does not cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians."[218] However, proportionality relates to "the size, duration and the target of the response".[219] In the Iranian Oil Platforms case, the ICJ rejected the use of force on the ground of self-defence because of the absence of proportionality.[220] Yet, the controversial issue here is how to assess the proportionality. Gray noted that the scope of proportionality will be affected by the different opinions in regard to the scope of self-defence, as in the case of anticipatory self-defence[221] or the accumulation of events.[222] However, there are two methods Green suggested.[223] The first method is looking at the scale and means used in the attack. The second is to evaluate the intensity and the level of force necessary to remove the attack or the threat. In the Nicaragua Case, the court stated that "Whatever uncertainty may exist as to the exact scale of the aid received by the Salvadorian armed opposition from Nicaragua, it is clear that these latter United States activities could not have been proportional to that aid."[224] The court here followed the second method and ignored the scale assessment. The court adopted the same position in the Nuclear Weapons case.[225]

---

[218] Ibid.

[219] Gray C, International law and the use of force, Ibid,150

[220] Oil Platforms Case, (Islamic Republic of Iran v. United States of America), [2003], ICJ, para 77.

[221] Gray C, International law and the use of force, Ibid,150

[222] Gray C, International law and the use of force Ibid, 150.

[223] Green, J A.. The International Court of Justice and Self-Defence in International Law, Ibid, 88

[224] Nicaragua Case,para 237.

[225] Green, J A.. The International Court of Justice and Self-Defence in International Law, Ibid, 88

This method can also be found in state practice. The United States support for South Korea in its conflict with the North, was “required to ensure the security of South Korea”.[226] Moreover, during the Israeli conflict with Hezbollah in Lebanon in 2006, Israel announced that “One important principle established by international law . . . is that the proportionality of a response to an attack is to be measured not in regard to the specific attack suffered by a state, but in regard to what is necessary to remove the overall threat”.[227]

As mentioned previously, even if the second method is used more often, both methods are related. That has also been asserted by Green, who said if an attack “is disproportionate in scale to the initial attack [it] is also likely to be disproportional to the goal of abating that attack.”[228] Gray highlights that the main scope of proportionality is to not be a reprisal act because that act is unlawful.[229] He emphasized, however, that “This does not mean that the defending state is restricted to the same weapons or the same numbers of armed forces as the attacking state.”[230] From the previous discussion, It can be concluded that proportionality is closely connected to necessity, which underlines that they need to be assessed together. Yet, their scope varies from case to case. Consequently, to determine the necessity and proportionality of cyber self-defence, a case-by-case examination is required.

Besides the previous conditions of self-defence, Article 51 requires the victim state to inform the Security Council immediately. This is because the victim state's role in self-defence will end once the Security Council takes appropriate measures.[231] For example, during the Vietnam War in 1964, the United States informed the Security Council about its use of defensive force against a Vietnamese ship.[232] This is an example of informing the Security Council about the act of defence immediately. Contrarily, when the USSR invaded Afghanistan, they did not report to the Security

[226] Ibid

[227] Ibid.

[228] Ibid.

[229] Gray C, International law and the use of force, Ibid, 150.

[230] Ibid.

[231] Mohammed Khaleel Almousa, Using Force in contemporary international law, (2004),,103.

[232] Ibid, 105.

Council, which can be interpreted as bad faith.[233] Furthermore, in the case of the Armed Activities on the territory of the Congo (DRC v Uganda), the court noted the self-defence was unlawful because of the failure to report it to the Security Council.[234]

The right of self-defence is not only available to individual states, but can also be exercised collectively by numerous states. In the past, collective self-defence has usually been exercised according to a treaty on collective self-defence.[235] These treaties have not been invoked often. Some examples are: USA and Lebanon (1958), USA and Afghanistan (1979), Vietnam (1961-75), USA and others and Kuwait (1991).[236]

Besides the main conditions of self-defence (armed attack, necessity, and proportionality), there are two more conditions to exercise the right of collective self-defence legally. Initially, there should be an announcement of the victim state reporting the armed attack. Moreover, there should be a request from the victim state for military assistance.[237] In the Nicaragua case, the ICJ concluded that the victim states (El Salvador, Honduras and Costa Rica) did not provide a formal announcement of the attack and neither requested military assistance, therefore, the use of force from the United Stated did not trigger the collective self-defence boundaries.[238] The second condition for collective self-defence is the existence of a collective self-defence treaty. That condition has been established by state practice. Yet, even if the collective self-defence has been used without such a treaty, it could be still legal.[239] Either way, for using both individual or collective self-defence, the armed attack should be already accrued.[240] However, if the danger is imminent and has not happened yet but there is more than planning and preparation, the defence

[233] Gray C, International law and the use of force, Ibid,122.

[234] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits, Judgement of 19 December 2005.

[235] C Gray, International law and the use of force, Ibid,167.

[236] Ibid.

[237] Mohammed Khaleel Almousa, Using Force in contemporary international law, Ibid, 114.

[238] Nicaragua Case, para 232-234.

[239] M Almousa, Using Force in contemporary international law, Ibid, 116.

[240] Green, J A. The International Court of Justice and Self-Defence in International Law, Bloomsbury Publishing Plc, (2009), 96.

against it is known as anticipatory self-defence and might still be legal. This will be discussed in the next part.

2.6.1 Anticipatory self-defence

Anticipatory self-defence means that the defensive action takes place before the attack occurs. In other words, it is a reaction to a "distance threat".[241] The Caroline incident in 1837[242] established the formula of customary international law regarding pre-emptive self-defence. It establishes anticipatory self-defence can be used if "the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation".[243] In 1967, Israel attacked Egypt, Jordan, and Lebanon as anticipatory self-defence.[244] In 1981, Israel attacked an Iraqi Nuclear reactor. Israel based its defence on the imminent nuclear danger threatening its existence.[245] The Security Council did not have any comments or position regarding this case. On the Other hand, the General Assembly in its resolution 36/27 describes the Israeli action as "a premeditated and unprecedented act of aggression".[246] Moreover, the United States and the United Kingdom launched pre-emptive strikes in 1999 against Iraqi air strikes in order to protect their aeroplanes in the "no-fly" zone, which was established according to Security Council resolution 688 in 1999.[247] The high-level panel set up by the UN Secretary General proclaimed in its December 2004 report that "long-established customary international law makes it clear that states can take military action as long as the threatened attack is imminent

[241] SHI Jiuyong, Prohibition of Use of Force in International Law, Ibid, 6.

[242] On December 29, 1837 an American Steamboat, the Caroline, carried a group of reinforcements to the island. Fifty Canadian militia men crossed the river to the American side and attacked the Caroline. They drove off the American crew and destroyed the ship. https://www.historycentral.com/Ant/caroline.html.

[243] Simma ,The Charter of the United Nation: A commentary, Ibid, at 675-76.

[244] Gray C, International law and the use of force,, Ibid, 161.

[245] Ibid, 163

[246] United Nation General Assembly Res. 36/27 (1981).

[247] Gray C, International law and the use of force, Ibid, 162.

no other means would deflect it and the action is proportionate."[248] Even though this report makes the legality of anticipatory self-defence clear, there was no universal consent on it.

After the 9/11 attacks against the United States, the opinions about the right of using anticipatory self-defence have changed to some extent.[249] In 2001, the United States, next to several other states, launched a military attack called "Enduring freedom".[250] This operation aimed at preventing the usage of Afghan territory as a terrorist base from which terrorist attacks could be launched in the future.[251] This new approach was part of a new strategy, the so-called "Bush Doctrine". This doctrine authorised the right of anticipatory self-defence against terrorism. The announcement by President Bush mentioned that "Because of the new threats that the United States faces, he claimed that a proper understanding of the right of self-defence would now extend to authorizing pre-emptive attacks against potential aggressors, cutting them off before they are able to launch strikes against the US that might be devastating in their scale and scope. Under these circumstances, he concluded, If we wait for threats to fully materialize, we will have waited too long."[252]

Moreover, in 2003 the United States used force against Iraq as a pre-emptive self-defence because they claimed that Iraq had the capacity to use weapons of mass destruction.[253] Maogoto has described the attack on Iraq as "The war against Iraq is the defining moment in the evolution of the "Bush Doctrine" marking a growing coherence and confidence in the strategy of "offensive defence."[254] The principle,

---

[248] UN doc A/59/565 (2004) at 188-92.

[249] M Byers, Terrorism and international law after 11 September ICLQ, Vol 15, (2002), 406

[250] Ibid.

[251] Ibid.

[252] Commencement address by President George Bush at the West Point Military Academy graduation, June 1, 2002, announcing an expansive new policy of pre-emptive military action. The speech can be Available at: the Whitehouse website <http://www.whitehouse.gov/news/releases/2002/06/20020601-3.html> (accessed on Aug. 2003).

[253] Gray C, International law and the use of force,, Ibid. 218-222

[254] J Maogoto, "Rushing To Break The Law? The 'Bush Doctrine' Of Pre-Emptive Strikes And The UN Charter On The Use Of Force; (2003), 7(1) University of Western Sydney, 3

formulated after 9/11, argues that the United States can invoke the right of anticipatory self-defence against any state that harbours terrorists or who allows its territory to be used for the preparation of a terrorist attack – as long as the state is unwilling or unable to prevent these actions or arrest the perpetrators after the fact. As Gill and Ducheine define, these are "defensive measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future."[255] Moreover, the Security Council has a limited role in this regard. Even though, it adopted Resolutions 1368 and 1373 in 2001, it just asserted that all states should fight the terrorism and take any measures to achieve this goal.[256]

Based on the previous discussion, it can be concluded that even though self-defence is an inherent right and exists in international customary law, there are restrictions and limitations drawn by the United Nation Charter in Article 51 and the ICJ judgements. Examples of this are the necessity and proportionality requirements and the duty to report to the Security Council immediately. However, the imminence requirement is controversial because it does, arguably, allow anticipatory self-defence. Nevertheless, it has been widely used after the 9/11 attacks, and during the so-called 'war against terrorism'. This is so because states required to defend their territory against any threat in any way. However, there is another ground for defending a state's integrity and independence, which is the non-intervention principle.

For example, many scholars, such as Vermeer[257], Helal[258] and Ruys[259], do not consider the Saudi air strikes and their current military operation a form of self-

[255] Gill T., Ducheine P, Anticipatory Self-Defence in the Cyber Context, (2013). 89 ILS 438, 452-453

[256] UN Security Council Resolutions, 1373 (28 September 2001); UN Security Council Resolutions, 1368 (12 September 2001).

[257] Zachary Vermeer, The Jus ad Bellum and the Airstrikes in Yemen: Double Standards for Decamping Presidents? Blog of the European Journal of International Law, 2015. https://www.ejiltalk.org/the-jus-ad-bellum-and-the-airstrikes-in-yemen-double-standards-for-decamping-presidents/.

[258] Mohamed Helal, Clouds of War Over the Persian Gulf – A Jus ad Bellum Analysis (Part I),

defence. This is because these scholars argue the Houthi acts do not amount to an imminent armed attack. However, the Saudi position, which is favoured in this thesis, believes these attacks cross the threshold of an imminent armed attack which puts Saudi borders in danger and threatens the Kingdom's peace and security. Based on that, the Saudi government is entitled to use collective self-defence against the Houthi attack. Moreover, there were many missiles directed against Saudi territory, which left Saudi no choice but to defend itself. In the statement of the five Gulf countries of 26 March, it was stated that: "[The Houthi militias] have continued... to build up a military presence, including heavy weapons and missiles, on the border of Saudi Arabia."[260]

Also, Saudi Arabia has announced that "Saudi Arabia and the States members of the coalition responded (...) to the request of the legitimate Government of Yemen (...) in accordance with the principle of self-defence ".[261] It is clear that Saudi Arabia relied on the right of self-defence, especially against this non-state actor attack. Moreover,

---

04.06.2019, http://opiniojuris.org/2019/06/04/clouds-of-war-over-the-persian-gulf-a-jus-ad-bellum-analysis-part-i/.

[259] Tom Ruys and Luca Ferro WEATHERING THE STORM: LEGALITY AND LEGAL IMPLICATIONS OF THE SAUDI-LED MILITARY INTERVENTION IN YEMEN , The International and Comparative Law Quarterly, Vol. 65, No. 1 (JANUARY 2016), pp. 61-98 Published by: Cambridge University Press on behalf of the British Institute of International and Comparative Law Stable URL: https://www.jstor.org/stable/24761357, Accessed: 31-07-2022 08:00 UTC. He justified his opinion by that "the degree of external involvement prima facie appears insufficient to transf the Houthi 'aggression' into an armed attack in the sense of Article 51 U Charter justifying recourse to collective self-defence in support of Yem Second, absent an 'imminent' threat of armed attack, let alone an actual armed attack, by the Houthi rebels against Saudi Arabia, the operation can hardly be construed as an exercise of individual self-defence by the latter country".

[260] GCC statement: Gulf countries response to letter from Yemen president,(Mar 26, 2015), The National News Website, https://www.thenationalnews.com/uae/gcc-statement-gulf-countries-response-to-letter-from-yemen-president-1.4831

[261] UN Doc S/2015/359,2 about "Identical letters dated 19 May 2015 from the Permanent Representative of Qatar to the United Nations addressed to the Secretary-General and the President of the Security Council" https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/148/32/PDF/N1514832.pdf?OpenElement.

there are many states supporting this view, such as the US, the UK, and Canada.[262] Besides, the Arab League's position also confirmed Saudi Arabia's right to self-defence against the Houthi attacks.[263] On the other hand, there are some states arguing against this form of self-defence because they do not see a legal foundation for it. Russia and Iraq are, for example, in this group of states.[264]

---

[262] White House Statement on Yemen, dated 25 March 2015 (n 27) a White House spokesperson, it claimed the operation was undertaken to 'defend Saudi Arabia's border and to protect Yemen's legitimate government ... at the request of Yemeni President ... Hadi' ; United Kingdom, Prime Minister's Office, 'PM Call with King Salman of Saudi Arabia' (27 March 2015) <http://www.gov.uk/government/news/pm-call-with-king-salman-of-saudi-arabia 27-march-2015>. ; Canadian Minister of Foreign Affairs stressed that 'Canada supports the military action by Saudi Arabia and its Gulf Cooperation Council (GCC) partners and others to defend Saudi Arabia's border and to protect Yemen's recognized government at the request of the Yemeni president', 43 Canada, Department of Foreign Affairs, Trade and Development, 'Minister Nicholson Concerned by Crisis in Yemen' (27 March 2015), Available at:<http://www.international.gc.ca/media/aff/ news-communiques/2015/03/27d.aspx?lang=eng.

[263] At a summit of the Arab League, Arab leaders approved of the operation, affirming that its legality was based upon the triad of treaties invoked by Hadi, notably the Arab Treaty of Joint Defence. Tom Ruys and Luca Ferro WEATHERING THE STORM: LEGALITY AND LEGAL IMPLICATIONS OF THE SAUDI-LED MILITARY INTERVENTION IN YEMEN , The International and Comparative Law Quarterly, Vol. 65, No. 1 (JANUARY 2016), pp. 61-98 Published by: Cambridge University Press on behalf of the British Institute of International and Comparative Law Stable Available at: https://www.jstor.org/stable/24761357, Accessed: 31-07-2022 08:00 UTC, p 67.

[264] Russian Federation, Ministry of Foreign Affairs, 'Comment by the Foreign Ministry on the Situation in Yemen' (26 March 2015) Available at: http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f 128a7b43256999005bcbb3/20ca325c9ebff5d943257el40048cd74!OpenDocument; Republic of Iraq, Ministry of Foreign Affairs, 'Foreign Minister: The Summit Needs to Exert Efforts to Find Proper Solution to the Yemeni Issue' (29 March 2015), Available at:< <http://www.mofa.gov.iq/en/ news/foreign-minister-the-summit-needs-to-exert-efforts-to-find-proper-solution-to-the-yemeni issue>.

2.6.2 Self-defence against cyber operations

The prohibition of the use of force, as previously discussed, has generally two main exceptions in international law. Firstly, resolutions of the Security Council authorising the use of force under Chapter VII.[265] Secondly, the right of self-defence, which is recognised in customary international law and also stated in Article 51 of the United Nation Charter. Chapter two has already discussed the right of self-defence as a general rule - this constitutes the basis of examining the right of self-defence against cyber operations. In order to set out an applicable framework for the rules of self-defence in cyber space within Article 51 and customary law respectively, this section will discuss and examine all related issues and requirements to invoke the right of self-defence against cyber-attacks.

Initially, Article 51 stated that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[266] Which reflects the current customary international law.[267] Arguably, the least controversial and most common use of self-defence occurs in cases of armed attacks. While the use of self-defence in cases of "armed attacks" is universally accepted and has been confirmed by many scholars, the question is whether a cyber operation could qualify as an armed attack, or whether allowing the use of self-defence against cyber operations would be a broadening of its scope. Schachter noted that:

"Some commentators have gone so far as to contend that economic action of such intensity and magnitude would justify forcible self-defence by the target state, and collective defence by its allies. I disagree. Even egregious economic aggression, whether or not illegal, does not constitute an armed attack or a use of force in the

[265] Charter of United Nation, Ibid,.Article 42.

[266] Ibid.

[267] M. Schmitt, The Law of Cyber Warfare, Ibid, 281, Kammerhofer, Jörg, The Resilience of the Restrictive Rules on Self-Defence in Marc Weller (ed.), The Oxford Handbook on the Use of Force in International Law (2015), OUP, 632.

Charter sense. Allowing forcible reprisal to non-military coercion would broaden the grounds for use of force to an intolerable degree."[268]

Schachter forcefully criticised the broadened scope of self-defence and asserted there needs to be a limit of responding with force against such an 'armed attack' because it will otherwise result in out of control use of force.

The report of the International Law Commission on the Work of The Thirty-Second Session in 1980 has stated that:

"It is often said that acts of unarmed aggression also exist (ideological, economic, political, etc.), but even though they are condemned, it cannot be inferred that a state which is a victim of such acts is permitted to resort to the use of armed force in self-defence. Hence, these possibly wrongful acts do not fall within the purview of the present topic, since recourse to armed force, as analysed in the context of self-defence, can be rendered lawful only in the case of armed attack."[269]

The most notable term that has been used in this statement is "aggression". It further underlines and distinguishes armed and unarmed aggression. The Commission makes clear that any type of aggression other than an armed attack does not permit the use of self-defence. For more clarification, the term aggression is not a synonym of "armed attack".[270] In fact, armed attack is one particular form of aggression.[271] The definition of aggression in international law is "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition".[272] This reflects the broad meaning of aggression.

Since the 1980s, there have been a number of cases which enabled the ICJ to further specify its interpretation of the law. Given that an armed attack determines if

---

[268] O. Schachter, In Defence of International Rules on the Use of Force, Ibid, 127.

[269] U.N. Doc. A/35/10, reprinted in [1980] II(2) Y.B.I.L.C. 53, n. 176.

[270] Y. Dinstein, Computer Network Attacks and Self-Defence, Ibid,100.

[271] Ibid.

[272] Definition of Aggression On 14 December 1974, the General Assembly adopted by consensus resolution 3314 (XXIX). Article 1.

the right of self-defence is applicable, one must ask what amounts to an armed attack in international law. In 1986, the ICJ answered it in the negative in the Nicaragua case by stating what does not constitute an armed attack: “a mere frontier incident”.[273] On the other hand, almost 20 years later, in 2003, in the Oil Platforms case (Iran v. US), the ICJ noted that attacking “a single military platform or installation could rise to the armed attack level”.[274] Therefore, the level of the armed attack which is required to exercise self-defence must be an area between a military attack and a mere incident.

Two years after the Oil Platforms case, in 2005, the ICJ also rejected a broad interpretation. It commented on the case of *Armed Activities on the territory of the Congo* that: “Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters”.[275] The ICJ thereby confirmed a strict and limited reading of the use of force in self-defence situations - not allowing states to use other security interests to justify the use of force. However, irrespective if one follows the broad definition of armed attack or the limited one, the concept needs to be identified clearly, as will be illustrated below.

2.6.2.1 Cyber Armed Attack

Before and certainly since the publication of the Tallinn Manual, scholars have debated whether the general rules of international law apply also to the cyber space.[276] The author of this thesis strongly agrees with the Group of Experts that the

[273] Nicaragua case, 195. The ICJ also noted that “… it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein".

[274] Oil Platforms (Islamic Republic of Iran v. United States of America), ICJ, 57-61, (2003). See also M Schmitt, The Law of Cyber Warfare: QUO VADIS? , Ibid, 282.

[275] Case Concerning Armed Activities on the Territory of the Congo,Ibid, at 223–4.

[276] Dong, Yao.. The “jus ad bellum” in cyberspace: Where are we now and what next? New Zealand Journal of Public and International Law, (2019), 17(1), 41, 41-42.

law should be applied in this way. She, however, realises that there is not always sufficient evidence of customary international law to claim this Manual represents the *lex lata*. Therefore, states should consider regulating this issue further to remove confusion and enable swift responses to protect states' security.[277] The following parts will discuss this in more detail.

To legally use the right of self-defence against a cyber operation, a certain level of armed attack is also required. However, what does this mean in relation to cyber-attacks?[278] In Rule 71 of the Tallinn Manual, it is stated that "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its "scale and effects."[279] This rule confirms the requirement to qualify the force used in the act as an armed attack in order to lawfully use self-defence.[280] Moreover, the Group of Experts agreed unanimously on the scope of the armed attack, which is "any use of force that injures or kills persons or damages or destroys property".[281] That agreement is based on the ICJ Advisory Opinion on the *Threat or use of Nuclear Weapons,* which requires an armed attack regardless of the means of the attack.[282] It can be understood from the Tallinn Manual Experts' view in regard to the use of mass destructions weapons such as chemical or biological attacks which cause massive destruction and result in death and injury, that it is universally

[277] See also Hoisington, Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence, (2009), 32 B.C. Int'l & Comp. L. Rev. 439

[278] Harrison, Dinniss, Heather. Cyber Warfare and the Laws of War, (2012),CUP,40.

[279] Tallinn Manual (2017), 339.

[280] For Germany's position on self-defence in the cyberspace see: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; Similarly the UK's position: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf.

[281] Ibid. States like Germany, the US, the UK, France or India have so far not considered the stealing of information as use of force, 55.

[282] Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, [1996], ICJ, Para 39.

accepted they constitute an armed attack. This could be used as a model for cyber operations.[283]

It has been noted that the criteria to identify an armed attack which is drawn from Rule 71 are "the scale and effect".[284] These criteria were derived from the ICJ judgement in Nicaragua case, which was identified previously.[285] The Group of Experts in the Tallinn Manual adopted this view when assessing the concept of armed attacks in cyber operations, and they consider these criteria as an unsettled matter.[286] However, these Experts agreed that the destructive effect of a cyber operation would meet the "scale and effect" criteria.[287] Moreover, Dinstein clarified the Tallinn Experts' view with examples of some cyber operations which amounts to an armed attack such as "an extensive power grid outage creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas"[288]. As a result, the question here is: What happens if the cyber operation has only non-destructive consequences - does it meet the scale and effect parameter? Could it amount to an armed attack? Referring to the analogy with biological or chemical weapons: would the mere use of a cyber operation be enough, irrespective of any harm - similarly to the use of chemical or biological weapons? The author would indeed say yes, one can make this comparison.

With regard to non-destructive cyber operations, Schmitt's view is that non-destructive cyber operations do not rise to the level of an armed attack such as cyber theft or intelligence gathering which is reflected in state practice also, as discussed above.[289] Nevertheless, in some cases the cyber operation could result in severe non-destructive or non-injury consequences such as excessive cyber operation

[283] Tallinn Manual, (2017), 340.

[284] Nicaragua case, 195.

[285] Ibid.

[286] Tallinn Manual,(2017), 341.

[287] This is not always followed in practice. E.g. in the conflict between Russia and Georgia over South Ossetia there had been small scale attacks for months before any hostilities broke out. See Dinstein, Computer Network Attacks and self-defence, Ibid 54.

[288] Dinstein, Computer Network Attacks and self-defence, Ibid,105.

[289] M Schmitt, The Law of Cyber Warfare: QUO VADIS? , Ibid, 282.

against states' economic infrastructure. That has been illustrated by Gill when he stated that "an armed attack could arguably include a cyber-attack directed against a State's critical infrastructure, provided the cyber-attack had the potential to severely cripple a state's ability to carry out and ensure conducting of essential State functions or severely undermine its economic, political and social stability for a prolonged period of time".[290] He subsumes such non-destructive cyber-attacks targeting economic, political, and social stability as an armed attack. He also illustrated that the armed attack could be constituted regardless of the physical injury or damage. In his opinion, it is enough if "potential disruption of a State's essential functions or stability was severe".[291] He relied on the effect on the State's critical infrastructure. However, as mentioned in the previous part, the definition of the critical infrastructure is unsettled.[292] Therefore, every state has its own definition.

Furthermore, Habibi and Baradaran have a similar view to Gill in regard to the necessary intensity of cyber-attacks which do not cause "material damage or death of human beings" unlike an armed attack. They argue this because such attacks target critical infrastructure "which paralyse the government departments or cause large-scale destruction in them".[293] This view also has been justified with this statement: "It is not their physical destruction as such, but their unavailability in the sense of not being able to fulfil the purpose for which they have been set that makes an attack on them an armed attack".[294] On the other hand, Roscini requires a high intensity of "destruction or disturbing" to constitute an armed attack.[295] He emphasised that if the cyber-attack does not cause "material damage" to the national

---

[290] Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defence in the Cyber Context, (2013).89 INT'L L. STUD. 438

[291] Ibid.

[292] The GGE report also recognises this without defining critical infrastructure: Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (2021), 7.

[293] Nazanin Baradaran and Homayoun Habibi, 'Cyber Warfare and Self-Defence from the Perspective of International Law' (2017) 10 J Pol & L, 40.

[294] Tsagourias, Nicholas, Cyber-attacks, Self-Defence and the Problem of Attribution, (2012), 17(2) Journal of Conflict & Security Law, 229–244, 231

[295] Roscini, Cyber Operation and the Use of Force in International Law, Ibid, 73-77.

infrastructure, it could still amount to an armed attack in the case when a "coordinated cyber-attacks seriously disturbing several or all NCIs of heavily digitized state for prolonged time".[296] It is obvious that Roscini has a high threshold for non-destructive cyber-attacks. He requires a high level of the scale and effect to meet the threshold of an armed attack.

As an example of a state's political position, the United States requires some "disruptive activity in cyber space" for an armed attack character.[297] The US made its position on when the use of force can be considered as an armed attack clear when the Office of General Counsel of the US Department of Defence stated that:

"[I]f a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no-one would challenge a victim nation if it concluded that it was the victim of an armed attack, or of an act equivalent to an armed attack"[298]

Nevertheless, the US also agrees: "It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack."[299] This means, in the US's view, there needs to be a threshold crossed. However, they do suggest they have a right of "self-help" short of self-defence to expel the attacker and also prevent re-entry. "It seems beyond doubt that any unauthorised intrusion into a nation's computer systems would justify that nation at least undertake self-help actions to expel the intruder and to secure the system against re-entry. An unauthorised electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty"[300]

---

[296] Ibid.

[297] UN Doc. A/66/152,at 18.

[298] Office of General Counsel, An Assessment on International Legal Issues in Information Operations, United States Department of Defence (1999) www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

[299] Ibid.

[300] Ibid.

This case is still an unsettled matter even between the Group of Experts and among states. Some members of the Group of Expert extend the effect beyond the destructive or injury criteria, whereas others have a restrictive view to classify it as a necessary condition.[301] In this context, one also needs to consider cyber operations which have a financial loss as effect. Some members of the Group of Expert do not accept it as an armed attack. Others characterise this as an efficient effect to constitute an armed attack, and they describe it as "Catastrophic effect".[302] While others add a condition, which is that the cyber operation must be directed to critical infrastructure and cause a severe effect.[303] On the other hand, the Group of Experts agreed unanimously that the "effect" must be a "reasonably foreseeable consequences of the cyber operation".[304] Ohlin criticised this "approximate cause standard" by naming many difficulties, especially in the case of the stock market crash.[305] However, Ohlin assumed a chain of causation of cyber operations because the possibility of human intervention in the form of looters and rioters which affect the chain of causation comes into question. On the other hand, Harrison, Dinniss and Heather argue for the "effect" criteria by noting that "A state is therefore permitted to respond in self-defence when it is the victim of a computer network attack causing damage to property or persons of sufficient scale and effect to elevate it beyond the equivalent of a frontier incident".[306] In other words, they used the "frontier incident" as an evaluation tool to determine the scale and effect of the attack.

In the same context of the "effect" of the attack, the Group of Experts is divided into two camps regarding the intention of the attacker and whether it has a severe effect. For instance, in a situation where a state commits cyber espionage against another but unintentionally causes severe damage to the state's cyber

[301] Tallinn Manual, (2017), Ibid, 341.

[302] Tallinn Manual, (2017), Ibid, 343.

[303] Ibid.

[304] Ibid.

[305] Ohlin J, Cyber Casuation", in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) Cyber War: Law and Ethics for Virtual Conflicts (Oxford University Press, Oxford,(2015), 45.

[306] Dinniss,. Cyber Warfare and the Laws of War, Ibid, 81

infrastructure.[307] The majority of the Experts consider it as an armed attack because they argue intention is irrelevant in the assessment of an armed attack.[308] Nevertheless, a minority of the Expert does not agree with this assessment because the effect was not intended.[309] Schmitt has commented on the Expert's view, saying "states will begin to treat such cyber operations as armed attacks to which they can respond forcefully when the consequences are sufficiently severe".[310] However, the Experts in the Manual agreed that the Stuxnet attack amounts to an armed attack based on its scale and effect. Roscini and O'Connell have criticised this view, saying it "goes too far".[311] This thesis's view on the Stuxnet attack has been illustrated in Chapter Four. To reiterate, the author classifies Stuxnet as an armed attack because the attack had a high level of intensity which meet the required level of scale and its consequences affected a significant facility in Iran which is considered a substantial element in the state.[312]

Another important issue regarding the phrase "armed attack" is that it may cause confusion because of the term "armed" which could indicate the necessity of involving "weapons". The Group of Expert concluded that as long as the effect of the cyber-attack is equivalent to a kinetic armed attack, it will meet the requirement irrespective of the weapon.[313] The thesis agrees with that assessment. However, the author would also like to point out that the "weapon" classification is not an issue regardless since cyber operations involve the use of malware, viruses and other destructive instruments which can be considered as weapons based on the previous discussion in part one. Interestingly, Schmitt concluded that once the cyber operation

---

[307] Ibid, 343.

[308] Ibid.

[309] Ibid.

[310] M Schmitt, The Law of Cyber Conflict: Quo Vadis?, Ibid, 283

[311] Roscini, Cyber Operation and the Use of Force in International Law, Ibid, 73-77.

[312] On the definition of armed attack and how its gravity and effect are used rather than the instruments used see: Nicholas Tsagourias, Cyber-attacks, self-defence and the problem of attribution, Journal of Conflict and Security Law, Volume 17, Issue 2, Summer 2012, Pages 229, 231.

[313] Tallinn Manual, (2017), Ibid, 34, Tsagourias, Cyber-attacks, self-defence and the problem of attribution, Ibid, 231

amounts to an armed attack, it will be dealt with as an “armed attack” not as an “information operation”.[314] He means that self-defence will be permissible against the armed attack, not the cyber operation itself. The present author does not agree with this statement, because we cannot ignore the fact that this armed attack originated from a cyber source. Therefore, characterising the cyber operation as an armed attack will not remove the cyber element from the attack. It should be dealt with as a “cyber armed attack”.

2.6.2.2. Accumulation of events within cyber context

In the context of classifying the operation as an armed attack, there is a case when a cyber-attack launches in several small-scale operations. As shown in a previous section of this Chapter, these series of attacks are known as “accumulation of events” or “pinprick”. The question here is whether these attacks together constitute an armed attack or not. Schmitt answered that question by saying these attacks are “constituent parts of a single broader campaign”.[315] Which means that he required the attacks to be connected to each other and equivalent to one attack amounting to an armed attack. Tsagourias, more hesitantly, agrees that an accumulation of cyber-attacks can indeed rise to the level of an armed attack and can trigger the right to self-defence.[316] This situation has been compared to an attack using “more than one soldier, or wave of bombers in an air strike”.[317] This is an appropriate image of the accumulation of events in cyber space.

Interestingly, France recognised this type of attack and stated that “if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or

---

[314] Schmitt M, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Ibid, 42.

[315] Michael N Schmitt "The Use of Cyber Force and International Law" in Marc Weller (ed) The Oxford Handbook of the Use of Force in International Law,(2015) OUP, 1121.

[316] Tsagourias, Cyber-attacks, self-defence and the problem of attribution, Ibid 233.

[317] Dinniss,. Cyber Warfare and the Laws of War, Ibid, 95

from different entities acting in concert."[318] Even though the ICJ does not have a clear position about this situation, it indicates in the Oil Platform case and Nicaragua case[319] that a series of small-scale attacks against the same target will amount to an armed attack.

Moreover, the ICJ in (DRC v Uganda) Armed Activities Case, the court considered the accumulation of events as an armed attack but concluded it did not apply in this case. The court stated that "even if this series of deplorable attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC".[320] The Group of Experts in the Tallinn Manual has considered this situation and agreed on equating the small-scale incidents of cyber operations as an armed attacks based on the scale and effect evaluation.[321] This thesis agrees with this by saying that a series of cyber-attacks could have the same damage and effect to the state as one individual cyber-attack. As a result, to protect the state from such cyber operations and provide the legal grounds for the state to respond, it has the right to use self-defence as the accumulation of cyber-attacks constitutes an armed attack.

As a final point, irrespective if the armed attack originated from one scale invasion or multiple small scales of attacks, if the act meets the scale and effect assessment, it will trigger the right to self-defence.

2.6.2.3. Self-defence against cyber operation by Non-state Actors

The previous discussion assumed the attacker is a state. However, what rules apply if the cyber-attack is launched by a non-state actor? The ICJ, in the Nicaragua case, stated that "'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (inter alia) an actual armed attack conducted by

[318] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, (2019), 8, Available at : https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)

[319] Oil Platform Case, Para 18; Nicaragua Case, 195.

[320] (DRC v Uganda), Armed Activities on the Territory of Congo, para. 146

[321] Tallinn Manual (2017), 342.

regular forces, 'or its substantial involvement therein."[322] Therefore, the non-state actor cyber-attack would amount to an armed attack if it is directed by or on behalf of a state.[323] However, in the aftermath of 9/11 the international community began to consider a non-state actor as a trigger for self-defence even without a direction by a state and characterised it as "self-defence against terrorist".[324] This is supported by the fact that Article 2(4) of the Charter only applies to inter-state relations, whereas Article 51 does not specify against whom self-defence is permissible. It stands to reason that, therefore, self-defence is permissible against any aggressor.[325] Even though the Security Council cannot change international law, it illustrates its position in this regard. It adopted some resolutions, such as the Res. 1368 and Res. 1373 in 2001, which reaffirmed the inherent right of individual or collective self-defence against terrorism.[326] Nevertheless, the ICJ has not adopted any view in this regard, which can be deduced from the Wall Advisory Opinion and the Nicaragua case.[327]

In this context, the majority of the Group of Expert confirmed the state practice in this regard and concluded that cyber-attacks by terrorists amount to an armed attack, which consequently allows the use of self-defence.[328] On the other hand, the minority of the Experts reject this approach as a matter of law.[329] The author, however, agrees with classifying the cyber-attacks by terrorists as an armed attack as the act of terrorism constitutes a threat to international peace and security. Besides this, the terrorist's goal from the cyber-attack is more than just disrupting the

---

[322] Nicaragua case, 195.

[323] This would also mean that these actions are likely attributable to the state as set out in the Nicaragua case. See Tsagourias, Cyber-attacks, self-defence and the problem of attribution, Ibid, 236.

[324] Tallinn Manual , (2017), Ibid, 344. The GGE report also recognises this: see 7.

[325] Dinniss, Cyber Warfare and the Laws of War, Ibid ,96.

[326] UN Doc. S/RES/1368 (12 September 2001); SC Res. 1373, UN Doc. S/RES/1373 (28 September 2001).

[327] Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice,[2019], ICJ , Para.139available at: https://www.refworld.org/cases,ICJ,414ad9a719.html [accessed 1 April 2020] ;Nicaragua case,Para. 146-147.

[328] Tallinn Manual, (2017), Ibid, 345

[329] Ibid.

servers. The attack will serve their own terrorist interests, such as gathering information to target the most vulnerable place to plant a bomb or using cyber means to open a dam instead of bombing it. Moreover, cyber terrorist could use cyber means to hack the air traffic system. Therefore, their act needs to be terminated, as state's will need to take steps to defend their territory from any terrorism act.

In the case of cyber operation, there is a likely possibility that the attacker launched the cyber-attack from another state's territory. The majority of the Experts accept the use of self-defence against said state if the state whose territory has been used for this attack is unable or unwilling to take defending actions and terminate this attack.[330] Dinstein called this form of self-defence "extraterritorial law enforcement" or "state of necessity". However, this must not be confused with 'necessity' as defined in the law of countermeasures, as set out in Rule 26 which discusses that the wrongfulness of an act is precluded if the operation is undertaken in a situation of 'necessity'.[331] Yet, the minority of the Experts are against this view in the absence of state consent or an authorisation under Chapter VII by the Security Council.[332]. Schmitt looked at this issue by considering the degree of organisation of the group. He does not consider an attack by an unorganised non-state actor group as an armed attack.[333]

However, the author maintains that the unwilling and unable test, which has been discussed previously, is the most useful examination of the event to determine the use of self-defence against the non-state actor. This is because the focus should be on remedying and stopping the attack. However, states have a divided view in this regard. For instance, Germany has accepted that self-defence against cyber-attacks from non-state actors is permissible.[334] On the other hand, France rejected

---

[330] Tallinn Manual, (2017), Ibid, 347

[331] Yoram Dinstein, Computer Network Attacks and Self-Defence, Ibid, 108, This Necessity is not the same in the context of state responsibility which allow the using of countermeasures.

[332] Ibid.

[333] M Schmitt "The Use of Cyber Force and International Law", Ibid, 1123.

[334] Deutscher Bundestag, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE", BT-Drs. 18/6989, (2015) 11.

this position and requires the cyber operation to be attributed to the state itself.[335] While, in Saudi Arabia, the position has not been stated in documents, one can assume their approach given its attitude against the Houthi group in Yemen. Therefore, one can assume Saudi supports the idea of self-defence against non-state actors. Saudi Arabia led a coalition of nine countries from West Asia and North Africa[336] to respond to the Houthi armed attack. In the non-state actor context, states will have a duty to protect their territory from being used by non-state actors to launch cyber operations against another state. As Dong commented: "This may entail the expansion of the obligation to cover the provision of a virtual shelter to a hacker group. Thus, host states may have an increased duty to control their IT systems".[337] Given that cyber operations could be launched from many locations, it means all states will be obliged to follow the due diligence principle. The due diligence principle in relation to cyber activity in a state's territory will be examined in the upcoming parts.

One final big point in this regard is the attribution problem. In cyber space, it will be hard to track the source of the attack. Moreover, there is a possibility that the origin of the attack may be manipulated by the terrorist group to mask the true place of origin. Dinniss takes this into consideration when expressing their view on attribution of a non-state actor cyber-attack, by emphasising that the problem revolves around how to prove the level of state involvement.[338] Moreover, Dinniss highlighted more issues related to the assessment of proportionality in the case of non-state actor cyber operations. This includes identifying an acceptable target in a state since the attacker is a non-state actor and only located there.[339] However, the

---

[335] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, Ibid, 8-9.

[336] Egypt, Morocco, Jordan, Sudan, the United Arab Emirates, Kuwait, Qatar, Bahrain, and Academi (formerly called Blackwater) took part in the operation. Djibouti, Eritrea.Available at: https://dbpedia.org/page/Saudi_Arabian%E2%80%93led_intervention_in_Yemen

[337] Yoa Dong , The Jus Ad Bellum in Cyberspace: Where Are We Now and What next?, (2019), 17 NZJPIL, 41, 55

[338] Dinniss, Cyber Warfare and the Laws of War, Ibid.96

[339] Ibid.

GGE report makes clear that states should not knowingly allow their territory to be used for internationally wrongful acts using cyber technology.[340] Nevertheless, the thesis agrees with the view that the proportionality question must be assessed on a case by case basis because when a state needs to respond with a proportionate defence to the attack, it needs to look at the level of the attack and its circumstances which will vary from case to case. Another problem in regard to the attribution was flagged by Waxman: "even if investigation processes can trace a cyber-attack back through digital networks to its source, it may be difficult to publicize that information in a timely and convincing way."[341] Nevertheless, this is not a fundamental barrier against achieving attribution because publicising the information would not be necessary as states could distribute this in a classified way until they have decided on the act of defence. Furthermore, as Lotrionte commented on the publication question: "there is no requirement under international law for states to publicly disclose the basis for its attribution assessments."[342] Even in the GGE reports, there was no requirement to publicly disclose any information about the attribution.[343]

According to the GGE report, states must however be mindful that they cannot violate the principle of non-intervention in another state. Consequently, it must make sure that the attribution to a state is clear so that it can indeed direct its right to self-defence against said state's territory.[344] The attribution problem exists not only in non-state actor cases, it is also an issue surrounding the examination of cyber operations in general. However, the non-state actor cyber operation could still be attributed to a state if it has been proven the group acted on behalf of the state or under its direction. This does not include cases where the state is unable or unwilling to terminate non-state actor operations. In these situations, the state will be responsible for that cyber-attack and trigger the right of self-defence against it.

---

[340] UN GGE Report 2015, 10.

[341] Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), (2011).36 Yale J. Int'l L. 444

[342] Lotrionte C., Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law, (2018), 3, (2) CDR, 73-114.

[343] UN GGE Report 2015, para. 28(f).

[344] Ibid, 17 (para 70 (c)).

2.6.2.4. Necessity and Proportionality

Besides the condition of requiring an "armed attack" to exercise the right of the self-defence, there are four conditions that need to be met. These are necessity, proportionality, imminence, and immediacy. The necessity and proportionality requirements of the counter-attack as self-defence have been acknowledged by the ICJ in several judgements: the Nicaragua case, the Oil platforms judgement beside the Nuclear Weapons advisory opinion.[345] The necessity requirement demands that defensive force is needed to defeat the attack, and that non-forceful measures would be insufficient to do so.[346] The proportionality requirement limits the scale, scope, intensity and duration of the defensive act.[347] The Group of Expert in Tallinn noted that cyber operations may be deployed in response to a kinetic armed attack and *vice versa*. They stated that "A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.".[348] Gill illustrates the proportionality requirement by stating that:

"If a digital attack rises above the threshold of armed attack, the response may be to employ cyber weapons or kinetic force or a combination of the two to neutralize the attack, as long as the response did not exceed that required to repel the attack."[349]

Which means that proportionality will be assessed on a case by case basis, without being "construed too strictly".[350] Dinniss asks how appropriate the use of traditional armed force in defence against a cyber-attack is. [351] Nevertheless, he agrees that the cyber-attack has been used to "prepare the battle space for a

[345] Nicaragua judgement, paras. 176, 194; Oil Platforms judgement, paras. 43, 73–74, 76; Nuclear Weapons advisory opinion, para. 41.

[346] For more details see Chapter Two page…., also see. C Gray, International Law and the Use of Force, Ibid, 148-155.

[347] Tallinn Manual, (2017), Ibid, 349.

[348] Ibid, 348

[349] Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defence in the Cyber Context, Ibid, 450

[350] Y Dinstein, War, Aggression and Self-Defence, (1994), 86 CUP, 210.

[351] Dinniss, Cyber Warfare and the Laws of War,Ibid, 104.

conventional attack".[352] Moreover, Gray agrees and argues states are not required to use the same weapons or same number of armed forces in response to be proportionate.[353] This thesis's view is that it will be difficult to specify the proportionality scope because it depends entirely on the nature and intensity of the attack, and that will vary from case to another. However, the required element of proportionality is not to exceed the level of the original attack. If the cyber-attack reaches a level of intensity which requires a response with kinetic methods, it might still be considered proportionate because it is not about the type of the self-defence, but it is about the intensity of the attack.[354]

Regarding state's positions on this, the United States announced that it will use any method to respond to cyber-attacks, even if it is with a nuclear weapon.[355] Russia has the same position. It has been stated by officials that "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then the aggressor state itself."[356] However, this statement is still controlled by the proportionality condition. Russia has made it clear that choosing this means to respond is "in accordance with the norms and principles in international law".[357] This position complies with previous ICJ rulings and the UN Charter. As the court stated in its Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, "The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons."[358] Moreover, the US's and

---

[352] Ibid.

[353] C Gray, International law and the use of force, Ibid, 150.

[354] Ibid.

[355] David E. Sanger and William J. Broad , U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber-attack, (16 Jan 2018) , Available at: https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html [Accessed on 21 Jan 2023]

[356] Rosicni, Cyber Operation and the Use of Force in International Law, Ibid. 70.

[357] Ibid.

[358] Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ, 1996, Para 39 . It is worth to mention that even though the use of nuclear weapons in self defence might comply with the jus ad bellum, it would almost certainly violate the jus in bello and human rights law and the court in the same judgement require the use of these weapons to comply with humanitarian law and human rights law .

Russia's position indicate the huge effect of cyber operations on states, which demand to respond to such attacks by any means necessary to defend the state. Iran, as a state owning nuclear weapons, likely has a similar position to Russia, and they may consequently use nuclear weapons as a response to cyber-attacks. However, Saudi Arabia does not have a written document or any other official statement which could illustrate its position in this regard, but it tends to have similar views to the United States. In Saudi Arabia's war in Yemen, Saudi did not hesitate to use any method in response to Houthi's attack: Saudi military used drones and Apaches.[359] President Biden strengthened the Saudi position in this regard by declaring that the US will support Saudi "to help strengthen its defences, as necessitated by the increasing number of Houthi attacks into Saudi territory". Therefore, Saudi Arabia will go as far as required to defend its territory from any attack, whether it is kinetic or cyber.

2.6.2.5. Immediacy and imminency

The imminence and immediacy requirement has been confirmed in Rule 73 of the Tallinn Manual: "The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy."[360] An imminent cyber-attack could, for example, occur when there is intelligence information about another state preparing for a cyber-attack which will destroy the former's primary oil pipeline within two weeks. In this case, the state has the right to use force in self-defence to protect its critical infrastructure, which includes the oil pipeline, against this imminent threat.[361] Immediacy means the period of time between the attack and the act of self-defence, which needs to be in a reasonable relation.[362]

---

[359] Biden's $500m Saudi deal contradicts policy on 'offensive' weapons, critics say | US foreign policy | The Guardian available at : https://www.theguardian.com/us-news/2021/oct/27/joe-biden-saudi-arabia-arms-weapons-deal [Accessed on 31 Jan 2023]

[360] Ibid.

[361] Tallinn Manual , (2017), Ibid, 352.

[362] Ibid, 353.

In regard to the imminence requirement, there are two possibilities. The first one is when the attack has been launched already and that indisputable. The second one is when there is an imminent threat, or the attack is about to be launched. The defence against this type of attack is called “anticipatory self-defence” which has been discussed in detail before.[363] In the cyber context, it is important to assess what an imminent cyber threat would look like. The same divide as to how Article 51 should be interpreted also exists regarding cyber-attacks. To reiterate, Article 51 declares that states have the right to self-defence if an armed attack ‘occurs’. As Milanovic explains regarding Russia’s armed attack against Ukraine in February 2022, the definition of imminence must allow the (potential) attacker to change his mind. Therefore, a state must not start pre-emptive self-defence too soon, as they might then actually trigger a conflict that otherwise would not have occurred.[364] Therefore, it remains a difficult to properly define imminence.

Going back to the cyber-realm, Dinniss suggests assessing the target when weighing imminence. If the target is a warning system, emergency response system or military communication system, he suggests the cyber operation should be classed as imminent. On the other hand, if the target is an electric power grid or financial system, it will not constitute an imminent armed attack until there are other indicators of it. Greenwood based its determination on two factors: the method of delivery and the gravity of the attack.[365] However, Schmitt requires three conditions in determining imminency.[366] The capability of the attacker, its intent to commit an armed attack, and the target state losing the “last window of opportunity” to response.

The Schmitt-view aligns with the majority of the Group of Experts. They adopted the criterion of “last feasible window of opportunity” which means the state may act in self-defence in that moment because waiting will render the state unable

---

[363] See page 37.

[364] Milanovic M, “When Did the Armed Attack against Ukraine Become 'Imminent'?” EJIL, (April 20, 2022) Available at: https://www.ejiltalk.org/when-did-the-armed-attack-against-ukraine-become-imminent/ [Accessed on 21 Jan 2023]

[365] Christopher Greenwood, ‘International Law and the Pre-Emptive Use of Force: Afghanistan, Al-Qaida, and Iraq’ (2003) 4 San Diego Int’l L.J. 7.

[366] M Schmitt, The Law of Cyber Warfare: QUO VADIS?, Ibid. 285

to defend its infrastructure and make it lose its opportunity to act. Schmitt reasoned he "combined the requirement for a very high reasonable expectation of a future attack with an exhaustion of remedies component."[367] Moreover, Lubell characterised the "last window of opportunity" standard as "opening up a wider temporal framework with no regard to the immediacy of the threat."[368] While Roscini has required an evaluation of "the last window of opportunity" in good faith.[369] For the aim of this thesis, the author supports "the last window of opportunity" standard. The reason for favouring this standard is because it achieves the goal of anticipatory self-defence against the cyber-attacks, which is defending the state against any cyber operation could happen in seconds. Moreover, it is not easy to prove the existence of an imminent cyber-attack, which makes invoking the right of anticipatory self-defence very difficult. This means in practice, it will not occur often, but it can sometimes be a necessary step to prevent harm. Due to all of this, there needs to be "clear and convincing evidence of the imminent attack".[370] The author therefore is of the opinion that this high threshold is enough to safeguard good faith, and does not see any problems with allowing the "last window of opportunity" standard.[371]

However, Roscini and Gill consider anticipatory self-defence in cyber space as an "impossible task" to be achieved.[372] That is due to the difficulty of determining many necessary factors of a cyber operation's origin, its nature, assessing imminency and even the proportionality and necessity of the operation.[373] Gill based his argument on the fact that there is no cyber operation in the history of cyber

---

[367] Schmitt M., Preemptive Strategies in International Law, (2003).24 MICH. J. INT'L L. 513, 534–35

[368] Lubell N., The Problem of Imminence in an Uncertain World, in THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW, 697–98, 702–05.

[369] Roscini, Cyber Operation and the Use of Force in International Law, Ibid.80

[370] Ibid.

[371] This reflects the Caroline Doctrine which is generally accepted as international law. See also Hoisington, Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence, Ibid, 450. For a broad discussion: Gill and Ducheine, Anticipatory Self-Defence in the Cyber Context, Ibid.

[372] Roscini, Cyber Operation and the Use of Force in International Law, Ibid, 79-80.

[373] Ibid

operations that could constitute an imminent armed attack by itself.[374] However, the cyber operations combined with a kinetic attack could amount to an imminent armed attack. That is because there is a state practice of recognising such combined attacks. An example would be the Russia and Georgia conflict regarding South Ossetia, where they

"support the military operations by degrading or neutralizing weapons and military communication system".[375]

Despite all the criticism of cyber anticipatory self-defence, there is still a need for it because the targeted state will find itself in a situation in which it has no choice but to respond by anticipatory self-defence to protect its infrastructure or its territory as a whole. As cyber operations could come in many forms, they could be discovered as a threat before they have been fully launched against the state. It would be unreasonable to expect of the victim state to suffer the first blow – especially because this could mean the victim state cannot react at all.[376] Depending on the type of cyber-attack, the first blow might be the only blow. Alternatively, there are types of attack that appear innocent at first but then evolve into an armed attack. One of these forms is known as "backdoor payload".[377] This technique prepares the cyber battlefield. It will infect unprotected computers which then will connect to others, which are known as "botnets".[378] Some scholars do not consider that type of operation as an imminent armed attack because of the time variety, which could take

---

[374] Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defence in the Cyber Context, Ibid, 461.

[375] Ibid.

[376] See the legal advice for President Bush regarding Iraq: Bybee JS, "Authority of the President under Domestic and International Law to Use ..." (*Opinions of the Office of Legal Counsel*October 23, 2002) <https://irp.fas.org/agency/doj/olc/force.pdf>

[377] "A backdoor is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms." While Payload is "refers to the component of a computer virus that executes a malicious activity. Apart from the speed in which a virus spreads, the threat level of a virus is calculated by the damages it causes. Viruses with more powerful payloads tend to be more harmful." Harrison, Dinniss, Heather. Cyber Warfare and the Laws of War, Ibid,88-89

[378] Ibid

months or years until the final attack is launched.[379] However, the author of this thesis previously explained that the idea of the existence of such malware in state's computers or servers will constitute an imminent threat, regardless of the time required to launch the final attack. Precisely this is the object and purpose of anticipatory self-defence, to protect the state from these main effects before they happen. As a result, from the date on which the state discovers the malware or this operation, the threat becomes imminent. The most important condition which needs to be considered carefully is that the state responds proportionately to the cyber operation. The author agrees that anticipatory self-defence as set out in the Tallinn Manual, is permissive, she, however, also concedes that it is a controversial opinion, which is underlined by the criticism of a number of scholars.[380]

2.6.5.6. Concluding points on cyber self-defence

In addition to the four requirements (necessity, proportionality imminence and immediacy), there is one other significant requirement derived from Article 51 of the United Charter, which is reporting the attack to the Security Council. This is also reiterated in Rule 75 of the Tallinn Manual with regard to Cyber-attacks.[381] Not reporting to the Security Council does not divest the right of self-defence, but it violates Article 51 of the Charter. Moreover, whenever the Security Council decides to take measures to maintain peace and security, the right of self-defence is terminated unless these measures are not effective.[382]

Lastly, it is worth noting that the right to self-defence is not just an individual right, it could also be exercised in a collective way.[383] Rule 74 of the Tallinn Manual requires a request from the victim state, and the assisting state or states must act

[379] Ibid.

[380] C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1633-1636

[381] "Measures involving cyber operations undertaken by States in the exercise of the right of self-defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council." Article 75, Tallinn Manual, (2017), 355.

[382] C Gray, International Law and the Use of Force, Ibid, 121.

[383] See Chapter Two page…

within the scope the ICJ set out in the Nicaragua case.[384] Moreover, collective self-defence could be based on a treaty such as the NATO treaty or an *ad hoc* arrangement.[385] Additionally, this type of defence must meet all other conditions, namely "imminence, immediacy, proportionality and necessity". [386]

It can be observed from the previous discussion that the right to self-defence can be applied in the event of a cyber-attack, but it must follow the legal requirements. Anticipatory self-defence is in high demand in the cyber space, because of the nature of the anticipatory self-defence, which can prevent any cyber-attack harm before the aggressor had the chance to hurt a state's cyber infrastructure or network. However, while this section demonstrated that international law recognises this type of self-defence in the same limited circumstances it does regarding kinetic warfare, many controversies remain. This might change in the future, given that there is already some state practice indicating the need and acceptance for a broader understanding of this type of self-defence. Naturally, state practice is an important part in creating international customary law. Therefore, if states continue to invoke anticipatory self-defence, especially against the cyber operations in broader ways, it will not only be evidence of state practice, but also constitute opinio juris and consequently will form a new or modified part of customary international law. This would result in the creation of clear regulations on this type of self-defence in cyber international law. The author holds that irrespective of the type of self-defence available, cyber operations should be considered not only as amounting to the use of force but indeed as an armed attack – if they meet the threshold as discussed earlier. Having said this, there are some cyber operations which do not rise to the level of use of force or armed attack, but are still unlawful. In these cases, they violate other international rules such as the non-intervention principle and the principle of state sovereignty, which will be studied in Chapter 3.

[384] Nicaragua case, para. 199.

[385] C Gray, International Law and the Use of Force, Ibid, 167-178.

[386] Ibid.

2.7 Conclusion

There are many international rules which regulate the use of force. The related principles to this thesis's aims and objectives have been discussed in detail in this chapter. The core of the prohibition of the use of force is Article 2(4) of the United Nations charter, which forbids any act against the territorial integrity and political independence. Moreover, this prohibition has influenced many principles such as the right of self-defence, which is an exemption of the prohibition of the use of force. Even though the right of self-defence is a natural right, there are some conditions that need to be met, which have been discussed in this chapter. Furthermore, it has been observed that even an authorised use of force is not permitted without some restrictions which prove how international law tries to limit the use of force as far as possible, even in a lawful way. In addition, the definition of 'use of force' within Art 2(4) UN Charter is *much* broader than 'armed attack' in Art 51 UN Charter. The Nicaragua case confirms that the right of self-defence in Art 51 is triggered *only* in response to the gravest uses of force, which by reason of their scale and effects constitute an armed attack.

In the context of self-defence, anticipatory self-defence has been discussed. The discussion shows that international law does not give legal characteristics to this type of self-defence. On the contrary, state practice has used anticipatory self-defence as a legal basis for the fight against terrorists. In this regard, the ability to apply these principles and rules to cyber operations come into question. If there is a cyber threat from any state to another, how could the latter use pre-emptive self-defence to protect its data and infrastructure? This will be studied in detail in the upcoming chapters. Moreover, the non-intervention principle is very related to the use of force. Even though any violation of the use of force it will include a non-intervention violation, but not every contravention of the non-intervention principle will be an armed attack or even a use of force. As a result, it is not necessary to characterise cyber operations as a use of force or an armed attack that violates the non-intervention principle.

This chapter discussed the main aims and objectives of this thesis, which is applying the use of force rules (jus ad bellum) to cyber operations. It has concluded that cyber

operations that cause injury or death to humans or physical damage to property will violate the prohibition of the use of force. However, any cyber operation should be assessed separately based on the criteria that have been explained in this chapter, such as the consequences-based approach, the instrument-based assessment and Schmitt's eight elements for assessing cyber operations. Moreover, it has been shown here that any cyber operation that amounts to an armed attack will by default be considered a use of force. Yet, any act or use of force that does not rise to the level of an armed attack cannot give the victim state the right to use self-defence.

This chapter has demonstrated the requirements to use the right of self-defence against a cyber operation. The criteria to determine that the act is equivalent to an armed attack is that of the scope and effect, which indicates that any use of force that injures or kills persons or damages or destroys property is an armed attack. Otherwise, non-destructive cyber operations, such as cyber theft or intelligence gathering, do not rise to the level of armed attack.

CHAPTER 3: STATE RESPONSIBILITY

3.1 Introduction

This chapter will outline the rules of state responsibility regarding international wrongful acts. Moreover, it will study the possibility of using countermeasures and

the plea of necessity in the case of cyber-attacks. Furthermore, it will clarify the state's role in exercising due diligence obligation against any cyber threats. It directly relates and builds upon the previous chapter, which applied the rules regarding the use of force and self-defence to cyber operations.

State responsibility is defined as "a set of international rules governing states' international obligations and their relations with other states."[387] State responsibility is a consequence of a wrongful act by the state which is prohibited by international law. This part plays a big role in the case of offensive cyber operations which may give rise to state responsibility if they are unlawful, even if they do not rise to the level of a use of force or an armed attack. There is a customary international rule that helps to constitute state responsibility in traditional international law. According to this rule, the injured state could demand a compensation or reparation for any damage or injuries accrued to its nationals or its property from another state who allowed these damages to happen.[388] Although this principle uses the term "diplomatic", it is not related to the regular meaning of diplomacy. It refers to "governmental" protection. The starting point of regulating state responsibility was in 1929. When a Draft Convention on Responsibility Of States for Damage done in their Territory to the Person or property of Foreigners has been prepared by Harvard Researchers in International Law.[389] The draft was revised in 1961 as the draft convention on the international responsibility of states for injuries to aliens.[390] It stated that any "State is internationally responsible for an act or omission which, under international law, is wrongful, is attributable to that State, and causes an injury to an alien".[391] The General Assembly of the United Nations has noted in 1953 that

[387] S Sucharitkul, State Responsibility and International Liability under International Law, (1996), 18 Loy. L.A. Int'l & Comp. L. Rev. 823.

[388] Ibid.

[389] Research in International Law, Harvard Law School, Responsibility Of states for damage done in their territory to the person or property of foreigners, printed in 23AM.J.INT'L L. 133.

[390] Draft Convention on the international responsibility of states for injuries to aliens, Reprinted in Louis B. Sohn & RR Baxter, Responsibility of states for injuries to the economic interests of aliens (1961), 55 AM. .J.INT'L L. 548.

[391],Ibid, art. 1, para. 1.

“it is desirable for the ·maintenance and development of peaceful relations between States that the principles of international· law governing State responsibility be codified”.[392]

After 50 years working on a draft convention on State Responsibility rules, finally, the ILC Commission at its fifty-third session in 2001, submitted it to the General Assembly as part of the Commission’s report covering the work of that session, the Responsibility of States for Internationally Wrongful Acts.[393] The first chapter is explaining the meaning of “wrongful acts” by referring to the international law characterization.[394] A wrongful act is considered an act of a state if it is conducted by state organs, persons or groups empowered by the government even when they exceed their official authority, any conduct directed by the government or acknowledged or adopted by the state or any act of insurrectional movement.[395] The Act also states that any state that assists, directs or coerces in the wrongful act with its full acknowledge of the circumstances.[396] For example, in the case of the American diplomats' hostage crisis in the US embassy in Iran, the Iranian government supported this seizure.[397] In this case, the Iranian government was responsible for the wrongful act. On the other hand, there are some circumstances where the wrongful act does not cause state responsibility. Consent is the most obvious reason for precluding wrongfulness. Additionally, self-defence, or any countermeasure which has been taken in response to an internationally wrongful act, or cases of force majeure, distress or necessity and any act that complies with

[392] G.A. Res. 799, U.N. GAOR 6th Comm., 8th Sess., Supp. No. 17, at 52, U.N. Doc. AJ2630 (1953).

[393] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1, available at: https://www.refworld.org/docid/3ddb8f804.html [accessed 14 November 2019]

[394] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid, part one, Chapter 1.

[395] Ibid, Articles 4-9.

[396] Ibid, Articles 16-18.

[397] United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), (1980), ICJ, available at: https://www.icj-cij.org/en/case/64 [accesses 29 January 2023].

peremptory norms preclude wrongfulness.[398] The legal consequences of state responsibility is either a continued duty of performance, which means performing the state obligation, or stopping the wrongful act and not repeating it again in the future.[399] The injured state could demand from the other state to make a full reparation, which could be a restitution if is it possible or compensation or satisfaction by formal apology or acknowledgment of the breach.[400]

If the injured state wants to induce the other state to do its obligation, it can take some countermeasures, but only as far as required to resume the performance.[401] Countermeasure are not available against alleged breaches of the law of armed conflict during a conflict. They are only available in peacetime. Moreover, countermeasures are about precluding the unlawfulness of a response to an unlawful act that did *not* rise to the level of an armed attack. It has been considered initially by the ICJ in the Nicaragua case. The court commented that "On the legal level, the Court cannot regard the response to an intervention by Nicaragua as such a justification. While an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot, as the Court has already observed, produce any entitlement to take collective countermeasures involving the use of force."[402] According to the court statement, any victim state of non-forcible intervention could respond with non-forcible measures in response to the countermeasures. The injured state should consider any international obligations such as the prohibition of the use of force, respect of human rights agreements and peremptory norms. Moreover, the countermeasures should be proportionate to the level of the injury.[403] Furthermore, an injured state should notify the other state of any countermeasures taken and should demand

[398] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid, Article 20-27.

[399] Ibid, Articles 28-30.

[400] Ibid, Articles 30-37.

[401] Ibid, Articles 49.

[402] Nicaragua Case, at para. 248, 249.

[403] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid, Articles 49-51.

performance from the state in question before taking any measures.[404] Once the state complies with its obligation, the countermeasures must be terminated immediately.[405] This illustrates the difference between countermeasures which aim to get the other state to comply with its obligation from the plea of necessity which is aimed at protecting the state's essential interests.

The plea of necessity is another method of response against a wrongful act which does not rise to the level of an armed attack. Moreover, the state should have no other alternative means to avoid this threat. This has been affirmed in the ILC Commentary "the peril must not have been escapable by any other means, even a more costly one, that could be adopted in compliance with international obligations."[406] Interestingly, the commentators mentioned the "cost" of the alternative means as a non-evaluation criterion to determine the possibility of using another means to protect the state's interests. To support that, the ICJ has noted in the Gabikovo-Nagymaros Case that "Hungary had means available to it, other than the suspension and abandonment of the works, of responding to that situation…. the purification of the river water, like the other measures envisaged, clearly would have been a more costly technique."[407] The court was clear about using other means even if it is more costly to protect the state's interest - it is an open option for the state to not invoke necessity.

Additionally, there are more conditions to be met before using the plea of necessity, which have been clarified in the Articles on State Responsibility. They state that the state cannot invoke the plea of necessity "unless the act: (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."[408] The first requirement to apply this method is that the "essential interest" of the state is threatened. This is known as "self-preservation", where the state can use

[404] Ibid, Articles 52.

[405] Ibid, Article 53.

[406] ILC Commentary, Ibid,note 6 , 49.

[407] Gabčikovo-Nagymaros Project, Hungary v Slovakia, Judgement, Merits, ICJ GL No 92, (1997), , para.55, 40.

[408] Art.25, Articles on the State Responsibility. Ibid.

measures to protect its essential interest regardless of its international obligations. There is no consensus definition of the “essential interests”. The ILC concluded that the scope of state essential interests is decided on a “case by case” basis.[409] The ICJ pointed out that “'The Court has no difficulty in acknowledging that the concerns expressed by Hungary for its natural environment in the region affected by the Gabdikovo-Nagymaros Project related to an 'essential interest' of that State”.[410] This indicates that the affected state’s interests could be on the part of state territory. The second condition is that the act needs to be grave, which does not constitute a mere risk and needs to be an “imminent peril”. The ILC commentators explained that it must be “a threat to the interest at the actual time.” [411] Therefore, the danger must exist at the time when using the plea of necessity, which means that the state’s interests have already become threatened. Lastly, the third condition is that there should be a balance between the state’s interest which needs to be protected and the other state's essential interests. It is worth noting that the plea of necessity does not make the wrongful act lawful, but it precludes the international responsibility of the state. This is contrary to the legal consequence of self-defence, as discussed in the previous chapter, which gives the act a lawful characterisation.

State responsibility defines the source of the wrongful act and helps with preventing the states from going into a conflict. The countermeasures and plea of necessity are helping to protect the targeted state without triggering any international responsibility. Countermeasures play a big role in the event of cyber operations which are below the level of use of force. There are many cyber activities which do not amount to a use of force or armed attack but violate other international principles such as the sovereignty and non-intervention principles. The countermeasures and plea of necessity will offer a method to respond and protect the state.

[409] ILC Commentary, Ibid,note2 , 202

[410] Gabčikovo-Nagymaros Project, (Hungary v Slovakia), [1997], ICJ Reports, GL No 92, para.53

[411] Crawford J.R., The International Law Commission’s Articles on State Responsibility: Introduction, Text and Commentaries, Cambridge University Press, (2002)

3.2 The principle of non-intervention and state responsibility

A violation of the non-intervention principle falls within actions below the threshold of the prohibition of the use of force or threat thereof. Nevertheless, any act not considered a use of force or armed attack, especially in the case of cyber operations, will still have legal implications if it violates the non-intervention principle. The non-intervention principle originated at the Peace of Westphalia, but it was not reflected in the state practice at that time.[412] Then in 1823, the Monroe Doctrine stated that “any interposition for the purpose of oppressing them [the newly formed states of the Americas] or controlling in any other manner their destiny' would be seen as a threat to the United States”.[413] Although this doctrine has been practised by America, it never bound other states in the world.[414] In 1933, the Montevideo Convention on Rights and Duties of States, states in Article 8 that “No State has the right to intervene in the internal or external affairs of another”.[415] Since 1957, there have been more than thirty-five resolutions who deal with non-intervention adopted by the General Assembly. Such as the 1965 Declaration on the Inadmissibility of Intervention, the 1970 Friendly Relations Declaration, and the 1981 Declaration on the Inadmissibility of Intervention and Interference.[416] The non-intervention principle is listed in the “Principles of International Law embodied in the Charter” in the preambles to the Vienna Convention on The Law of Treaties between 1969 and 1986.[417] Moreover, the non-intervention principle is the foundation of state sovereignty, which is codified in Article 2 (1) of the United Nation Charter.[418] State sovereignty will be examined in the next part.

---

[412] Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention' (2009) 22 LJIL 345, 349

[413] Ibid.

[414] Ibid, 350.

[415] The Montevideo Convention on Rights and Duties of States, (Signed on December 26, 1933, entered into force on December 26, 1934)159 LNTS i99.

[416] Jamnejad and Wood, 'The Principle of Non-intervention', Ibid, 350.

[417] Ibid, 347.

[418] Charter of the United Nations, Ibid, Article 2: “…1. The Organization is based on the principle of the sovereign equality of all its Members.”.

State actions which could amount to an unlawful intervention must be an intervention in another state's affairs.[419] Furthermore, it must bear on "matters in which each state is permitted, by the principle, both state sovereignty to decide freely".[420] Oppenheim describes what constitutes an unlawful intervention by saying that "The interference must be forcible or dictatorial, or otherwise coercive (…). Interference pure and simple is not intervention".[421] Therefore, the core of the intervention is coercion. This has been the case since the 1970 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States. It states that "No State may use or encourage the use of economic, political or any other type of measure to coerce another State to obtain from it the subordination of the exercise of its sovereign rights and to secure from its advantages of any kind".[422] That means the intervention needs to include coercion or any other forcible means. Moreover, the coercion element has been affirmed by the ICJ in the Nicaragua case. It stated that: "Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State"[423]. Therefore, only acts that are "coercive" will contravene the non-intervention principle. The coercive act could be in circumstances when there is a pressure on the government or forcing the state to act in a specific way. In regard to the coercion requirement, the Declaration on Principles of International Law concerning Friendly Relations and cooperation among states according to the United Nation Charter, has mentioned that prohibited coercion could be "economic, political or any type."[424]

The principle of non-intervention was developed in customary international law as a part of *opinio juris.* It can be seen in debates and resolutions of the General

[419] Jamnejad and Wood, 'The Principle of Non-intervention' Ibid. 350.

[420] Nicaragua Case, para. 205.

[421] Jennings, R., & Watts, A. Oppenheim's International Law, (1992).1 OUP, ed.9th 150.

[422] UN Doc. A/Res/2625 (XXV).

[423] Nicaragua Case, para. 205.

[424] UN Doc.A/Res/2625 (XXV).

Assembly and other bodies, in particular the Friendly Relations Declaration of 1970 and the Helsinki Final Act of 1975.[425] The Declaration on Non-intervention in 1976, provided in paragraph 2 that non-intervention "Denounces any form of interference overt or covert, direct or indirect, including recruiting and sending mercenaries by one state or group of states and any act of military, political, economic, or other form of intervention in the internal or external affairs of other states regardless of their character of their mutual relations or their social and economic systems." This statement gives the prohibition of intervention a wide scope. It will include direct or indirect state participation in any form of intervention, not just the military one, but also political and economic coercion. Therefore, it includes cyber operations as an intervention in a state's affair – as long as there is a coercive element.

It is worth mentioning that the non-intervention principle has been reaffirmed in many organisations' treaties. For example, the Treaty on European Union in Article 1a.[426] It is also mentioned in the Constitutive Act of the African Union, in Article 4(g), which includes the fundamental principles of the Union.[427] The pact of the League of Arab States in Article 8 has prohibited intervention in another state's matters.[428] Furthermore, the Charter of the Organization of the Islamic Conference 2008 also recognised the non-intervention principle. Not just these organisations have recognised this principle but also the ICJ in its judgements. Indeed, the non-intervention principle has been considered in numerous cases. The Corfu Channel case was the first case in which the ICJ discussed this principle.[429] It stated that "[t]he Court can only regard the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to the most serious abuses and as such cannot, whatever be the present defects in international organisation, find a

[425] Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention', Ibid, 352.

[426] The Treaty on European Union,35 O.J.C 191, (Signed on on 7 February 1992 and entered into force on 29 July 1992).

[427] Article 4(g) stated that:"non-interference by any Member State in the internal affairs of another;"The Constitutive Act of the African Union, (Signed on 11 July 2000 and enter into force on 26 May 2001),7

[428] Pact of the League of Arab States, (1945)70 UNTS 237, Art. 8.

[429] Jamnejad and Wood, 'The Principle of Non-intervention', Ibid, 356.

place in international law".[430] Then, the court adopted this principle in the Nicaragua case by prohibiting the intervention in another state's affairs directly or indirectly. The court underlines the sovereignty right of the state to make its own choices in its political, economic, cultural, and foreign affairs. Also, any intervention by coercion in these matters is an illegal act and violates the non-intervention principle.[431] A similar position has been taken by the court in DRC V. Uganda.[432] The court noted that: "Uganda had violated the sovereignty and also the territorial integrity of the DRC. Uganda's actions equally constituted an interference in the internal affairs of the DRC and in the civil war raging there."[433]

The prohibition of the use of force, as stated in Article 2(4) of the United Nation Charter, has a strong relation with the non-intervention principle. Any use of force will also result in a violation of the non-intervention principle.[434] However, it does not work the opposite way: not every violation of the non-intervention principle will be an armed attack or even a use of force. Exceptions to these rules, are, as previously discussed, interventions authorised by the UN Security Council and the use of force in the context of self-defence. The non-intervention principle is an important legal rule giving rise to state responsibility in the case of the use of force. It is related to the state's independence and its authority to exercise its power without any intervention. However, coercion is at the core of the intervention. Whenever it is present in any action, it will be considered as an intervention in state affairs.

3.2.1 Lawful intervention

As mentioned above, intervention can be legal for three reasons. First, by Security Council authorisation. Second, by using countermeasures, and third, if the

[430] Corfu Channel (United Kingdom v. Albania), Merits, Judgement of 9 April 1949, ['949] ICJ Rep. 9, at 35.

[431] Nicaragua, paras. 202, 205, 206, 208, 209.

[432] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits, Judgement of 19 December 2005, [2005] ICJ Rep., paras.64 and65.

[433] Ibid.

[434] Nikolas Stflrchler, The Threat of Force in International Law (2007).CUP, 60

state consents. The authorising intervention by the Security Council is regulated in Chapter VII of the United Nation Charter. In the event of a threat or breach of international peace or security or an act of aggression, the Security Council may use both force and non-forcible measures to restore the peace.[435] To illustrate that, take the example of the military junta in Sierra Leon in 1997.[436] The Security Council imposed sanctions against members of the military junta because of the new election of the government. The situation was a threat to peace and security. Therefore, any intervention from any state following the UNSC's resolution will not be unlawful.[437] The Second lawful way of intervening in another state's affairs is by using countermeasures. This method has been used initially by the ICJ in the Nicaragua case. The court concluded that "On the legal level, the Court cannot regard the response to an intervention by Nicaragua as such a justification. While an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot, as the Court has already observed..., produce any entitlement to take collective countermeasures involving the use of force."[438] According to the court's statement, any victim state of non-forcible intervention could only respond with non-forcible measures. The last possibility for a lawful intervention is consenting. This type of intervention is known as "Intervention by Invitation" which will be discussed in detail in the following part.

3.2.2 Intervention by invitation

[435] Furthermore, should a cyber operation fall short of being a use of force, the UNSC could authorise measures under Article 41 rather than 42. This will be discussed in more detail in the last chapter of this thesis.

[436] United States Bureau of Citizenship and Immigration Services, Sierra Leone: Information on the 1997 coup d'etat, ECOMOG harassment of civilians, and the current situation in Sierra Leone, 5 January 2000, SLE01001.SND , available at: https://www.refworld.org/docid/3df0dba62.html [accessed 23 August 2021].

[437] UN Doc. S/RES/r132.

[438] Nicaragua Case, para,248, 249.

The Charter of the United Nation does not have any provision indicating the legality of intervention or mentions an exception to Article 2(4).[439] Nevertheless, state practice accepted this type of intervention to put an end to internal conflicts and war.[440] The intervention by invitation needs a request from the competent state, which must be obtained without any coercion. Moreover, one must consider if there is any internal conflict or civil war. Additionally, the request needs to come from a legitimate government. Alternatively, it could be legitimate to engage in an intervention to help the rightful government be reinstated. For instance, in 1964, France intervened in Gabon by the request of its government to help them against an army mutiny to prevent disorder during the governmental elections.[441] Furthermore, the Hungarian prime minister requested the USSR to intervene in Hungary in 1956 to repress the move away from one-party rule.[442] In 1991, Iraq claimed that the Free Provisional Government in Kuwait requested its intervention to "establish security and order so that Kuwaitis would not have to suffer".[443] In the French case, the Security Council kept silent, contrary to the case of Kuwait, where the Security Council rejected Iraq's claims and condemned Iraq's invasion into Kuwait's territory with Resolution 660,1990.[444] In the case of Hungary, the General Assembly condemned the USSR intervention by 50-8-15.[445]

An intervention in response to a prior foreign intervention is known as a "Counter-intervention". This intervention is the most abusive one among all other methods of intervention. It has been invoked by the USSR in its military intervention in Czechoslovakia in1986 and in Afghanistan in 1979.[446] In the case of Czechoslovakia, its government denied any request from the USSR to intervene in the Security Council meetings.[447] In the other case, the General Assembly

[439] M Almousa, Using Force in contemporary international law, Ibid, 154.

[440] Ibid, 155.

[441] KEESING'S Contemporary archives, 14 Keesing's, (1963-1964), 20024.

[442] C Gray, International law and the use of force , Ibid, 87.

[443]United Nation Security Council Res.2932, 2nd meeting, (1990).

[444] Ibid.

[445] C Gray, International law and the use of force, Ibid, 87.

[446] Ibid.

[447] Ibid.

condemned the USSR's intervention in Afghanistan.[448] In the same context of abusing consent by the state, the ICJ noted in DRC v Uganda that "the parameters of that consent, in terms of geographic location and objectives, would have remained thus restricted."[449] Even though the court affirmed the existence of the consent, but the scope of it has not been respected.

To conclude, the non-intervention principle plays a big role in the case of political or economic coercion or any other type of coercion which does not rise to the level of use of force, like e.g., a cyber operation. It gives the target state the right to raise a state responsibility claim against the violating state. However, not all interventions are prohibited. The intervention by invitation in the case of requesting assistance in internal conflict is one example. This type of intervention requires the state's consent to that intervention, and the intervening state should respect the limits of that consent. The non-intervention principle is protecting the state's sovereignty and gives the state a chance to protect its territory in the case of a non-use of force act. The sovereignty principle is connected to the non-intervention principle because when a state violates the non-intervention principle, it violates its sovereignty. Consequently, the next part will investigate state sovereignty in the conventional way, as well as in cyber space.

3.3 State sovereignty and sovereignty over cyber space

3.3.1 State sovereignty

For the aim of this thesis, there is a need to analyse the position of sovereignty in international law, as sovereignty is a significant element in determining other principles such as non-intervention and due diligence. To analyse

[448] UN. General Assembly (6th emergency special session , Resolution A/ES-6/7, (1980).

[449] Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)), [2005], ICJ, ICJ, 196.

how sovereignty operates within the international system, it will also help to examine the existence of cyber sovereignty and how states exercise their authority over it. The concept of state sovereignty represents the basic constitutional doctrine of the law of nations, which governs the community of states that, in principle, have a uniform legal personality.[450] If international law exists, the dynamics of state sovereignty can be addressed in terms of law, but if they are only conceived of as sovereign, this means that they are equal and such equality is recognised in law.[451] This principle means that the state has sovereignty over its own territory and the population that lives there, and that other states and international organisations must respect this.[452] It is also important to note that whilst territory is included in a legal definition of state sovereignty, there are certain areas where, due to custom and constitutional agreement, no state can assert sovereignty. For example, the seabed or the moon are treated as 'common heritage of mankind', which means that they belong to all states and must be utilised to benefit all states (and not only one). As opposed to this, there is also the concept of 'res communis' which means anyone (any state) can use it, but no one can own it.[453]

Two different theories have been applied to explain the presence of sovereignty in the international system: the historical definition and the concept of sovereignty as an organising principle. Another interesting perspective to be considered here is that of theorist Hans Kelsen. In consideration of a historical definition of sovereignty, it has been observed that since the state is regarded as historically and ontologically prior to the system of states in the discourse on

[450] James Crawford, Brownlie's Principles of Public International Law,(2019) 9th Ed., (Oxford University Press),431.

[451] Ibid.

[452] Ibid.

[453] Eric Talbot Jensen, 'Cyber Sovereignty: The Way Ahead,' Texas International Law Journal, (2014) 50 (2), (2014), 283–284; "res communis." Encyclopaedic Dictionary of International Law. Eds. Grant, John P., and J. Craig Barker. : Oxford University Press, 2009. Oxford Reference. <https://www.oxfordreference.com/view/10.1093/acref/9780195389777.001.0001/acref-9780195389777-e-1964>.

international politics, the essence of statehood appears to be the necessary condition also of the larger whole, the international system.[454] In more traditional interpretations of international political theory, this foundational character of sovereignty is considered a historical precedent resulting from the decline of large areas of political unity, such as the Roman Empire and later the Holy Roman Empire.[455] Notably, Martin Wight asserts that "International politics . . . came into existence when medieval Christendom dissolved and the modern sovereign state was born."[456] Similarly, Hans Morgenthau states that "Supreme power over a certain territory" is the main source of political decentralisation, so without the sovereign state, a "state system based on it could not exist."[457] Therefore, it can be suggested that sovereignty is the basis of order both within and outside the state system. From a historical perspective, then, sovereignty is the way through which states are governed and has then dictated the character of the international system.

On the other hand, other political theorists, such as Kenneth Waltz, see sovereignty not as a historical principle, but as an organisational one.[458] Instead of linking the emergence of sovereignty as the outcome of political fragmentation to the alienation within Christianity, those who promote sovereignty as an organisational principle assert that it explains "the striking sameness in the quality of international life through the millennia."[459] Thus, for Waltz, sovereignty served to explain the current position and character of the international system and its tendency toward conflict and anarchy.[460]A further perspective on sovereignty is offered by Hans Kelsen. He felt that most definitions of sovereignty emphasised the primacy of national law over international law.[461] However, Kelsen rejected this notion of

[454] Jens Bartelson, A Genealogy of Sovereignty, (Cambridge University Press, 1995), 23.

[455] Ibid.

[456] Martin Wight, Power Politics, (Leicester University Press, 1978), 25.

[457] Hans Morgenthau, Politics among Nations, (Knopf, 1985), 328–329.

[458] Jens Bartelson, A Genealogy of Sovereignty, (1995) ,Cambridge University Press, 23.

[459] Kenneth N. Waltz, 'Reductionist and Systematic Theories,' in Robert Keohane,\ ed., Neorealism and its Critics, (1986), Columbia University Press, 53.

[460] Jens Bartelson, A Genealogy of Sovereignty, Ibid23–24.

[461] Hans Kelsen, 'Sovereignty and International Law,' GLJ, 48 (4), (1960), 627; 634.

sovereignty as it led to the false conclusion that states are not bound to any majority decision made by a tribunal or collegiate organ.[462] As such, Kelsen's perspective demonstrates how notions of sovereignty lead states to ignore international law.

In the context of international law, sovereignty means that the government of a nation state has full control within the area it governs.[463] Disputes can arise when it is uncertain which state possesses sovereignty over a particular geographical area. States can express reluctance to accept responsibility for incidents that are not clearly their responsibility, such as those that occur over the internet, as cyberspace allows for anonymity.[464] There is also an expectation that both *de jure* (the legal right to do so) and *de facto* (the factual ability to do so) sovereignty exist at the same time and place in relation to the territory under dispute. An example of such a disputed territory is Taiwan. When the People's Republic of China (PRC) came under Communist rule in the 1940s, the United Nations declared that Taiwan (then the Republic of China) was the legitimate government of China.[465] But in 1971, this ruling was overturned by the UN, and it was decided that the PRC represented China and, by extension, Taiwan.[466] As such, Taiwan has the *de facto* right to rule its territory, but not the *de jure* right to do so.

State practice on international sovereignty emphasises that when states exercise their sovereignty and sovereign rights, they must consider the sovereignty and sovereign rights of other states. This means that a state's sovereignty and sovereign rights are not absolute and that in exercising these rights, states are not to

[462] Ibid, 637.

[463] Thomas Gangale, How High the Sky? The Definition and Delimitation of Outer Space and Territorial Airspace in International Law, (Brill, 2018), 32.

[464] Eric Talbot Jensen, 'Cyber Sovereignty: The Way Ahead,' 50 (2)TILJ, (2014), 279.

[465] Jonathan Manthorpe, Forbidden Nation: A History of Taiwan, (St Martin's Press, 2008), 94.

[466] Lu Hsiu-lien et al., 'Case Studies of Contemporary Neutrality Advocacy,' in H.R. Reginbogin & P. Lottaz, eds., Permanent Neutrality: A Model for Peace, Security, and Justice, (Lexington Books, 2020), 211.

infringe unduly upon the rights of other states.[467] The general obligation resulting upon a state regarding the rights of other states within its own territory was referred to in the case of the *Island of Palmas Arbitration* (1928). When summing up, Judge Max Heber stated:

"Territorial sovereignty . . . has a corollary a duty: the obligation to protect within it other states, in particular the right to integrity and inviolability in peace and war, together with the rights which each state may claim for its nationals in foreign territory."[468]

This example shows that even within its own territory, a state's sovereignty is restricted by the rights other states may have therein. This means that even within its own territory, a state may not exercise its sovereignty in an absolute manner. On the other hand, it is notable that sovereignty may be recognised in instances where the sovereign body possesses no actual territory, or its territory is under total or partial occupation by another power. The case of the PRC and Taiwan is a recent example of this.[469] Another example is the position of the Holy See between the annexation of the Papal States by Italy in 1970 and the signing of the Lateran Treaties in 1929. Despite this, the Holy See continued to be recognised as a sovereign entity by many and by international law, although it had no territory during the interim period.[470] These examples suggest that sovereignty can be possible in instances where the state possesses no territory or cannot exert rule and possession over another territory.

---

[467] Ellen Hey, The Regime for the Exploitation of the Transboundary Marine Fisheries Resources: The United Nations Law of the Sea Convention Cooperation between States (Martinus Nijhoff Publishers, 1989), 25.

[468] Ibid, 26.

[469] Lu Hsiu-lien et al., 'Case Studies of Contemporary Neutrality Advocacy,' in H.R. Reginbogin & P. Lottaz, eds., Permanent Neutrality: A Model for Peace, Security, and Justice,(2020), (Lexington Books), 211.

[470] Alina Kaczorowska-Ireland, Public International Law, (2015), 5th edn., Routledge, 184.

In instances where states share geographical territory, case law suggests that no state is entitled to exercise its right in an absolute manner to the detriment of other states involved. For example, in the *Case of Relating to the Territorial Jurisdiction of the International Commission of the River Oder* (1929), the Permanent Court of International Justice found that:

"The community of interest in a navigable river becomes the basis of a common legal right, the essential features of which are the perfect equality of all riparian states in the user of the whole course of the river and the exclusion of any preferential privilege of any one state riparian in relation to the others."[471]

In this case, the court emphasised that a balance between the rights of all states concerned is necessary to guarantee the sovereign rights of all parties in such instances. This seminal case may be applied to China's attempts to establish a nine-dash maritime boundary line in the South China Seas, which represents its claims over the entire seas and ignores the competing claims of Vietnam, the Philippines, Indonesia, and Taiwan.[472] China's claims were rejected by an international arbitral tribunal in 2016.[473]

3.3.2 Sovereignty over cyber space

As discussed in the last section, sovereignty is a significant principle in international law. This section seeks to explore if and how this principle can be applied to cyber space. In 1928, in the Island of Palmas Arbitral Award, the judges declared: "states being independent of one another in the sense that within a

[471] Ellen Hey, The Regime for the Exploitation of the Transboundary Marine Fisheries Resources: The United Nations Law of the Sea Convention Cooperation between States,(1989), Martinus Nijhoff Publishers, 26.

[472] C. Gray, International Law and the Use of Force, Ibid, 36–37.

[473] Philippines v China, PCA case no 2013-19, (12 July 2016); C. Gray, International Law and the of Force, Ibid, 36.

state's sovereign territory the state has the right to exercise, among other things, the functions of a state"[474]. With regard to cyber space, there has been a huge debate about the nature of sovereignty over the cyber space - the most pressing question is: does sovereignty exists within it or not?

Ella Shoshan considers servers that are located in a state's territory and the cyber infrastructure of that state as part of the state's territory, which the state has the total sovereignty and authority over.[475] Moreover, J P. Barlow, a political activist and cyberlibertarian, has noted that "cyberspace is a space subject to internal governance".[476] Another author who supports these views is J P. Trachtman, he stated that so long as the servers and the actors are located on the state's territory, they will be subject to the state jurisdiction and its sovereignty.[477] These views make it clear that the cyber space is included in state sovereignty and subject to the territorial state jurisdiction. Moreover, it is noteworthy that these authors made their assessment by looking at the physical elements related to the cyber operations and the location of the cyber infrastructure.

On the other hand, there are also scholars who argue that the cyber space is an independent domain and that no state has authority over it, just like the high seas and outer space, e.g., like D. Hunter.[478] Also, some consider it as a Common Heritage of Mankind.[479] J. Frake noted that there are five consequences of considering the cyber space as a CMH. First, even though the public or private sector owns the network and the internet access, they do not own the data packets

[474] Islands of Palmas (Netherlands v US) (1928) 2 RIAA 829, 838.

[475] Ella Shoshan, Applicability of International law on Cyber Espionage Intrusions, Stockholm University, (2015), 34.

[476] 4 J P. Barlow, 'A Declaration of the Independence of Cyberspace' (1998) <https://projects.eff.org/~barlow/Declaration-Final.html> .

[477] J P. Trachtman, 'Global Cyberterrorism, Jurisdiction, and International Organization' The Law and Economics of Cybersecurity, (2005), 1st edn CUP, 268.

[478] Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons." California Law Review 91, no. 2 (2003): 439-519.

[479] Hereinafter CHM.

and the internet itself, which means there is no one who owns the cyber space.[480] As a second point, Frake argues that there will be cooperation between all states around the world to manage this CHM because it belongs to all of them. Furthermore, there is a need for an agency or an authority which administers sources of the cyber space, such as the organisations which sell domain names and track data (e.g., ICCAN).[481] The third result of characterising cyberspace as a CHM is the benefits of the resources should be shared actively among nations.[482] Fourth, there should be no weapons or military installations in cyberspace.[483] Finally, the last result is that all the recourses of the cyberspace need to be preserved for the benefit of the future generations.[484]

The Group of Experts commented on this view, saying "although no state may claim sovereignty over cyberspace per se, states may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[485] Moreover, the Group of Expert emphasised that "although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States."[486] Indeed, the Tallinn Manual, in the author's view, is logical because if we assume that cyberspace is a CHM, how could cyber-attacks against infrastructure placed in the territorial area of a specific state be explained? Furthermore, state practice in this regard proves the existence of cyber sovereignty. For instance, India has announced that "states have responsibility to ensure that their ICT is not

[480] Jennifer Frakes,The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?, (2003), 21 (2) Wisconsin International Law Journal, 409-434.

[481] Internet Corporation for Assigned Names and Numbers (ICANN), Homepage, http://www.icann.org/tr/english.html.

[482] Jennifer Frakes, The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?, Ibid, 412

[483] Ibid.

[484] Ibid.

[485] Tallinn Manual, (2013), R1 comment 1.

[486] Tallinn Manual, (2017), 12

abused, either covertly or overtly, by others to target or attack their ICT infrastructure of another nation state."[487] Similarly, China stated that "sovereign states have the responsibilities and rights to take necessary management measures to keep their domestic Cyberspace and related infrastructure free from threats, disturbance m attack and sabotage".[488] Furthermore, Russia stated that all states should be responsible for any action carried out within their jurisdiction.[489] Likewise, the US has stated in its International Strategy for Cyberspace that they

"recognize the international implications of their technical decisions and act with respect for one another's networks and the broader Internet."[490]

Schmitt has noted that France acknowledged its cyber sovereignty and considered any interference with governmental election as a violation of France's sovereignty. He also mentioned more states which agree with this definition of cyber sovereignty such as Finland, Iran, Germany, and Switzerland, and some NATO states.[491] There is thus clearly some evidence of state practice in favour of recognising cyberspace sovereignty. Schmitt has also made this point, arguing that there is growing agreement on sovereignty applying to the cyber space. He lists Finland, France, Germany, the Netherlands, Iran, the Czech Republic, Austria and Switzerland.[492] However, the UK took an opposing position in this regard. The Attorney General Jeremy Wright announced: "I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention".[493] He argued that affirming cyber sovereignty, will result in some violations of privacy and

---

[487] Eric Talbot Jensen, Cyber Sovereignty: The Way Ahead, (2015), 50 TEX. INT'L L. J. 275, 297

[488] Ibid.

[489] Ibid.

[490] Office of The President, International Strategy for cyberspace, (2011), 10

[491] Schmitt M., Foreign Cyber Interference in Elections, (2021), 97 INT'L L. STUD. 739, 750-751.

[492] Ibid.

[493] Wright J. , Cyber and International Law in the 21st Century, Speech of the The Attorney General Jeremy Wright QC MP in Chatham House Conference,(May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-internationallaw-in-the-21st-century.

freedom to access the internet, besides other human rights issues. For the sake of having a balance between national security and privacy, the UK prefers not to have rules to regulate cyber sovereignty.[494]

Moreover, the Tallinn Manual noted in the previous official statement that there will be obligations corresponding to the right of sovereignty. These obligations include, e.g., the responsibility to protect and monitor the state territory against any unlawful cyber activities against another state.[495] In the context of a state knowing of a harmful attack on its territory, it has the responsibility to prevent and terminate it.[496] In circumstances different from these, when the state does not know about cyber activities on its territory, it is questionable if such a responsibility still exists or not.[497] Indeed, this was precisely the situation faced by the ICJ in the Corfu Channel case, when the ICJ stated that "Albania is liable for harm to England, even though there was no direct evidence that Albania knew of the harm."[498] Therefore, the ICJ makes it clear that a state's knowledge is not a condition for its responsibility for the harmful attack on its territory.

In this regard, Eric Jensen noted that there is a standard test, namely the "must have known" requirement. Heintschel von Heinegg stated that in a situation where a cyber operation was launched from within the governmental cyber infrastructure which should be under full state control, the state's knowledge will be assumed.[499] The state's responsibility regarding a variety of cyber-attacks will be discussed in detail in the next part.

Going back to the nature of cyberspace sovereignty, John Herz is in favour of the theory that there is sovereignty within cyberspace in regard to special types of

---

[494] Ibid.

[495] Tallinn Manual, (2017), 339-344.

[496] E Jensen, Cyber Sovereignty: The Way Ahead, Ibid, 298.

[497] Ibid.

[498] Corfu Channel Case, Para19-20.

[499] Heintschel von Heinegg, Wolff. "Territorial sovereignty and neutrality in cyberspace." (2013), 89.1Inte'LStud: 17.

sovereignty called “neoterritorality”.[500] This concept proposes that the mutual interests of sovereign states should be recognised and that there should be co-operation between states and that they should decide what set of rules could apply for the cyberspace.[501] Similarly, Michael Mann's view is “sovereignty is now universal, having migrated from Europe and become a mainstay of global politics and a central philosophy of the world's sole remaining superpower.”[502] Besides John Jackson, who termed “Sovereignty-modern”. It means that “nation-state sovereignty will fall to international institutions that embrace a series of legitimising good-governance characteristics.”[503] All these views are mere theories which are inconsistent with the state practice and the main elements of any state, which are population, territory, government and sovereignty. On the other hand, Janice Thomson distinguishes between state control and state authority. With regard to cyberspace, she stated that

“this authority should take the form of national and international efforts to regulate the largely privatized information commons”[504]

Therefore, this view is nearly similar to the adopted view of the Group of Experts in Tallinn Manual. The Group of Expert agreed that the principle of sovereignty in cyberspace consists of three layers (physical, logical and social).[505] The physical layer is any physical network component such as servers, cables and routers.[506] Whereas the logical layer is the connection between these components like the requesting by the state of electronic signature or encrypted protocol to

---

[500] Tuomas Forsberg, Beyond Sovereignty, Within Territoriality: Mapping the Space of Late-Modern (Geo)Politics, 31(4), Cooperation and Conflict, (1996), 355-386.

[501] Scott J., Shackelford, From Nuclear War to Net War: Analogizing Cyber-attacks in International Law, Berkley Journal of International Law (2009). 25(3)BJIL, , 215

[502] Hugh Willis, The Doctrine of Sovereignty Under the United States Constitution, (1929).15 No. 5 VA L. REV. 437

[503] John Jackson, Sovereignty-Modern: A New Approach to an Outdated Concept, (2003). 97 AM. J. INT'L L 782, 785

[504] Janice Thomson, State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research, (1995), 39 INT'L STUDIES Q. 213,225

[505] Tallinn Manual, (2017), 12.

[506] Ibid.

communicate.[507] The last layer, which is the social one, is regulated by the state and allows it to create rules for natural and legal persons. For example, the state can criminalise some web content like child pornography.[508] However, this state's authority it restricted by human rights law.[509] Furthermore, the Tallinn Manual stated in Rule 2 that "a State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[510] This rule explains the internal sovereignty of the state over the cyber layers, which have been mentioned above.

Furthermore, this internal sovereignty has two implications. The first is the state has the authority to apply its cyber regulation over cyber entities, activities or persons on its territory irrespective if they are public or private in character.[511] The second, is that the state is granted the right to take any measures to protect its cyber infrastructure or activities located on its territory.[512] Although, the state has the right to act in its internal affairs freely, international law sets some limitation on exercising that right. For instance, the state has no authority over diplomatic and consular personnel or buildings, or over aircraft or ships which are owned by another state due to the principle of immunity and inviolability.[513]

So, what would the law say if the data that is stored or transmitted belongs to a third state? Or what happens if data owned by a state is transferred abroad onto the territory of another state? The majority of Experts do not give the state the right of sovereignty over it unless international law specifies it or where there are other circumstances that would give the right of prescriptive jurisdiction over data abroad.[514] Contrarily, few of the Experts agree that the state's right of sovereignty over this data exists outside its territory. For this minority, state sovereignty extends to its persons or activities across borders to anywhere. Yet, Rule 3 in the Tallinn

[507] Ibid, 14.

[508] Ibid, 14.

[509] Ibid.

[510] Ibid, 13.

[511] Ibid.

[512] Ibid.

[513] Ibid, 15.

[514] Ibid, 16.

Manual recognises external sovereignty of the state by stating that “a State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.”[515] This rule indicates that a state is free to decide its external relation with other states. Moreover, it is independent in joining a cyber treaty or signing an agreement about cyber activity with another state, as long as this agreement complies with international law.

The previous discussion assumes the state has internal and external sovereignty over its cyberspace, and that any violation of that right by another state triggers state responsibility.[516] However, the violation could also be committed by a non-state actor, does this then also constitute a violation of this principle? Similarly to how the US supported the Contras in Nicaragua and thereby violated the non-intervention principle despite acting through a non-state group, states can also violate this principle by acting through third parties within a cyber context.[517] The Group of Experts also concurred that a violation of cyber sovereignty can happen on account of a state – if it is not done on behalf of a state, it will violate another international principle but not sovereignty.[518] These questions of state responsibility have been investigated in previous parts. However, to reiterate for the cyber context, the state may apply countermeasures against a state whose territory has been used by a non-state actor to launch a cyber-attack against another state. The basis for this is the principle of due diligence, which requests from the state to prevent its territory from being abused for an attack against another state.[519]

There are some circumstances that need to be illustrated with regard to the principle of sovereignty and cyber operations. One of them is when an organ or official of a state, who is physically located in another state, conducts a cyber-attack against another state while physically located in the victim state. The Group

[515] Ibid

[516] On how the violation of cyber sovereignty constitutes a breach of obligations see Alex Xiao, Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election, Ibid, 371.

[517]S Watts, Low-intensity Cyber Operations and the Principle of Non-intervention from Cyber War: Law and Ethics for Virtual Conflicts,Ibid, 21.

[518] Ibid, 17.

[519] Ibid, 18.

of Expert considered that such conduct is a violation of state sovereignty.[520] Another matter is when a state conducts cyber espionage against another one from within its territory, means the person who collects the data is physically on the territory of the victim state. The majority of the Group of Expert agreed to consider this activity as a violation of sovereignty because it is non-consensual espionage.[521] However, a few of them consider it as an exception to the sovereignty principle since this activity is merely surveillance and gathering data without altering or damaging it.[522] Moreover, when a cyber operation has been launched against another state but does not get to that state, for example because of its high level of security, the Group of Experts does not consider it a violation of the state's sovereignty because the consequences must be at least starting to manifest to be considered a violation.[523]

However, regarding the intention of creating harm, the Group of Experts holds that even if a cyber operation is not directed against a state but accidentally damages cyber infrastructure, it must still be considered a violation of sovereignty regardless of the intention.[524] The Experts also agreed that a cyber operation against private cyber infrastructure which is located in international territory such as the high seas or international airspace is not a violation of sovereignty.[525] On the other hand, if a cyber operation targets infrastructure belonging to a state, no matter where it is located - even on the high seas - it does amount to a violation of that state's sovereignty.[526] The Group of Experts agreed further that some specific matters did not constitute a violation of state sovereignty, irrespective of where they are located: cyber operation which result in severe economic loss, propaganda, and cyber crime. In addition, state consent for the cyber operation removes any accusation of wrongdoing.[527] The Group of Experts discussed another controversial

[520] Ibid, , 19.

[521] Ibid.

[522] Ibid

[523] Ibid, ,24.

[524] Ibid.

[525] Ibid.

[526] Ibid.

[527] Ibid, , 25-27.

matter, namely remote cyber operations, such as disturbing wireless signals. If these remote cyber operations do not manifest any consequences, they will not be considered a violation of sovereignty. On the other hand, if consequences of the remote cyber operation do manifest, it has not yet been settled in international law what would apply.

The Group of Experts suggests two criteria for deciding this case. The first is the degree of affecting territorial integrity, and the second is how far the interference would inhibit governmental functions.[528] With regard to the first part of the assessment, there are three possibilities (physical damage, loss of function, consequences below the loss of function).[529] The majority of the experts were in favour of the view that remote cyber operations which result in physical damage are to be considered a violation of sovereignty because the object and purpose of sovereignty is protecting state integrity and this has then been violated by the cyber operation.[530] However, a minority of the experts noted that this cannot be the rule for all types of physical damage situations - it may appear that some cases do not rise to the level of a violation of state sovereignty.[531] On the other hand, the Group of Experts does not have a contrasting view in regard to the loss of function result. They agreed that a remote cyber operation which affects another state, resulting in a loss of functionality of its infrastructure, violates its sovereignty if this attack's consequences require the state to reinstall and replace physical items. However, the experts could not draw a line or define a limit of what loss of function could amount to a violation and which would not because of the lack of state practice.[532]

In this context, the Shamon attack on Aramco cyber infrastructure is a suitable example because Aramco had to repair thousands of the company's hard drives due to this attack.[533] This will be analysed in more detail in Chapter 4. The third possibility regarding the degree of infringement is that the remote cyber operation consequences fall below the threshold of loss of functionality. The Group of Experts

[528] Ibid, 20-23.

[529] Ibid.

[530] Ibid.

[531] Ibid.

[532] Ibid.

[533] Ibid.

did not reach an agreement in this case. However, some experts suggested some examples amount to a violation of sovereignty such as “altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; embedding malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation.”[534]

The second basis of determining the lawfulness of a remote cyber-attack is assessing the interference with inherent governmental functions or the usurpation of it.[535] The Group of Experts agreed that this level of effect is considered a violation of state sovereignty because the state has the right to decide freely how to perform.[536] The Tallinn Experts define cyber operations which affect the inherently governmental functions as “a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions”.[537] The author holds that this is a rather vague definition, given that there are no specifications of operations or effects or services. Furthermore, there is no level required for the interference or even an accurate threshold. The author, therefore, suggests that there is a need to define what exactly they mean by “necessary”. This would make it clearer and more fit for purpose.

However, the experts listed some examples of cyber operations that could belong to that category, such as targeting data or collecting taxes or the conduct of elections.[538] Moreover, this assessment will be used is cases where cyber operations conducted by a state block the access of another state to its internet. If

[534] Ibid.

[535] Ibid, 21-23.

[536] Ibid.

[537] Ibid.

[538] Ibid. See for a discussion on how the Russian interference in the 2016 US elections could be constructed as an unlawful intervention: Tsagourias, N. Electoral cyber interference, self-determination and the principle of non-intervention in cyberspacem Ibid, 2; see also Annachiara Rotondo and Pierluigi Salvati, Fake News, (Dis)information, and the Principle of Non-intervention, in: The Cyber Defence Review, SPECIAL EDITION: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition (2019), pp. 209-224, 210 et seq.

this operation interferes with inherent governmental functions, the operation would be a violation of sovereignty.[539] Another case used for this assessment is a cyber operation targeting cyber infrastructure owned by a state but located on another state's territory. The majority of Experts considered it a violation of sovereignty as long as it inhibits inherent governmental functions. Yet, a few experts reject that view because they stipulate that the targeted cyber infrastructure is located in the state's territory.[540] There are two terms in this context that need to be illustrated to avoid confusion. 'Inherently governmental function' refers to government functions, whereas intervention deals with *domain reserve.* Moreover, a violation of the latter requires an element of coercion, whereas a violation of the inherently governmental function does not.[541] However, a violation of any of these principles is a wrongful act which leads to state responsibility being triggered, which may be difficult in the cyber realm due to the attribution issue. Watts discussed this issue as well when applying the basic rules of non-intervention to the cyber context. The author agrees with his assessment that the rules do apply, but that collecting evidence to that effect will be often impossible.[542]

This section on non-intervention and cyber space reiterated some general points made earlier regarding the principle of non-intervention, and then discussed and applied it in relation to the cyber space. Following an analysis of coercion and determining that a casual nexus was also relevant and necessary for classifying whether a specific cyber operation can be classified as an unlawful intervention, the author also discussed the question of sovereignty over cyber space. It can be concluded that cyber operations may still violate international law, even if they do not rise to the level of use of force or to the level of an armed attack. There are many activities, as has been shown, in this part that would violate the non-intervention principle and the state cyber sovereignty.

---

[539] Ibid.

[540] Ibid.

[541] Ibid,, 24; also Tsagourias, N. Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace, Ibid,8.

[542] S Watts, Low-intensity Cyber Operations and the Principle of Non-intervention from Cyber War: Law and Ethics for Virtual Conflicts,Ibid, 8.

3.4 Due diligence

With regard to state practice of sovereignty on its territory, it is also important to consider the concept of due diligence. That concept has been mentioned previously in assessing the state involvement in any non-state actor attack. The assessment of an "unable and unwilling" state to stop any illegal activities on the state territory is relied on in this discussion on the due diligence principle. Due diligence means the care that can be reasonably expected or required toward the rights of states in an international context.[543] The concept of due diligence emerged in international law in the seventeenth century in order to mediate the relations between different nation states, and continued to evolve during the nineteenth and twentieth centuries in order to consider state neutrality and the need to protect individuals who were not citizens of the nation state in question.[544] Perhaps the most important example of the exercise of the due diligence principle in international law is the 1949 *Corfu Channel Case*. In this instance, the International Court of Justice (ICJ) found that the second British passage through the Straits undertaken with the intention of using force to repeal an attack amounted to a demonstration of force. In normal circumstances, this would be considered unlawful, but because the British forces were justified in defending themselves in light of previous illegal use of force by Albania, their act was not a violation of Albanian sovereignty.[545] In light of this, the ICJ stated that it was "every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states."[546]

---

[543] Camilla Gambarini, 'Due Diligence,' (4 June 2021). Available at: https://jusmundi.com/en/document/wiki/en-due-diligence-1 [accessed 5 July 2021].

[544] Ibid.

[545] Jan Kittrich, The Right of Individual Self-Defence in Public International Law, (2008), Logos Verlag, 177.

[546] Radim Polcak and Dan Jerker B. Svantesson, Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law, (Edward Elgar, 2017), 70–71.

With this in mind, due diligence is generally understood to be a principle guiding and/or obligation related to relations between nation states.[547] However, there are a number of challenges to applying due diligence in practice. First, it must be determined what level of due diligence is required of the state regarding their activities in the international arena. To this end, it is questionable whether their activities should be determined in relevance to the due diligence principle or in reference to individual state practice.[548] It also needs to be decided whether the obligation incurred by the due diligence principle is subjective or objective. This means that it must be determined whether a failure to practise due diligence is due to faulty organs or due to an objective assessment of the state's actions and their likely consequences.[549] As well as this, it needs to be considered whether the content of state commitment to due diligence is fixed or flexible, depending on the factual circumstances where the duty applies.[550] Finally, there is a need to identify the limits of due diligence.[551]

Although the Corfu Channel case confirms the subjective perspective on due diligence, an objective approach is often more relevant.[552] This is especially apparent in reference to the increasing capacity of internet-based technology. Notably, a state's economic and technical capacities may affect how it fulfils its due diligence obligation.[553] In response to this concern, a report by the ILA Study Group on Due Diligence in International Law published in July 2016 emphasised the tripartite core of the due diligence principle, proposing that the sovereign state is obliged to ensure that its jurisdiction (including all spaces where the sovereign exercises formal jurisdiction or effective control) other state's rights and interests, including those with respect to the production of their citizens and companies, are

[547] Joanna Kulesza, Due Diligence in International Law, (May 2017), 17(11) JIL. 24, 29-31.

[548] Ibid, 263.

[549] Ibid.

[550] Ibid.

[551] Ibid.

[552] Ibid.

[553] Radim Polcak and Dan Jerker B. Svantesson, Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law, 2017), Edward Elgar, , 71.

not violated.[554] Due diligence is therefore a default standard related to sovereignty in international law that is subject to interpretation. These examples indicate that sovereignty holds a complicated position in international law. Notably, a state possesses sovereignty over the geographical area it is in control of; however, it cannot overrule another sovereign state if both have equal right over the same territory, states can have sovereignty even if they do not possess any territory or cannot rule the area they have legal sovereignty over, and the due diligence principle is challenging to apply, as discussed earlier, in reference to the expanding capacities of the internet.

Saudi Arabia is an important example in this thesis, it issued a Counterterrorism Law in 2017 which prevents Saudi territory from being utilised by terrorists. Furthermore, this law forbids any terrorist act against Saudi from inside and outside its territory and criminalises any act within its territory against any state. This Saudi position supports the due diligence principle and activates it by law. This is a deterrence to protect its territory to prove Saudi Arabia is working in good faith to stand against the non-state actor activities.

To conclude, sovereignty is a right of a state which can be exercised independently and without any interference from any other states. It will allow states to exercise its power internally over its territory and externally by determining its own foreign policy and international relations with other states. Moreover, it enables states to exercise their extraterritorial authority over some areas, such as the state's embassies and councils abroad. This right comes with an obligation on the state. The state is obliged to guarantee its territory has not been used illegally against another state or as a safe haven for terrorist groups. This due diligence principle is not a heavy burden on the state, as it comes with some flexibility because its application depends on the state's military and cyber capacity and the power of the government.

[554] Ibid.

3.5 Attribution of state responsibility for cyber operations

In section 3.2 the author examined the primary rules concerning state responsibility, whereas this section will discuss how these rules can be attributed to cyber space. As a brief reiteration of the relevant points, one needs to underline that the basic rules of international state responsibility originated from customary international law, which can be seen in the International Law Commission's Articles on State Responsibility. This chapter, however, will analyse and then apply these rules to the cyber space. First, this part will discuss the question of attribution and how it applies in a cyber context.

The Group of Experts agrees on applying these general rules of state responsibility to cyber operations.[555] In the Tallinn Manual, there is consequently a rule that says a 'State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.'[556] It is important to point out that the Manual uses the phrase 'cyber-related act', which indicates that state responsibility covers all wrongful acts related to cyber circumstances, even if an action or event is not considered a cyber operation in itself. This is the case, for example, if a non-state actor conducts a cyber operation against another state by using the state's cyber infrastructure without any deterrence from the state or any act to stop this cyber operation. In this circumstance, the state still bears the responsibility for the non-state group's cyber operation.[557]

Furthermore, if the wrongful cyber act violates any peacetime or armed conflict rules, the state will still be held to account.[558] In the cyber realm, it is necessary to use such a phrase (cyber-related act) because there are many more cyber-related activities than just conduct that constitutes a cyber-attack. Furthermore, unlike the threshold for the use of force, state responsibility does

[555] Tallinn Manual, (2017), 84

[556] Ibid, 84.

[557] Ibid, 8–85.

[558] Ibid.

neither require physical damage nor injury.[559] In addition, both intention and geographic location of the attack source are not preconditions to consider a cyber operation a wrongful act. Moreover, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security stated that "States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."[560] It is clear that this report considers cyber-attacks against another state as an "internationally wrongful act" which triggers state responsibility for that attack. Moreover, it does find the state responsible for the cyber operations which were launched by the non-state actor as long as it originated from its territory.

In order to categorise a cyber operation as an international wrongful act, it needs to be conducted by a state organ.[561] For illustration, any wrongful cyber act conducted by 'the intelligence, military, internal security, customs, or other State agencies'[562] will be considered as undertaken by the state. Furthermore, the state will bear the responsibility for a wrongful cyber act even if domestic law does not qualify the acting person as a state organ or, in the case of a state official, if an organ exceeds its authority or does not follow orders.[563] Sometimes, a state may authorise persons or entities to undertake certain activities. If these activities breach

---

[559] Ibid.

[560] Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly Res. A/68/98, Paragraph 23, (June 7, 2013) http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[561] Tallinn Manual, (2017) Rule 15, 87.

[562] Ibid, 85–86.

[563] The ICJ stated in the Genocide Judgement 2007 that 'persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in "complete dependence" on the State, of which they are ultimately merely the instrument', Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), [2007] Judgment, I.C.J. Reports, para 393.

a binding obligation of the state, the state will be found responsible for that act.[564] This is obvious when the state grants a private corporation the authority to launch a cyber operation against another state.[565] Additionally, the state will be responsible for the wrongful act even if it originated from a private group or persons without the state's direction or if the state is unable to exercise its authority.[566] In this regard, the Tallinn Manual adopted the same rules on state responsibility which are stated in the Draft Articles on State Responsibility.[567] This confirms the Tallinn Manual approach of applying international law rules to cyber operations.

In this context, it is worth noting that not all cyber operations that originate from governmental sources can be defined as originating from the state. It is just an indication that the attack was conducted by using state resources. This is because governmental infrastructure might have been hacked or that its IP addresses were used by feigning tactics.[568] That occurred in 2013, when Ukrainian government websites were attacked by malicious cyber activity that appeared to have been launched from the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), which was not the case, but rather by 'spoofing' the source of the IP address.[569] This is clearly an issue complicating attribution in the cyber realm because it is very common for the true origin of an attack to be disguised; moreover, it is also something which hackers can easily do. There are cases where a state puts

---

[564] Tallinn Manual, (2017), 85–86.

[565] Ibid.

[566] This rule is based on Article 9 of the Articles on State Responsibility, which states that 'The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority'. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid.

[567] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid.

[568] Ibid.

[569] Spoofing is defined as 'the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.'
https://www.forcepoint.com/cyber-edu/spoofing.

its official organs at the disposal of another state. If the loaned organ has full control over the authority and acts, it is considered acting on behalf of that state. However, if the sending organ is directed by its own home state and follows its instruction, the state that the organ is placed in will not be responsible for any wrongful acts.[570]

Another difficult case occurs when a cyber operation is attributable to a non-state actor. In this situation, a state may be found responsible for the actor's activities only in two circumstances. First, if the conduct of the non-state group is under the state's direction and instructions. Second, if the state adopts the operation and claims attribution.[571] Therefore, states 'do not escape the legal responsibility for internationally wrongful acts by perpetrating them through proxies.'[572] Moreover, it is worth considering that both the Tallinn Manual and the Draft Articles on State Responsibility use more than one term to describe the connection of a state with the activities of non-state groups, which are 'instruction, direction and control'. The commentary on the Articles on State Responsibility illustrates that all three terms need to be 'understood in the disjunctive'.[573] That means each term needs to be interpreted separately. As a result, each term has a distinct meaning based on the case circumstances and indicates that they cannot be considered synonyms for each other. Otherwise, the ICJ has used the phrase 'effective control' both in its Nicaragua and Genocide judgements,[574] which indicates that the terms 'direction' and 'control' are treated by the court in the same way.

Furthermore, the court describes the way of control required in its judgements as 'effective', which is dissimilar to the 'overall control' that is required in the characterisation of armed conflict.[575] At the same time, 'overall control' has been recognised by the International Criminal Tribunal for the Former Yugoslavia (Tadic

[570] Tallinn Manual,(2017), 93.

[571] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid, Art 8, para 7. Tallinn Manual (2017), Rule 17.

[572] William Banks, State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0, (2017), 95 Tex L Rev 1487, 1496.

[573] ILC Commentary to the Articles on State Responsibility, Ibid, Article 8, para 7.

[574] Nicaragua case, para 115; Genocide judgement, [2007] Judgment ,Ibid, para 400.

[575] Genocide judgement,Ibid, [2007] Judgment, para 404–406.

case).[576] The Tribunal stated that 'Where a state has a role in organizing, coordinating, and providing support for a group, the group's acts are attributable to the state.'[577] However, the ICJ continues to use the term 'effective control'. In the application of the Genocide Convention (Bosnian Genocide Case),[578] the court required a 'smoking-gun' to decide if Bosnia intended to commit genocide, which means the Court followed a standard of 'beyond any doubt', not a 'reasonable doubt'.[579] Grosswald commented on the "effective control" test by "it became customary to analyse the level of effective control exercised by the agents of one state over the private actors of another state in order to determine the level of responsibility to attribute to the host-state".[580] Which means the overall control test has not been used regularly by states. In the cyber context, 'effective control' occurs when the state decides the 'execution and course' of the cyber operation that is conducted by a non-state actor.[581] Otherwise, the standard the ICJ adopted, cannot be applied in the cyber domain due to its lacking flexibility and the difficulties of tracing cyber-attacks.[582] In order to achieve the right attribution, we need an 'overall control' standard that has more portability to apply in the case of cyber-attacks. Grosswald made an explanation between the ICTY judgements, which based on the degree of control.[583] He emphasised that:

---

[576] The Prosecutor v. Duško Tadić a/k/a "Dule", [1997],ICTY, IT-94-1-T, para.128.Generally, however, one needs to be mindful that Tadic was about individual criminal responsibility, whereas the Bosnian Genocide case was on state responsibility.

[577] Ibid.

[578] Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Yugoslavia) [1996],,ICJ 422.

[579] Scott J Shackelford, and Richard B Andres. 'State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem.' (2010), Geo J Int'l L 42, 986.

[580] Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, (2011), 36 Brook. J. Int'l L, 1160.

[581] Tallinn Manual (2017), 96

[582] Scott J Shackelford, and Richard B Andres. 'State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem', Ibid, 988.

[583] Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, Ibid.1161

> "the ICTY requires control beyond financing and equipping forces and should, but does not necessarily, include planning and supervision of military operations. Importantly, the ICTY in Tadic focused on individual responsibility, distinguishing the case from Nicaragua, which focused on state responsibility. After all, the Tadic court believed state responsibility should be based on a "realistic concept of responsibility."[584]

In this context, acts that are performed ultra vires in relation to a cyber operation conducted by a non-state actor with the 'effective control' of a state will be attributable to the state as long as the non-state actor is essentially integrated in that operation.[585] However, the Group of Experts noted that the state may be found irresponsible if the ultra vires cyber operation does not have a purpose related to the operation.[586] Even though supporting and encouraging a non-state group in its activities by a state is not considered a wrongful act, the state will still be considered to have violated another principle of international law, namely the principle of non-intervention.[587] However, regarding this point, the Tallinn Manual has a contrary opinion. There is a contradiction which makes it impossible to say whether Tallinn has a strict or flexible approach in this regard. On the one hand, they refer to the "overall control" approach in deciding the state engagement in a cyber operation but on the other hand, they did not count the "supporting and encouraging" of a non-state actor by a state as a wrongful act.

The acts categorised as "supporting and encouraging" acts are still prohibited acts and if they amount to an intervention, they will still constitute a wrongful act. This analysis is based on Article 3 of the Articles on State Responsibility for Internationally Wrongful Acts. This Article considers an act as a wrongful one when it "constitutes a breach of an international obligation of the State."[588] The Tallinn Manual considers the ILC Articles to reflect customary law, this can be seen for

---

[584] Ibid.

[585] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid, Art. 8, Tallinn Manual (2017), 81

[586] Ibid.

[587] Ibid.

[588] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid, Ibid, Art.3

example in rule 17, which is reflective of the previously discussed ICJ's 'effective control' test adopted in e.g., Nicaragua. They do note that 'overall' control is of a lower threshold, but ultimately agree to adopt the higher threshold of effective control.

Another approach was introduced by the ICJ in the case of the Iranian hostages' crisis, which the court called 'government awareness'.[589] According to this approach, if the government is aware of its obligation to prevent its cyber infrastructure from being used to launch cyber-attacks against another state, and it fails to comply with this obligation, the state will be found responsible for those attacks.[590] This approach is part of the argument that acknowledges the standard that states are required to be aware of and prevent harmful cyber operations against another state. There will be a further discussion on this subject within the section on due diligence.[591]

In the context of the extension of state responsibility, there is also the possibility that the wrongful action has been conducted by another state that is responsible for that activity. There are three methods for finding a state responsible for a wrongful act against other states: by aid and assistance, direction or control of the operation, or coercion of the other state. In all these ways, the state must acknowledge that the acts are wrongful and breached international law.[592] As illustration, the state will be found responsible for directing and coercing another state for just the result of the wrongful act, which means that in this situation, state responsibility depends on the consequences. In contrast, in the event of the assistance of another state, the responsibility of the assisting state depends on the level of contribution and causing the wrongful act. For instance, consider state A finances state B for its wrongful cyber act against state C. In this circumstance, state A may be found responsible for the act of assisting (financing) to the extent of causing the wrongful cyber act.[593] Another example is a situation where state A has the money but lacks the technology and aims to target state B. In this scenario, state

[589] Ibid.

[590] Ibid, 989.

[591] See page 136.

[592] Ibid.

[593] Tallinn Manual (2017), 81

A requests technical assistance from state C, and they consequently launch a cyber-attack against state B. The responsibility of state C is dependent on the level of the technical support which it has given to state A.

With regard to the coercion of another state to conduct a wrongful cyber act, this coercion must be 'extremely high' to establish the responsibility.[594] However, the third state may be found not responsible for all the wrongful acts, which will be discussed below in the next part.

3.6 Precluding the wrongfulness of the act

In some circumstances, such as in cases of self-defence, consent, countermeasures, necessity, force majeure or distress, the wrongfulness of an act may be precluded. The situation of self-defence was discussed and emphasised earlier in Chapter 2. The second situation occurs when a state has consented to the cyber action of another state. For instance, if state A asks state B to take control of some cyber infrastructure in its territory in order to assist them in responding to and defending their cyber capacities from malicious attacks. The actions of State B act are not considered a wrongful act or a violation of the principle of non-intervention or sovereignty.[595]

The consent could be understood expressly or implicitly.[596] However, mere consent is not enough, as stated in the Nicaragua judgement by the ICJ: 'merely presumed on the basis that the State would have consented if it had been asked'.[597] Therefore, the consent needs to be obvious beyond any doubt.

---

[594] Ibid, 81.

[595] Tallinn Manual (2017), 79–84.

[596] Arrest and Return of Savarkar, (France v Great Britain), [1911] Award, XI RIAA 243, ICGJ 401 252–255.

Russian Claim for Interest on Indemnities, (Russian Federation v Turkey) [1912], PCA Award, ICGJ 399, at 446.

[597] Nicaragua Case, para 99.

The third situation that precludes the wrongfulness is the use of force majeure, which is defined as 'circumstances that involve "the occurrence of an irresistible force or of an unforeseen event, beyond the control of the State, making it materially impossible in the circumstances to perform the obligation."'[598] On the one hand, this indicates that the unavoidable event needs to be the main cause for the impossibility of the state performing its obligation.[599] On the other hand, changes in the economic and political circumstances that make the state unable to perform its obligation do not amount to a force majeure.[600] Furthermore, if the impossibility of performance caused by the negligence of the state or the latter assumes the risk previously in the treaty, it will not be a force majeure.[601] Force majeure is a significant case in international law that frees the state from fulfilling its obligation. The fourth ground for preclusion is distress. In this situation, the state in question has no option other than to dismiss the state's obligation to save the life of an individual or other people.[602] The fifth and sixth situations, which are the concepts of countermeasures and necessity, which are the most related situations to cyber cases. They will be illustrated in detail below.

3.6.1. Countermeasures

Countermeasures are the most used type of reaction from states. These are known as 'a response to actions taken by a party to an international armed conflict with respect to violations of legal regimes other than the law of armed conflict'.[603]

---

[598] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid,, Art 23.

[599] See, eg, Gould Marketing, Inc v Ministry of Defence of Iran, Interlocutory Award No ITL 24–49-2, 3 Iran–US CTR 147, 153 (27 July 1983).

[600] Rainbow Warrior (New Zealand v. France), [1990],Arbitration Tribunal award , 82 I.L.R. 500, para 77.

[601] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts , Ibid, Art 23(2)(b).

[602] Ibid, Art 24(1).

[603] Tallinn Manual (2017), 111–112.

These have been acknowledged by the ICJ in several cases.[604] Moreover, Rule 21 of the Tallinn Manual states that 'Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State.'[605] Such compliance of a state with its obligation will include providing assurances or guarantees and making reparations.[606] Banks explains, 'countermeasures are designed to persuade the perpetrator to stop its unlawful actions, not as punishment or escalation.'[607] As a result, countermeasures have a temporary character. As described by the ICJ, 'countermeasures should, to the extent feasible, be taken in such a way as to permit the resumption of performance of the breached obligations underlying the countermeasures'.[608] To achieve a legal use of countermeasures, such need to be proportionate to the injury or damage.[609] That means they need to 'commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question'.[610] Proportionality in this context is distinguished from the requirement for self-defence. There is no requirement for mutuality for the type of act or the number of attacks.[611] There is also no need for specific procedures and targeting the same point of a launched attack.[612] Moreover, the countermeasures should not affect any obligations owed to a third state. Therefore, the injured state should terminate any countermeasure that violates a third state's right.[613] The countermeasures need to

[604] Nicaragua judgement, para 249; Gabčikovo-Nagymaros Project, Hungary v Slovakia, [1997], ICJ Reports, , paras 82–83.

[605] Tallinn Manual (2017), 111–14.

[682] Nicaragua judgement, para 24949 (1).

[607] W Banks, State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0, Ibid, 1502.

[608] Gabcˇíkovo-Nagymaros Project ,Ibid, para 87; International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid Art 49(3)

[609] Harrison, Dinniss, Heather. Cyber Warfare and the Laws of War, Cambridge University Press, 2012, 105.

[610] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid, Art 51.

[611] Tallinn Manual (2017), para.9, 119

[612] Ibid.

[613] Ibid, Rule 25.

be applied in compliance with human rights rules and diplomatic and consular rules. In addition, they should not violate a peremptory norm.[614] Furthermore, the non-state cyber operation could justify countermeasures if the state violates the due diligence obligation.[615]

With regard to countermeasures, the target must be a state.[616] However, the Group of Experts in the Tallinn Manual also considered the case of a non-state actor being a target of countermeasures if there is an agreement between them and the state and the NSO breached their obligations.[617] Otherwise, there was a disagreement between the Experts because international law prohibitions only apply to states. It is worth noting that the Security Council measures pursuant to Chapter VII of the UN Charter do not amount to a countermeasure because they are lawful in nature.[618] In contrast, the countermeasures must be taken by the injured state. There is, for example, the Sony hack in 2014, which has been attributed to North Korea and gave the United States the right to 'hack back' as a countermeasure.[619] Moreover, a minority of the Group of Experts allowed a non-injured state to take countermeasures once the injured state has requested the non-injured state to do so.[620] On the contrary, the majority takes a position similar to that of the ICJ in the Nicaragua case, stating that 'purported countermeasures taken on behalf of another State are unlawful'.[621] Nevertheless, the minority view seems reasonable because it is made in reliance on the injured state's request.

---

[614] A peremptory norm is 'a norm accepted and recognised by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character' .Vienna Convention on the Law of Treaties, Ibid, . Article 53

[615] C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid,1620

[616] Tallinn Manual (2017), 116–120.

[617] Ibid.

[618] Charter of the United nation, Ibid,Chapter VII.

[619] Tallinn Manual (2017), Rule 24, 130.

[620] Ibid, 132.

[621] Ibid.

In some cases, a state may assist an injured state in taking countermeasures against a wrongful cyber act. In this regard, the Tallinn Experts have three views. One is the view that such an action is similar to taking measures on behalf of a state that is prohibited, as discussed above. The second considers the assistance a violation of an obligation owned by the state. The last one considers aid for an injured state as lawful because it is not similar to doing so on behalf of the injured state. However, the experts agreed unanimously that the 'State that aids or assists a cyber operation that fails to qualify as a countermeasure may be held responsible for aiding or assisting an internationally wrongful act'.[622] This thesis agrees with the second view, which confirms that assistance is a lawful act. A basis for this legality can be found in the United Nations Charter, which encourages cooperation between states and helping each other.[623] There are some state views on collective countermeasures. Estonia noted that non-injured States "may apply countermeasures to support the state directly affected by the malicious cyber operation".[624] Schmitt has described this view as "an advantageous development in the catalogue of response options that international law provides to deal with unlawful acts". While France has rejected this view as it is, in its opinion, against international law.

It is worth noting that countermeasures do not have an anticipatory element like self-defence arguably does. Therefore, it can be described as a 'reactive' not a 'prospective act,[625] which means it cannot be employed for an imminent attack or as a protective measure. The ICJ noted this in the Gabčíkovo-Nagymaros judgement by stating that such an action 'must be taken in response to a previous internationally wrongful act of another State'.[626]

Taking any other measures before countermeasures is not an acceptable condition.[627] Otherwise, the Group of Experts could not reach a consensus regarding

[622] Ibid, 132.

[623] Charter of the United Nation,Ibid, Art.1/3.

[624] President of Estonia, Kersti Kaljulaid, 'President of the Republic at the opening of CyCon 2019' (29.05.2019). Available at: https://president.ee/et [Accessed on 2 Feb 2023]

[625] Tallinn Manual (2017), 132.

[626] Gabčíkovo-Nagymaros project judgement,Ibid, para 83.

[627] Ibid.

taking lesser means before starting any countermeasures. The majority were of the view that there is no need for such means because it is required to give a notification before taking any measures.[628] However, the injured state can employ 'urgent countermeasures' without a prior notice. With regard to cyber operations, such a notification could make the countermeasures meaningless because the cyber operation has a very fast effect and there would be no time for negotiations or any other form of procedure.

Based on customary international rules, a minority of the Group of Experts requires the injured state to negotiate prior to taking any countermeasures. In contrast, the majority of the group does not require such previous steps before launching countermeasures.[629] Given the nature of the cyber operation and how fast and immediate its effects are, it would be more effective to take countermeasures directly without any prior steps. After all, the goal of countermeasures is to terminate the harmful cyber act. Therefore, the victim state should act immediately in response to the direct effect of the cyber operation. However, regarding the necessity of a prior notification before using countermeasures, the United States noted that "Before an injured State can undertake countermeasures in response to a cyber-based internationally wrongful act attributable to a State, it generally must call upon the responsible State to cease its wrongful conduct, unless urgent countermeasures are necessary to preserve the injured State's rights."[630] The Netherlands as well agreed with that view and requires a prior notification unless there is "immediate action is required in order to enforce the rights of the injured state and prevent further damage".[631] The GGE finds that it is necessary to notify the responsible state before employing any countermeasures against it. The reason is to give that state a last

[628] Tallinn Manual (2017), 116–133.

[629] Ibid.

[630] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 142.

[631] Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace, 26 September 2019, 7-8, Available at: file:///C:/Users/suliman%20AL-Omari/Downloads/international-law-in-the-cyberdomain-netherlands.pdf [Accessed on: 2 Feb 2023]

chance to comply with its obligation before taking any steps against it.[632] On the other hand, the United Kingdom does not consider a prior notice as a legal requirement to use countermeasures.[633] It justified its position because "prior notice could expose highly sensitive capabilities and prejudice the very effectiveness of the countermeasures in question."[634]

As explained previously, this method cannot be realistically used in the cyber realm due to the speedy nature of the cyber operation. As Liu commented, "Notification" consumes time, does little to reduce injury, and tarnishes inter-State relations."[635] Also, Roscini has criticised this requirement because it "deprives the operation from one of the main advantages, i.e. their anonymity."[636]

Another controversial issue is whether countermeasures' limitations go beyond the threshold of the use of force. The experts reached an agreement that countermeasures must not amount to an armed attack. At the same time, they are divided with regard to the use of force. The majority prohibited the countermeasures from including any type of activity considered as a use of force, while the minority does not require that.[637] The experts concluded that: 'What this approach might mean in the cyber context will remain an open question until uncertainty as to the use of force and armed attack thresholds is resolved.'[638] The United Kingdom and Netherlands would not allow exercising the use of force in countermeasures.[639]

---

[632] Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF U.S. PRACTICE IN INTERNATIONAL LAW, ch 18, § A(3), at 13, https://www.state.gov/documents/organization/244486.pdf [https://perma.cc/5VDX-2M7X].

[633] United Kingdom Foreign, Commonwealth & Development Office, Application of international law to states' conduct in cyberspace: UK statement, 3 June 2021.

[634] Ibid.

[635] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 234.

[636] M Roscini, cyber operation and the use of force, p106.

[637] Tallinn Manual (2017), 135–142.

[638] Ibid.

[639] The UK stated that "They must be carried out in accordance with the conditions and restrictions established in international law and must in particular not contravene the prohibition on the threat or use

However, the view of the thesis in this regard is that the countermeasures need to be proportionate to the wrongful act as an essential condition and any other threshold needs to be assessed on a case by case basis. Because of the unpredictability of the cyber realm, no hard restrictions should apply – one cannot tell what measures might be necessary before it happens. As a result, the countermeasures should be decided on a case-by-case basis.

3.6.2. Necessity

The final situation that precludes any wrongfulness from an act is necessity. This is identified by the Articles on State Responsibility as 'a circumstance in which a State's "essential interest" faces "grave and imminent peril" and the sole means of averting that peril is temporary non-compliance by the State with its international obligations of "lesser weight or urgency".[640] This definition mentions the 'essential interest', which has no internationally accepted definition. Interestingly, in the 2013 Tallinn Manual, which was the first version of the Manual, barely addressed necessity in the cyber realm. However, the second version of the Manual has discussed it in detail starting with Rule 26 where the Group of Experts defined it as 'an essential interest is one that is of fundamental and great importance to the State concerned.'[641] Another significant phrase in the definition is a 'grave and imminent peril', which the Group of Experts described as 'when the threat is especially severe. It involves interfering with an interest in a fundamental way, like destroying the interest or rendering it largely dysfunctional.' Moreover, Schaller describes "necessity

---

of force," United Kingdom Foreign, Commonwealth & Development Office, Application of international law to states' conduct in cyberspace: UK statement, (3 June 2021), Available at : https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement [Accessed on 2 Feb 2023]; Netherlands noted that countermeasures "not rise to the level of use of force or breach peremptory norms of international law" Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace, Ibid, 7-8.

[640] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid Art 25, para 1 of commentary.

[641] Tallinn Manual (2017), 135–142.

[as a plea that] has been understood as a subjective right of the State to self-preservation".[642]

The Tallinn Manual follows the ILC Articles in many of its rules. However, there are also some differences between them. For example, the Tallinn Manual stats in Rule 26 that "A State may act pursuant to the plea of necessity . . . when . . ..", whereas the ICL Articles on State Responsibility declared that in Article 25 "Necessity may not be invoked . . . unless . . . .". The difference here is how the condition of using the plea of necessity is addressed. Tallinn used a less strict phrase by stating "When" but the ILC Articles used a stricter word which is "unless".[643] The Tallinn Manual says the necessity can be used only under these conditions, while the ILC Articles says the necessity cannot be invoked until meeting some conditions, which are formulated as a negative statement. Schaller points out another distinguishing feature between Tallinn and the ILC Articles: the latter adds two more conditions before allowing the state to act based on necessity.[644] The first condition is "the interest relied on must outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests, whether these are individual or collective."[645] This thesis agrees with that assessment. Such a condition implies that the state should not assess the importance of its interests based on its own assessment but also needs to consider other states and the international community in its assessment.

On the other hand, the second condition is that "the contribution must be sufficiently substantial and not merely incidental or peripheral."[646] The thesis does not agree with it because both the author and the Tallinn Manual believe that the effect of the measure is what determines if there was a violation of state responsibility. The Group of Expert stated that "mere failure to take preventive

[642] C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1621.

[643] C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1621.

[644] Ibid, 1624.

[645] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid,Art 25. para.17.

[646] Ibid, para 20.

measures to protect a State's cyber infrastructure from harmful cyber operations amounting to 'grave and imminent peril' does not bar measures based on necessity."[647] Moreover, the Group of Experts noted that the state's "contribution must be more than marginal."[648] This indicates that the Tallinn Manual considers the contribution as a criterion determining the necessity, which is contrary to Schaller's observation. However, he recants by saying that "Despite some textual differences, there is thus no substantial discrepancy between Rule 26 of Tallinn Manual 2.0 and Article25 of the ILC Articles on State Responsibility.[649]

For illustration, the essential interests in the cyber sphere could be to 'debilitate the State's banking system, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system'.[650] Geiß & Lahmann noted that "[I]t seems reasonable to assume that at least the protection of critical infrastructure would be accepted as such an essential interest."[651] Heathcote commented that there should be an agreement between "international community" in regard to which interests are really essential.[652] Nevertheless, some states reached an agreement to define the "critical infrastructure" which are United States, United Kingdom, Canada, New Zealand and Australia.[653] They define it as "the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic

[647] Tallinn Manual (2017), 140.

[648] Ibid.

[649] C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1624.

[650] Tallinn Manual (2017), 135–142.

[651] Robin Geiß & Henning Lahmann, Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat Prevention, in Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Tallinn,621, 644 646.

[652] Heathcote, S, 'Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity', in J Crawford, A Pellet & S Olleson (ed.), The Law of International Responsibility, (2010). Oxford University Press, 491-492

[653] See also Article by C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid.

security, prosperity, and health and safety of their respective nations."[654] Moreover, they emphasised that there are some sectors amounting "critical" infrastructure which are "communications, energy, healthcare and public health, transportation systems, and water."[655] It can be observed that these sectors do not include the banking system and neither information technology nor emergency services, which are significant and have a core role in any state. However, for the purpose of this thesis, the banking system, information technology and emergency services pose a high level of risk to the state if they have been hacked and could potentially have a negative impact on the victim state. Therefore, these sectors should be included in the interests which invoke the plea of necessity.

Regarding the imminence requirement, it needs to be 'objectively established and not merely apprehended as possible.'[656] Moreover, the measures should be 'the sole means available' to face the danger. To illustrate the nature of a grave peril, consider a cyber operation launched against a banking system, which will be sure to have immediate consequences.[657] Otherwise, there will also be a long-term effect, which is the loss of confidence by clients. Whether invoking imminency requires invoking a plea of necessity does not have a consensus answer. As Bethlehem said, "There is little scholarly consensus on what is properly meant by 'imminence' in the context of contemporary threats."[658] However, Wilmshurst suggested that "imminence is not merely a temporal criterion but depends on the nature of the

[654] Forging a Common Understanding for Critical Infrastructure—Shared Narrative, CRITICAL 5 (2014).

[655] Ibid, 6.

[656] Tallinn Manual (2017), 135–142.

[657] Ibid.

[658] Bethlehem D., Self-Defence Against an Imminent or Actual Armed Attack by Nonstate Actors, (2012).106 AM. J. INT'L L.,at 773–774

threat."[659] Lubell defines imminence as "the expected harm is identifiable, specific, and is likely to occur in the immediate future."[660]

However, in the case of a cyber operation, it will be very difficult to meet these strict conditions. As a result, it would be more practical to follow the ICJ's approach of assessing imminency. In the case of Hungary v. Slovakia, the court held that "as soon as it is established, at the relevant point in time, that the realization of that peril, however far off it might be, is not thereby any less certain and inevitable."[661] Hence, the ICJ does not take the time element into account. So, this means whether the attack is imminent or far in the future, this circumstance will not prevent the state from using the plea of necessity as the peril is certain and inevitable. On the other hand, knowing the certainly is another issue, especially in the cyber domain. Regarding the "certainly" context, Schaller noted that "The problem of uncertainty is highly relevant in the cyber domain, since the purpose of a particular operation and the peril that it may pose cannot always be clearly identified at the time the incident is detected."[662] Certainty is a part of the imminence criterion which is required when using the plea of necessity. The key assessment for that criterion could be the same one which has been suggested previously in the anticipatory self-defence, which is the "the last window of opportunity.[663]

Yet, there are reasons to be wary of the plea of necessity – most notably due to the potential threat it poses to the victim state's rights. Unfriendly states, or indeed the attacker state, could argue that using the plea of necessity means the operation did not qualify as a use of force. They could hold the fact that the victim state did not

---

[659] Wilmshurst E., The Chatham House Principles of International Law on the Use of Force in Self-Defence , 55 INT'L & COMP. L.Q. 963, 967–68 (2006). C Schaller., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid.

[660] Lubell N., The Problem of Imminence in an Uncertain World in The Oxford Handbook of the Use of Force in International Law, (2015),697–98, 702–05

[661] GabCikovo-Nagymaros Project (Hungary v. Slovakia), Judgement, 1. C. J. Reports 1997, 42.

[662] Schaller C., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1635.

[663] See pages 114-115.

immediately use self-defence against it and further violate its rights. Alternatively, the attacker state might argue this was an act just permitting a plea of necessity, not self-defence, and therefore limit the victim state's right to invoke self-defence.

Nevertheless, the Group of Experts agreed on applying the plea of necessity for a cyber operation, as the origin of this plea is customary law. The Group of Experts applies assessing the necessity in the cyber realm when the harm has manifested, and the operation is underway. If the plea of necessity includes some use of force activities, one view of the Group of Experts prohibited using force as a plea of necessity as it violates international law because the exception for the use of force applies just in the cases of self-defence and authorisation by the UN Security Council. Schaller agrees with that view and explains it with necessity, which, in his opinion, "does not provide a separate legal basis for military action."[664] In contrast, some experts maintain that it can be allowed if this is the only way to use a plea of necessity to protect the aggrieved state's cyber infrastructure.[665] The present author is of the view that the plea of necessity is available in exceptional circumstances when the state's interests are in danger, therefore the use of force could be available in the case of cyber operations against a state's interests when the use of force is the only option to protect the state interests and when there will be a huge harmful effect to the state if the state does not use force to defend its interests.[666]

In some circumstances, there will be co-operation from other states or international organisations on the basis of a plea of necessity. The majority of the experts in the Tallinn Manual argued that if co-operation could protect the state's interest, there would be no need for the plea of necessity as grounds for their activity. However, the minority took the position that if the cooperation is necessary to protect the state's interest and the only means available, it will be as if conducted by the state itself based on the plea of necessity.[667] The plea of necessity could be caused by a natural disaster or any other cause without another state being involved,

[664] Schaller C., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1621.

[665] Tallinn Manual,(2017), 137

[666] Gill, Terry D. and Tibori-Szabó, Kinga, Twelve Key Questions on Self-Defence against Non-State Actors – and Some Answers, International Legal Studies vol. 95 (2019), 494.

[667] Ibid.

which is distinguished from the countermeasures that require another state to breach its obligation. As a result, there is no requirement that the act be conducted by a state. If a cyber operation is conducted by a non-state actor, the victim state will be allowed to use the plea of necessity to defend itself if the operation does not amount to an armed attack, and the state cannot use self-defence.[668] Furthermore, this is not similar to force majeure, which has been explained above. To illustrate, when a state cannot comply with its obligation because of the circumstances, it will be a force majeure case. However, the necessity comes into account because of the essential interests of a state that faces grave harm.[669]

It is worth mentioning that necessity has been considered in line with customary international law, which is reflected in the Tallinn Manual. This has been mentioned in many cases. These cases have been characterised by Sloan and Schaller in three categories based on the ILC commentary, which are "classical or (security-related) necessity, economic necessity and environmental necessity".[670] In the case of the Anglo-Portuguese dispute in 1832, there was a treaty between Portugal and the British government regarding the protection of British properties which were located in Portuguese territory.[671] The treaty stated that this obligation does not deprive the Portuguese government from acting against this agreement during necessity incidents, such as for safety and existence of the state. This case shows the classical character of the necessity, or what Schaller calls security-related basis for necessity. Another case in that scope is the Caroline incident in 1837.[672] When the British government launched a raid on United States territory on the ground of necessity and self-preservation.

With regard to the second category, "economic necessity", the dispute between Greece and Belgium is one example. In that case, Greece refused to pay

---

[668] Ibid.

[669] Ibid.

[670] Sloane R., On the Use and Abuse of Necessity in the Law of State Responsibility, (2012)106 AM. J. INT'L L. 447, 454. Schaller C., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual's Conception of Necessity, Ibid, 1625

[671] General Assembly 35th session, U.N. Doc. A/35/10 (Supplement No. 10), at 84 (1980).

[672]Christopher Greenwood, The Caroline,[2009] , Max Planck Encyclopaedia of International Law , vol. I, pp. 1141-1143.

its debt to Belgium. The Permanent Court of International Justice in 1939 decided that if the payment will affect the essential interests of Greece and will "jeopardize the country's economic existence", the state could be precluded from the payment.[673] The last type of necessity is environmental necessity. In the ICJ judgement in the Gabčíkovo-Nagymaros case, in 1997, the court did not accept the argument of Hungary which refused to proceed building a dam with the Czech and honour their treaty obligations accordingly. Hungary based this refusal on environmental necessity.[674] The court held that Hungary does not meet the necessity conditions which were stated in the ILC draft. The court noted that the plea of necessity has its origin in Customary International Law.[675] The above-mentioned cases are proof that necessity has been recognised by the community of states in its practice and has developed an international custom in this regard.[676]

From this section, we can conclude that countermeasures and necessity will likely be the most utilised methods in the case of cyber operations. That is because a cyber operation requires an immediate response to deal with the resulting harm and terminate it. Countermeasures can be used in the event of a cyber operation that has more than one phase. The injured state will take measures to ensure that the harm of the cyber operation will not be continued. In contrast, the plea of necessity is used when a cyber operation has targeted governmental cyber interests. That is a very likely occasion for a cyber operation because it could target the state's power grid, water supplies system, or any essential cyber infrastructure in the state.

3.7. Obligation of States Concerning Internationally Wrongful Acts

[673] Société Commerciale de Belgique (Belg. v. Greece), Judgement, [1939] P.C.I.J. (ser. A/B) No. 78, at 160 .

[674]Gabcˇíkovo-Nagymaros Project, Ibid, 56

[675] Ibid

[676] Most importantly, the court identified a three-part test, as Harrisson Dinnis points out, to identify justifying proportionate measures: Dinniss, Cyber Warfare and the Laws of War, Ibid,107.

International law gives the injured state the right to demand a cessation, assurances, guarantees, and reparations from the state that has conducted the wrongful action.

This is based on the Articles on State Responsibility and has been adopted by the Group of Experts of the Tallinn Manual.[677] On the one hand, these rights consist of distinguishing assurance from guarantee by referring assurance to the actions of communication and contact. On the other hand, such a guarantee refers to ensuring that the cyber-wrong will not be repeated.[678] However, the need for reparations for the injury is acknowledged by the Permanent Court of International Justice: 'as far as possible, wipe out all the consequences of the illegal act and re-establish the situation which would, in all probability, have existed if that act had not been committed.'[679] In addition, the Tallinn Manual states in Rule 28 that 'A responsible State must make full reparation for injury suffered by an injured State as the result of an internationally wrongful act committed by cyber means.' Moreover, in cases where reparation cannot be achieved, the court emphasises the need for '[r]estitution in kind, or, if this is not possible, payment of a sum corresponding to the value which restitution in kind would bear'.[680] In order to determine the amount or type of reparation, the type of damage must be referred to. Usually, material damage can be assessed financially. Regarding cyber operations, the experts characterise the 'interference with cyber operations or the loss of data that results in financial loss' as material damage. At the same time, they consider the 'mere distress over having temporarily lost access to the Internet or losing personal e-correspondence that lacks pecuniary impact' as not a material damage.[681] Another type of damage that could require reparation is 'moral damage'. This refers to any damage resulting from 'an afront to the dignity and prestige of the injured State.'[682] In the cyber context, moral damage could result when an attacker that 'manipulates information posted on

[677] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid,Arts 42, 46. Tallinn Manual (2017), Ibid, Rule 27.

[678] Tallinn Manual (2017), 143.

[679] Factory at Chorzow judgement, 47.

[680] Tallinn Manual (2017), Ibid, 143–151.

[681] Ibid.

[682] Ibid.

a governmental website may undermine confidence in the government.' Furthermore, the damage needs to be caused by the wrongful act, which means it is not consequentially remote. However, in many cases, in cyber operations, the result could be remote. For example, some malware can be highly contagious, which means that it will spread to other systems and cyber infrastructures over time. It is worth noting if the injury caused to nationals or companies will qualify as an injury to the state.[683]

To illustrate, restitution means to return the situation as it was before the wrongful act. However, sometimes full restitution is impossible, and the situation can be only partially re-established. In these circumstances, the victim state could request compensation and satisfaction in addition to the restitution; for example, consider a distributed denial of service (DDoS) attack that hit the system. The damage incurred includes the time wasted and financial loss because of the recovery time. Therefore, the restitution could not be enough considering the unrecovered damage. As a result, the injured state could request compensation in addition to the restitution. Compensation is an amount of money to be paid to the injured state because of the damage resulting from the wrongful act, in case restitution is impossible or is not satisfactory. The need for satisfaction is explained by the Draft of Articles on state Responsibility as 'an acknowledgment of the breach, an expression of regret, a formal apology or other appropriate modality.'[684]

3.7.1. Due diligence

In the context of determining the responsibility of a state for an internationally wrongful act, the burden lies on the state to ensure its territory is not misused by any groups or individuals or that state could be found in violation of that duty. This means that the state has an obligation to prevent any harm being caused to other states that have been launched from its territory. This obligation is known as 'due diligence',

[683] Ibid.

[684] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Ibid, Art 37 (2).

though it could also be known as ‘obligation of vigilance’ or ‘the duty of prevention’. In the cyber context, the Group of Experts chose to use the term ‘due diligence’ because it does not compromise the ‘obligation to take material preventive steps to ensure that the State’s territory is not used in violation of this Rule.’[685] In Bergwik’s opinion, the Tallinn Manual 2.0 is “a great addition to the doctrine of due diligence in cyberspace. The International Group of Experts’ arguments are well-founded, and it greatly follows the case law and seems to be in line with the few existing statements about due diligence in cyberspace. Although Rule 6 is necessarily kept general, it is a start to shaping the due diligence principle in the field of cyberspace”.[686] However, there are still many issues that have not been settled by the Group of Experts, which will be illustrated below.

To illustrate the meaning of this principle, take the example of a hacker who has launched a cyber operation against state A by using cyber infrastructure located in state B. In this scenario, state B should take feasible measures to make sure its territory is not used illegally.[687] The acceptance of the obligation of due diligence in cyber space among states can be based on the acceptance of its sovereignty over its territory. However, the GGE in its 2013 report only used the phrasing that states ‘should’ do due diligence.[688] Moreover, the GGE has stated afterward in another report that “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”.[689] France has declared within the GGE report 2015 that “sovereignty over computer systems on the State’s territory creates a customary obligation of due diligence and that the duty means that the State should not knowingly allow its territory to be used for internationally wrongful acts using ICT”.[690] Furthermore, Väljataga has noted that “States agree that cyber due

[685] Tallinn Manual (2017), 32.

[686] Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, Ibid, 53.

[687] Ibid.

[688] UN GGE 2015 Report para. 20.

[689] UN GGE 2015 Report para. 13(c).

[690] Roguski, P, France’s Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I, Opinio Juris (24 September 2019), as cited in Bergwik,

diligence follows from cyber sovereignty, but that they "have not agreed on whether and how cyber due diligence can form the basis for state responsibility."[691]

The General Assembly in its 2001 session has declared that states should take all preventative measures to protect cyber space. It also stated that states should "ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies."[692] However, there are a few states who reject applying due diligence in cyber space. Their argument is based on the language of the GGE report. Because, in their view, the report used "should" rather than "must" in considering the due diligence.[693] Furthermore, Hankinson has noted that "not all States have readily accepted cyber due diligence as customary and because of this, there is a hesitation to "accord the rule *lex lata* status."[694] However, to develop a state practice or opinio juris, there is no requirement to get a complete consensus between all states. It is enough to have the practice or acceptance of most states. There is an interesting argument made by Bergwik. He affirmed the application of the due diligence principle on the cyber space, based on the application of this principle in environmental law.[695]

However, there is an argument about the required knowledge of the state to be violated regarding the due diligence principle. The required knowledge is the

---

M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, UPPSALA Universitet, Mater Thesis, 2020.

691 Väljataga, A, Tracing opinio juris in National Cyber Security Strategy Documents, NATO CCD COE, Tallinn, (2018), as cited in Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, UPPSALA Universitet,Ibid, 2020.

692 179 A/RES/55/63, Combating the criminal misuse of information technologies (4 December 2000), 2.

693 Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, UPPSALA Universitet, Master Thesis, 2020.

694 Hankinson, O, Due Diligence and the Gray Zones of International Cyberspace Laws, Michigan Journal of International Law, Volume 39 (2017), Available at: http://www.mjilonline.org/due-diligence-and-the-gray-zones-ofinternational-cyberspace-laws/#_ftn16. [Accessed: 08th June 2021].

695 Bergwik, M., Due Diligence in Cyberspace. An Assessment of Rule 6 in the Tallinn Manual 2.0.

actual knowledge of the harmful act. This view of the Tallinn Manual Group of Experts has been acknowledged by many authors, such as Schmitt, Jensen and Heinegg.[696] The Tallinn Manual acknowledges due diligence in Rule 6 by stating that 'A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.'[697] This rule includes two descriptions of the required effect. The cyber operation needs to be contrary to the law and have 'serious adverse consequences.'[698] The first requirement means that the cyber operation violates an international obligation owed to the other state, which means that this rule applies only when the act is considered an international wrongful act. To illustrate, consider state A spying on state B by using cyber infrastructure located in state C. In this case, state C has no obligation under the due diligence principle because, according to international law, espionage is not a wrongful act.[699]

Another example is if a private company publishes classified information about state A on a website hosted by state B. The latter has no obligation to remove this data, even though it has serious adverse consequences. Yet, it has no effect on any international obligations state B must observe.[700] The Group of Experts gave an example of serious adverse consequences which do not consist of physical damage, which is "a major impact on the economy."[701] Moreover, they illustrated that "physical damage to objects or injuries to individuals is not necessarily required."[702] In regard to minor adverse consequences, the mere effect on the state's interest such as a minor disturbance is not considered harm that constitutes a violation of the

[696] E Jensen, Cyber Sovereignty: A Way Ahead, Ibid, 298–299, V Heinegg, Territorial sovereignty and Neutrality in Cyberspace, 89 International Law Studies 123, 127 (2013), 137.

[697] Tallinn Manual (2017), 30.

[698] Ibid, 34.

[699] Ibid, 35.

[700] Ibid,, 36–38.

[701] Tallinn Manual(2017) 38.

[702] Ibid 25.

due diligence principle.[703] Furthermore, there is no requirement for physical damage. As a result, serious adverse consequences could be an economic impact or a disruption of an online banking system.[704] Bergwik has commented that "cyberspace is somewhat concerned with transboundary harm. The harm is, of course, rather different, but the aim is the same."[705] In the Trail Smelter Arbitration case, it was stated that it needed to be "of serious consequence", and the ICJ in Pulp Mills held that the conduct had to amount to "significant damage" for another State.[706] It also noted that "no State has the right to use or permit the use of its territory in such a manner as to cause injury … when the case is of serious consequence."[707] Moreover, regarding state practice, the Netherlands stated that it is "generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences."[708] They also held that "the precise threshold depends on the circumstances in each case, and that physical damage is not a requirement."[709] However, cyberattacks that target multiple sectors and cause "initial serious injuries", should invoke cyber-diligence obligations. That would protect the other networks from injury afterward.[710] Harm assessment in this context has been categorised by Liu in three ways: injury to persons or loss of life; physical damage or destruction of objects, loss of network

---

[703] Ibid; Trail Smelter Arbitration (United States v. Canada), [1938], International Arbitral Award) VOLUME III pp.1905-1982; Pulp Mills on the River Uruguay (Argentina v. Uruguay), [2010]

Judgment, I.C.J. Reports, p. 14

[704] Ibid.

[705] Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0,Ibid,43.

[706] Ibid, 44.

[707]Trail Smelter Arbitration (United States v. Canada), Ibid,1905-1965.

[708] Minister of Foreign Affairs, Letter to parliament on the international legal order in cyberspace + Appendix: International law in cyberspace (26 September 2019) p. 5; Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, Ibid,44.

[709] Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, Ibid, 44.

[710]

functionality and cyber-exploitations.[711] In the case of the first category, he stated, it is rare that the cyber-attacks result in loss of life. Therefore, he concluded that "A lower level of damage should also trigger cyber-diligence."[712] That takes the discussion to the second category, which is the loss of network functionality. Contrary to the first category, this one is the most accrued in the case of cyber-attack. Liu concluded, "once a cyberattack causes serious disruptions to a network's proper functioning, the cyberattack is then "destructive" and constitutes "serious injury."[713] This thesis agreed with that statement because it makes it easy to determine the harm required, and it is usually the result of the cyber operation. Moreover, this type of harm could happen gradually, not immediately, which leaves time for the territorial state to use its due-diligence obligation to stop the cyber operation and terminate the harm.

Furthermore, The Budapest Convention on Cybercrime defines system interference as "the serious hindering … of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."[714] The definition could be guidance in assessing the "destructive" criteria. Interestingly, the due diligence standards change according to "new scientific or technological knowledge [and] risks involved in the activity."[715] This statement indicates that the assessment of harm relies on how fast states could realise a cyber operation is taking place and predict the harm. This cannot be done without appropriate technologies and cyber tools. The last category of harm is cyber exploitations. It is defined as "an activity intended to clandestinely access and exploit a network's vulnerabilities without disturbing the network's operation."[716] One clear

[711] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 244-250.

[712] Ibid, 247.

[713] Ibid.

[714] European Convention on Cybercrime, art. 5 ; Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 248.

[715] Seabed Mining Advisory Opinion on Responsibility and Liability, [2011], the Seabed Disputes Chamber, 117.

[716] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 249.

example of this operation is intelligence gathering. This is one of the grey zones in cyber space because there is no clear answer if this type of harm is considered a "serious injury". That has been confirmed by the Committee on Offensive Information Warfare, which noted that "the distinction between cyberattack and cyber-exploitation may be very hard to draw from a technical standpoint and may lie primarily in the intent of the user."[717] In the thesis' view, this type of harm cannot be considered a "serious injury". This type of cyber activity is usually done without the state's knowledge, and the core of the due diligence is to require reasonable action that is within the state's capability. However, such a type of activity would not make the due diligence standard reasonable, rather it will render it impossible. Another cyber act which is considered below the threshold of due diligence is defacement. Oppenheim's International Law stated that "due diligence obligations do not extend to "suppress[ing] criticism of, or propaganda directed against, other States or governments on the part of private persons."[718] Therefore, the mere corruption of public web page or sending a political message does not rise to the required level.

There is a very controversial issue in the cyber context with regard to constituting 'serious adverse consequences', which is a cyber operation that involves botnets.[719] On this issue, the Group of Experts is divided into two groups. On the one hand, the majority was of the view that the due diligence principle would apply regardless of where the harm manifests.[720] On the other hand, the minority took the position that the operation will be treated as a composite armed attack as in self-defence. Therefore, the due diligence obligation will be assessed for each state

[717] Committee on Offensive Information Warfare, ch. 1.6. The Legal Framework Governing Cyberattack.

[718] Jennings, R., & Watts, A. Oppenheim's International Law, Ibid, 150-154

[719] A botnet is a 'a collection of internet-connected devices, which may include personal computers (PCs), servers, mobile devices and internet of things (IoT) devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system.' https://searchsecurity.techtarget.com/definition/botnet.

[720] Tallinn Manual (2017), 38–39t.

individually.[721] This disagreement among experts makes the “serious adverse consequences” a grey zone in the cyber study field.

Another significant requirement is that the action needs to be attributable to a state. Which, as discussed before, can also be the case when a non-state actor takes action on behalf and under the direction of a state.[722] The Group of Experts in Tallinn Manual noted that “when a non-State actor engages in conduct that affects a right of the target State, that is, the conduct would, if conducted by the territorial State, breach an obligation that State owes the target State.”[723] However, if a private company releases classified information against another state, even if there is a huge effect on the economy or other serious adverse consequences, it will not trigger the due diligence of the territorial state because this act does not affect any right of the targeted state.[724] Bangwik emphasised in this regard: “Since non-State actors cannot generally affect a right of a State, it has to be determined if the non-State cyber operation would breach an obligation that the territorial State owes the target State had the territorial State been the one conducting the cyber operation in question.”[725] Therefore, the territorial state is not responsible to prevent the non-state actor unless the state was the conductor or violated the targeted state’s right.[726] In contrast, the target of the wrongful act could be either a government or private infrastructure.[727] Moreover, this principle has been applied by the ICJ in the Corfu

[721] Ibid.

[722] Müllerson discusses this in detail: Rein Müllerson, Self-defence against Armed Attacks by Non-State Actors, [2019] 18(4) Chinese Journal of International Law,751–775, 765-774.

[723] Ibid.

[724] Ibid.

[725] Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, Ibid,43.

[726] This is also why Müllerson argues that the territorial state needs to give the victim state permission if it wants to use self-defence against a non-state actor in such cases in which the cyber-attack can be classified as use of force. See: Rein Müllerson, Self-defence against Armed Attacks by Non-State Actors, Ibid, Pages 751–77.

[727] Ibid, 35.

Channel case when it stated that 'it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[728]

Moreover, in some cases, the state may not be aware of cyber operations on its territory. However, based on the 'should have known' standard, this is not an excuse, which means the state should have known its territory was being misused as an obligation on the state.[729] Indeed, this was precisely the situation faced by the ICJ in the Corfu Channel case. The court adopted the 'must have known' standard to oblige Albania to have known about the mines in its territory that caused harm to the UK.[730] That standard is higher than the 'should have known' standard, which has been stated in the Tallinn Manual. Furthermore, Heinegg's view is in favour of the 'should have known' view if the cyber-attack 'has been launched from cyber infrastructure that is under exclusive government control and that is used only for non-commercial government purpose.'[731] Rid and Buchanan explain which steps are included in testing attribution, using Stuxnet as an example. They identify that there are various layers, including a technical layer, non-technical analyses, and information on the geopolitical context.[732] However, while there were some indicators where Stuxnet might have originated, it became apparent that it requires a high level of technical expertise.[733]

Liu has divided different classifications of knowledge into four categories, The first two which are the actual knowledge, and connivance are grouped in the subjective knowledge category. The other two, which are evidential knowledge and constructive knowledge, were grouped in the category of objective knowledge. To illustrate, Liu described subjective knowledge as "the highest degree of intent. A state either intended the cyberattack to cause serious injury, or endorsed the

[728] Corfu Channel Case, 22.

[729] Tallinn Manual (2017), 41.

[730] Corfu Channel Case, 22

[731] V Heinegg, Territorial sovereignty and Neutrality in Cyberspace, Ibid, 137.

[732] Thomas Rid & Ben Buchanan Attributing Cyber-attacks, (2015) 38:1-2Journal of Strategic Studies, 4-37, 21.

[733] Thomas Rid & Ben Buchanan , Attributing Cyber-attacks, Ibid22-25.

outcome."[734] Trapp emphasised that "requiring proof of subjective knowledge would effectively act as a bar to any finding of responsibility for a failure to prevent."[735] On the other side, constructive knowledge "should be presumed when a cyberattack implicates a State's exclusive governmental infrastructure."[736] Heinegg has described it as "Constructive knowledge is prima facie established if the infrastructure was under direct State control and used only for public purposes."[737] Liu has described this type of knowledge with the word "tempered". This type cannot be relied on because in some cases the attacker could "compromise" the server of the state or the hackers could use the "spoofing" tactic to frame the state.[738] This thesis agrees with this argument for the same reasons. The author sees in this an indication of a desperate demand for a more accurate method to be used to solve the attribution problem, which could only be done by technical experts, not lawyers.

In this regard, there is a view that indicates that there should be a resumptive constructive knowledge, which relies on the "reverse presumption juris" approach.[739] That means the territorial state has the burden of proof to deny such knowledge. However, this view cannot be a strong argument because it "conflicts with I.C.J. jurisprudence".[740] The ICJ, in many cases, like the Corfu Channel case and Pulp

---

[734] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, 4(2) The Indonesian Journal of International and Comparative Law 191-260 (Forthcoming), Monash University Faculty of Law Legal Studies Research Paper No. 2907662, (January 30, 2017), 233.

[735] Kimberley Trapp, State Responsibility for International Terrorism, 65, (2011). 68.

[736] Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in Proceedings of the 4th International Conference on Cyber Conflict 9-10, 15 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds, 2012)., 17; Benedikt Pirker, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, 205-06.

[737] Heinegg, Territorial sovereignty and Neutrality in Cyberspace, Ibid,151

[738] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 237.

[739] Daniel J Ryan et al., International Cyberlaw: A Normative Approach, (2011). 42 Geo. J. Int'l L. 1161, 1185

[740] Liu, Ian Yuying, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Ibid, 237.

Mills, has rejected the reversal of the burden of proof.[741] For example, in the Bosnian Genocide case, the ICJ held that a "State's obligation to prevent the occurrence of genocide is engaged at the instant that the State learns of, or should normally have learned of, the existence of a serious risk that genocide will be committed."[742] As mentioned previously in this section, in the cyber domain, flexible approaches and principles are required when assessing a cyber act because each involves other difficulties that must be considered. Therefore, for the aim of this thesis, the analysis should be to clarify such situations and make them easy to assess, not the contrary.

It is worth noting that the key to due diligence is for the state to have control over its cyber infrastructure.[743] However, there are two events in which the due diligence principle extends extraterritorially.[744] First, when the government has control outside its territory, like in the case of military occupation.[745] Second, if a governmental cyber infrastructure is located outside its territory, such as the cyber infrastructure in a diplomatic premise.[746] There are some special cases in the context of state duty of due diligence, such as the case of the existence of a transit state that plays a limited role in transiting data. The Group of Experts agrees that the transit state could be responsible if it has knowledge of the cyber operation and does not take any feasible measures to terminate it.[747] If the cyber operation was underway, but it fails to reach its target, the territorial state will not be in violation of the due diligence principle because no harm has been done to the target state.[748] However, if the cyber operation has not been launched, but the territorial state knows about the preparation of that attack, the latter state will be obliged by due diligence and must

[741] Corfu Channel, , 51 (Judge Winiarski), 65 (Judge Badawin Pasha), 127 (Judge ad hoc Ečer); Pulp Mills Case, Ibid, para. 164.

[742] Genocide Case, Ibid, 221-22 [431].

[743] Müllerson describes it as "unwilling or unable test": Rein Müllerson, Self-defence against Armed Attacks by Non-State Actors, Chinese Journal of International Law, Volume 18, Issue 4, December 2019, Pages 751–775, 765 et seq.

[744]Tallinn Manual (2017), See also Article by Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, (2011).36 Brook. J. Int'l L.

[745] Tallinn Manual (2017),para 9,33

[746] Ibid.33,34,35

[747] Ibid.

[748] Ibid.

take feasible measures to prevent the operation from being launched.[749] In this regard, Schmitt has a very logical explanation, which is that 'It would be peculiar if international law allowed victim states to respond to ongoing harmful actions from another state's territory (a piercing of its sovereignty), but imposed no ex ante obligation on the latter to prevent them in the first place.'[750] This comparison is very useful in this regard and means that the duty to prevent is more required than the duty to act in response. This is because acting as a response is inevitable to protect the state from harm, but acting before the harmful cyber operation has been launched to make sure the state's territory is not used in any illegal manner is an instance of correct due diligence. In other words, the right to respond could be a mirror of the obligation to prevent.

One last point in this context is the obligation of the state to take preventive measures. In this regard, the Group of Experts is of two minds. The first is to reject that obligation for the state because it will be a heavy burden on the state - it is not predictable and therefore affects the condition of 'state knowledge'. In contrast, the second view is that states should take feasible preventive measures that are appropriate to the potential harm, such as adopting regulations to oblige private companies to report to the government immediately when there is any threat.[751]

Not only the Tallinn Manual has divided views in this regard. On one hand, there is Schmitt's view, which indicates that "there seems to be an evolving consensus amid scholars and State legal advisers that there is no obligation of States to monitor cyber activities on their territory or to prevent the wrongful use of their cyber infrastructure."[752] The International Group of Experts concluded that the due diligence principle does not include an obligation to prevent, and therefore there is no obligation for states to monitor cyber activities on their territory.[753] On the other hand, Bannelier-Christakis concluded opposingly, that due diligence does imply "not

[749] Ibid.

[750] M Schmitt, The Law of Cyber Warfare, ibid, 277.

[751] Tallinn Manual (2017), 46.

[752] Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, (2015), 125 Yale L.J. F. 68, 75.

[753] Tallinn Manual (2017), 42.

only an obligation to react but also to prevent".[754] Furthermore, in the Alabama case, the Tribunal found that "[t]he British government failed to use due diligence in the performance of its neutral obligations; and especially that it omitted, notwithstanding the warnings and official representations made by the diplomatic agents."[755] In favour of this view, the ICJ, in the Corfu Channel case, further held that "nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania."[756] Moreover, in Armed Activities on the Territory of the Congo, the ICJ stated that Uganda was responsible "for any lack of vigilance preventing violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account".[757]

Stockburger argues that a preventive feature should be included in the due diligence obligation.[758] Additionally, Sklerov has argued that: "States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders."[759] Interestingly, the Tallinn Manual does not require states to adopt legislation in regard to preventing its territory from being used

---

[754] Bannelier-Christakis, K, Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, (2014) ,14 Baltic Yearbook of International Law, 8.

[755] Alabama claims of the United States of America against Great Britain, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Volume XXIX, pp. 125-134,130.

[756] Corfu Channel Case, 23.

[757] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, ICJ Reports 2005, para. 179, 168.

[758] Stockburger, Peter, From grey zone to customary international law: How adopting the precautionary principle may help crystallize the due diligence principle in cyberspace. . (2018), 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, CYCON, 245-262.

[759] Matthew Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defences against States Who Neglect Their Duty to Prevent', (2009), Military Law Review 201, 1.

illegally and complying with the due diligence rule.[760] However, the deterrence would be greater if states enacted such legislation targeting the cyber realm precisely. This is because many of the states preclude their responsibility for a wrongful cyber act by attributing the act to an individual, however, if the state remembers its obligation to prevent, it is likely to have second thoughts about that.[761] For this reason, the thesis agrees with the side that includes an obligation to prevent in the due diligence principle.

From this section, we can conclude that in the cyber realm, the matter of attribution constitutes a barrier to determining responsibility.[762] What makes the attribution more difficult in the cyber realm is the requirement to take many elements into account to decide the source of the attack: who has pressed the button and which particular jurisdiction has the action in question fallen within.[763] Moreover, it needs to be determined if the perpetrator is a state, an individual, or a terrorist group. Even though states may identify all of these elements, in many cases they will keep it classified from the public. In the absence of a set of lucid customary international rules or a state practice that identifies the required level of attribution to determine the state responsibility, the Group of Experts leaves that issue for the states to agree between each other to set specific practices or rules.[764] The author's view in this regard is similar to Banks' description of the Tallinn Manual when discussing state responsibility for cyber operations; that is, 'It fails to provide prescriptive norms that will help deter malicious cyber operation.'[765]

---

[760] Ibid.

[761] Dinniss, Cyber Warfare and the Laws of War, Ibid, 100.

[762] Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, (2011), 36 Brook. J. Int'l L. , 1166.

[763] Scott J Shackelford, and Richard B Andres. 'State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem.' Ibid, 985; Dinniss,. Cyber Warfare and the Laws of War, Ibid, 99-102.

[764] Tallinn Manual (2017),80.

[765] W Banks, State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0,, ibid, 1495.

3.8 Conclusion

This chapter demonstrated that cyber-attacks which are not considered international wrongful acts still trigger state responsibility – that means countermeasures come into play. It is worth to mention that countermeasures are not available against alleged breaches of the law of armed conflict during a conflict. They are only available in peacetime. It was very significant to look at state responsibility in this chapter because offensive cyber operations may give rise to state responsibility if they are unlawful, even if they do not rise to the level of a use of force or an armed attack. Additionally, the victim of an internationally unlawful act (of any kind) may attempt to preclude the unlawfulness of a cyber response using the preclusions set out here. This chapter's aim was to get a full picture of the relevant international law principles which can be invoked when analysing cyber operations. Consequently, these principles will be applied in the next chapter to some selected cyber operations incidents.

A principle related to non-intervention is cyber sovereignty. This chapter recognised cyber sovereignty and offered proof of its existence. There is thus clearly ground for state practice in favour of recognising sovereignty of cyberspace, where there will be obligations corresponding to the right of sovereignty. These include such obligations as the responsibility to protect and monitor the state's territory against any unlawful cyber activities against another state.

The violation of any of these principles is a wrongful act that leads to a violation of state responsibility. Yet, it may be difficult to prove this in the cyber realm due to the issue of attribution. Therefore, this chapter discussed state responsibility and attribution. It has shown that state responsibility covers all wrongful acts that are related to cyber means, even if each individual one is not considered a cyber operation in itself. Moreover, contrary to the requirements that the act must amount to the use of force, physical damage or injury is not required for applying the state responsibility rules. The legal consequences for wrongful acts demand that the state responsible for the injury or harm needs to provide reparation to correct the situation. If this is not possible, there is an option for compensation. Furthermore, states have an obligation to act even before the cyber wrongful act has been achieved. This is a

due diligence obligation to ensure that its territory or any cyber infrastructure under its control is not used for launching any harmful cyber operation. Even though there was some controversy regarding the required knowledge of the state, for the aim of this thesis, the author agrees with the 'should have known' standard, which is a flexible standard for determining the state's knowledge of a harmful cyber act. Finally, the attribution for a cyber operation is still a very controversial matter due to the technical issues involved; even though some legal standards have been proposed, uncertainty in identifying the cyber operation's origin still exists. For that reason, the thesis proposes that experts in technology collaborate with legal experts in the area of cyber operations to solve the issue of attribution.

CHAPTER 4: SKETCHING CONTOURS OF MAJOR KNOWN CYBER OPERATIONS

4.1. Introduction

As per a report by the Centre for Strategic and International Studies, cyberattacks have increased since 2006.[766] This is particularly worrying for many small nations and emerging economies because they depend on the internet for governmental functions, defence, banking and businesses.[767] While individuals or groups who seek fame or profit may take up hacking, cyberwarfare is much more serious and the damage it causes could be considered equal to that of a nuclear attack. Nations such as: the United States of America, Russia, China, Pakistan, and others, are often accused of running cyberattacks with sustained Distributed Denial of Service (DDoS) attacks against nations who they consider enemies.[768] As this

[766] CSIS, 'Significant Cyber Incidents' (Center for Strategic and International Studies, 2019) <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity> accessed 14 May 2019.

[767] ibid para 2.

[768] ibid para 3.

chapter will show, it is difficult to blame the government of a country for attacks that originate within its territory.[769] Even if a few computers are traced to the attacking nation's network or to their Internet Protocols (IPs), it is often not enough evidence that the government was involved in the attack.[770] Furthermore, one could argue, there is another issue, which is the definition of force as per the United Nations' charter.[771] Definitions drafted many decades ago, such as the Charter, arguably understand force as the use of the military, and as such, the attack should kill or injure people and destroy infrastructure.[772] None of the cyberattacks such as Stuxnet, DNS attack or the Estonia attack have shown any use of the conventional definition of force. However, there are some other interpretations of the use of force which hold that Article 2 (4) can be understood to include cyber-attacks as a use of force. While some organisations like NATO, or the European Union have laws or policies, individual nations are free to accept or reject them.[773] Even if attacking nations accept the laws, they can carry out clandestine attacks hidden from external legal purview.[774] In such a scenario, the Haataja recommendation is for nations to harden their security, draft laws that punish any internal hacker, and seek cooperation among other nations to adhere to the laws.[775] Therefore, this chapter will investigate four different cyber-attacks and apply a legal analysis of these attacks. Moreover, it will examine the actus reus of the attack to determine if it can be considered a use of force or intervention, how it violates state sovereignty, and to establish if and when the attack gives rise to the right of self-defence. Furthermore, this chapter explores the international implications, such as the allowing of countermeasures. All these will be explored from the perspective of major authors. Simultaneously, this chapter will serve the aim and objective of this thesis by

[769] J Lewis, 'Cyber-attacks Explained' Centre for Strategic and International Studies (2007), 1-2.

[770] Rowe Neil, 'The attribution of cyber warfare' (Routledge, 2015, 75).

[771] Ibid.

[772] Ibid 80.

[773] S Haataja, 'The 2007 cyber-attacks against Estonia and international law on the use of force:
an informational approach' Law Innovation and Technology (2017), 9 2, 159.

[774] ibid 182.

[775] ibid 184.

showing that applying existing paradigms to those attacks does not give a conclusive answer to the ability of applying *jus ad bellum* to the cyber-attacks. Also, it will help Saudi Arabia to determine its policy on reacting to cyber operations based on other states practice in the cyber realm.

The chapter examines a few well-known cyber-attack cases from a legal point of view. The incidents examined are the Estonia DDoS attacks, the Stuxnet Malware attack, and the Aramco hacking of the refineries and oil production centres. These cases are worth studying because they illustrate the technical difficulties of attribution of malware in cyber-attacks, which lead to difficulties in determining international responsibility.[776] Moreover, they show how difficult it is to use the right of self-defence since the actor of the cyber-attack remains anonymous. Furthermore, all the cases show a different method of technology and a distinguishable scenario. Finally, the point is to show the variety of cyber-attack around the world and suggest possible ways for international law to deal with each one individually. For instance, the DDoS attack against Estonia was the first DDoS attack in the world, as well as the first 'cyber war'. It was a massive attack and had a huge impact on Estonian infrastructure.[777] This prompted a wake-up call for governments all over the world to review their cyber vulnerabilities and polices.[778] The 2007 attack has been examined by many scholars in the context of jus ad bellum.[779]

The Stuxnet virus as well is a very sophisticated malware. The target of this attack was Iran, which is part of the author's case study. The most significant aspect of the attack is that it resulted in kinetic damage, which begs the need to assess the attack based on the use of force rules.[780] The DNS attack has been chosen to be studied in this thesis because it is a very different form of cyber-attack that involved hacking an email. Moreover, the legal studies about this case are limited. As a result,

[776] J Jason, Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law. (2017) PhD thesis University of Glasgow 18.

[777] A Russell, 'Cyber Blockades' (Georgetown University Press, 2014), 69.

[778] Ibid, 70.

[779] Such as Roscini, Schmitt and Haataja.

[780] M. Schmitt, Cyber Operations and the Jud Ad Bellum Revisited, 56 Vill. L. Rev. 569 (2011).

it needs to be studied to understand the ability of applying jus ad bellum to numerous cyber-attacks.

The last case to be studied in this chapter will be the Aramco attack. The Aramco attack is undoubtedly at the heart of this thesis' scope. This is because the victim is a company based in Saudi Arabian territory; moreover, it is also half owned by the Saudi government. The similarity of these attacks is that they were all allegedly organised and supported by nation states. The Estonia DDoS attacked was run by Russia, though this was never legally proven, which will be shown in section 2.2 which analyses the legal aspects of the attack.[781] Stuxnet Malware, on the other hand, was allegedly developed by the USA and Israel. This worm was directed at Iran's nuclear operations, and the worm reportedly crashed the centrifuges, destroying them and risking a potential nuclear disaster.[782] The Aramco hacking was allegedly run by Iran and directed at oil fields, causing several rigs to malfunction and stop working.[783] The common element in all these attacks is the relative ease with which a few hackers managed to penetrate secure systems, making them crash, and the lack of legal framework to bring the alleged hackers to justice. The next section will discuss the legal aspects of the Estonian DDoS attack.

4.2. Estonia DDoS

Estonia is a small country in Northern Europe and a former satellite country of Soviet Russia. Estonia was occupied by Soviet forces after World War II. Thousands of Russian citizens were asked to settle in Estonia to create a large native Russian population. The country consequently suffered from low economic growth and

[781] A Russell, 'Cyber Blockades' (Georgetown University Press, 2014), 35.

[782] A Shubert, 'Cyber warfare: A different way to attack Iran's reactors' (CNN.com, 8 November
2011) <http://www.cnn.com/2011/11/08/tech/iran-stuxnet/> (accessed 6 May 2019).

[783] P Paganini, 'Iran Suspected for the Attack on the Saudi Aramco' (SecurityAffairs.com, 20 August 2012). <www.securityaffairs.co/wordpress/8300/malware/iran-suspected-for-the-attack-
on-thesaudi-aramco.html> (accessed 6 May 2019).

suppression from the Russians. After 1987, Estonia dissociated from Russia and became an independent country. It prospered under the support of the USA and NATO forces. However, Russia coveting the country gave it easy access to Europe.[784]

Estonia modernised, and invested in internet technology, rapidly adopting complex systems to manage the government services and private enterprises.[785] Estonia invested and developed extensive Information and Communications Technology (ICT) structure with internet enabled computer networks covering almost all government, business, and personal activities.[786]

Estonia has developed a system what is called “E-Estonia” in 1997. E-Estonia provides all government and healthcare services online. Today, it is used by 95% of the Estonian population[787], and it also provides tax claim service and the possibility of voting in elections.[788] Estonia has a new type of residential card called “Digital Residence” which provides a wide range of services for foreign workers and foreign companies invested in the country.[789] While the world has seen a large number of small and large cyberattacks, the cyberattack on Estonia was a show of overwhelming force. Estonia faced a severe attack from an unknown attacker, who was allegedly based in Russia. Although the Russian government vehemently denied supporting the attack, the operation is deemed an invasion and an attack on

---

[784] Taagepera Rein, 'Estonia: Return to Independence' (Boulder, Colo.: Westview Press, 1993)
36.

[785] R Kertu ‘Cyber War I: Estonia Attacked from Russia’ (2008) 9 1-2, European Affairs, 6

[786] ibid 8.

[787] S Bartłomiej, ‘The data embassy under public international law’ International & Comparative
Law Quarterly (2019), 68 1, 226.

[788] S Haataja, ‘The 2007 cyber-attacks against Estonia and international law on the use of force:
an informational approach’ Law Innovation and Technology (2017), 9 2,160.

[789] Ibid.

the sovereignty of the country. Allegedly this attack was state-sponsored by Russian.[790]

4.2.1. The 2007 DDoS: technical details of the attack

The nation came under a massive cyberattack from April to May 2007, crippling the network and making the information systems unusable.[791] This attack, being the first of its kind, was thus described as a "Cyber War".[792] The modus operandi of the attack was DDoS (Distributed Denial of Service). DDoS entails sending a large flood of connection requests and spam with malware to the victims' servers. Unable to cope with the huge service requests, the servers crash, allowing hackers to gain access to the server and internal networks, where they steal and delete information, or deface sites, thereby bringing the IT systems of the victim country to a standstill.[793] Russia is accused of carrying out this attack on Estonia because the Estonian government decided to move a bronze statue of a Russian soldier from the city centre to a cemetery, an action Russia considered an affront.[794] Consequently, there was a protest staged in front of the Estonian Embassy in Moscow and a clash between the Russian minority and Estonian police.[795] All that happened before the massive cyber-attack on the Estonian information entity. An

---

[790] Taagepera Rein, 'Estonia: Return to Independence' (Boulder, Colo.: Westview Press, 1993)
49.

[791] A Bright, 'Estonia accuses Russia of 'cyberattack' The Christian Monitor 1 November 2016)
<http://www.csmonitor.com/2007/0517/p99s01-duts.html> accessed 6 May 2019.

[792] Toomas Hendrik Ilves, 'Address by the President of Estonia' (67th Session of the United Nations General Assembly, New York, 26 September 2012) https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-unitednations-general-assembly-un-headquarters-new-york-september-2012/ (accessed 17 May 2019).

[793] J Lewis, 'Cyber-attacks Explained' ,Ibid, 1-2.

[794] ibid 48.

[795] K Andrzej, 'Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan' European Scientific Journal (2014), 10.7, 238.

editor of international affairs at the Estonian daily newspaper - Estonia Tuuli Aug, described the consequences of the attack: “although cyberattacks leave no bomb holes in the ground, the economic losses are real.”[796] Estonia suffered millions in losses and downgraded performance of its systems. One of the Estonian banks' losses was estimated to around $1 million in damages.[797] The total loses of the economy were estimated between $27 - 40 million.[798] The Estonian Minister of Foreign Affairs described the impact of the attack on the Estonian population as “virtual, psychological and real – all at the same time.”[799]

Different methods were used for the DDoS attacks against Estonia, and some of them included ping floods[800] and botnets[801] to flood the servers with spam.[802] Although it was clear that a single individual could not have carried out such a

---

[796] M Valentinas, Estonia: Attacks Seen As First Case Of 'Cyberwar' (30 May 2007), <https://www.rferl.org/a/1076805.html > accessed 16 May 2019.

[797] Ibid.

[798] Sheng Li, ‘When Does Internet Denial Trigger the Right of Armed Self-Defence?’ ,38 Yale Journal of International Law (2013) 179, 200.

[799] Declaration of the Minister of Foreign Affairs of the Republic of Estonia’ (Republic of Estonia
Government,1 May 2007) <https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia> (accessed 16 May 2019).

[800] “A ping flood is a denial-of-service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to
normal traffic.” What is a Ping (ICMP) flood attack? , retrieved from <https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ > accessed 17 May 2019.

[801] “The term bot is short for robot. Criminals distribute malware (malicious software) that can turn your computer into a bot, also called a zombie. When this occurs, your computer can perform automated tasks over the Internet without your knowledge.” What is a botnet?, retrieved
from < https://www.microsoft.com/en-us/security/pc-security/botnet.aspx > accessed 17 May 2019.

[802] The Economist, ‘Marching off to cyberwar’ The Economist 4 December 2008 <www.economist.com/node/ 12673385> (accessed 15 November 2016).

massive attack, and only a large organisation with sufficient resources could launch such an attack,[803] only one person was found guilty of launching the attacks, and he was fined about $1640.[804] The Russian authorities denied their role in the attacks, and the Russian Supreme Court denied any investigation and cooperation in the matter.[805] Experts in the field presumed that such an attack was too sophisticated and beyond the capability of one or two individuals.[806] They said that it would require the active assistance and participation of a large telephone network and a government apparatus to support the attacks.[807] As per the UN Charter, states are prevented from using force against another state, except for the use of self-defence. Article 51 states that nothing can prevent the right to individual or collective self-defence by the state or states when an armed attack is launched by another state.[808] The next section will provide a detailed legal analysis of the attack and ultimately argue for the need to apply the use of force rules to the Estonian cyber-attack. The section will also take the sovereignty principle into account and explore Estonia's jurisdiction. The findings of this analysis will ultimately help Saudi Arabia to plan its own method of protecting and defending its cyber capacity according to the applicable international rules.

---

[803] Ibid.

[804] Ibid.

[805] J Caso, 'The Rules of Engagement for Cyber-Warfare and the Tallinn Manual: A Case Study'
The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and
Intelligent Systems June 4-7, 2014, Hong Kong, China. 252.

[806] ibid 253.

[807] ibid 253.

[808] United Nations, 'Chapter VII — Action with respect to Threats to the Peace, Breaches of the
Peace, and Acts of Aggression' (Repertory of Practice of United Nations Organs, 23 August 2016) <http://legal.un.org/repertory/art51.shtml> (accessed 6 May 2019)

4.2.2. Legal aspects of the Estonian Attack and a discussion of international unlawfulness

While the cyber-attack against Estonia is well documented, the legal aspects and implications that arose thereafter were met with controversy.[809] For the attacks to be described as an act of war, it had to be proven that force was used, and one of the major problems was defining what constituted 'force'.[810] Conventional definitions of force include the use of the military, ammunitions, and other weapons. In the Estonian case, none of these weapons were used – even worse, the attacker was never identified. Merely suspicions pointed towards Russia.[811] Despite the fact that one Russian government computer was used, the Russians claimed that the computer itself was hacked.

Another problem was that Estonia was part of NATO, and the rules required that all members should take a collective action when Russia attacked one of the member states. However, NATO could not take any action since Russia had carefully hidden its tracks.[812] NATO subsequently formed the Cyber Defence Committee that is responsible to consult, control, and command resources against such cyber-attacks for other states. NATO further commissioned the drafting of the Tallinn Manual that is supposed to collect and interpret the international law

---

[809] "A blockade is a belligerent operation to prevent vessels and/or aircraft of all nations, enemy
and neutral (Neutrality in Naval Warfare), from entering or exiting specified ports, airports, or coastal areas belonging to, occupied by, or under the control of an enemy nation." Max Planck
Encyclopedia of Public International Law [MPEPIL] retrieved from
<https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e252>
accessed 17 May 2019.

[810] S Haataja, 'The 2007 cyber-attacks against Estonia and international law on the use of force:
an informational approach' Law Innovation and Technology (2017), 9 2, 165.

[811] Ibid.

[812] NATO. 'Cyber Defence' North Atlantic Treaty Organization (16 July 2018)
<https://www.nato.int/cps/en/natohq/topics_78170.htm> (accessed 6 May 2019).

applicable to cyber-attacks.[813] The opinion is that too many gaps exist in international law and that there is an ontologically constraint to the conceptualisation of damage, violence, and some form of material damage where death of people or destruction of property should occur.[814] In 2007, many assets and networks were not recognised as legal entities, though the organisations that managed these assets were legal entities.[815] Therefore, the recognition that a crime has occurred was the first obstacle, and then came the issue of finding the people responsible for the attacks.[816] To put it in simple terms, if a gunman uses public transport to reach a place and kills people there, then the transport firm cannot be held responsible for the crime. In this way, telecommunication firms that provide the network connectivity cannot be held responsible for cyber-attacks.[817] Even if the attack was traced to a specific computer, the computer owner can claim that a remote hacker used his computer to launch the attacks.[818]

As shown in the previous chapter, international law principles are applicable in cyberspace, though not all international community members accept it. Some assert that the existing laws cannot be applied to cyberspace, and claim they need to be modified to make them applicable and adaptable to the new technology.[819] Nevertheless, cyberspace is not a law-free zone where any kind of behaviour is acceptable. Cyber operations and cyber-attacks can, in certain circumstances, be considered as a use of force as per Article 2 (4) of the UN Charter and Customary International Law.[820] However, the examiner must find out if there was a direct

[813] M Schmitt, Tallinn Manual on the International Law Applicable to Cyber Operations (Cambridge University Press, 2013), 36.

[814] S Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defence?' (2013) 38 Yale
Journal of International Law 179, 202.

[815] Ibid.

[816] S Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defence?' Ibid, 202.

[817] Ibid 203.

[818] Ibid.

[819] H Koh, 'Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012' (2012) Harvard International Law Journal 54.

[820] Ibid 5.

physical injury, death, damage to property from the use of cyber-weapons.[821] Certain events can be considered as acts of war. For example, deliberately causing a nuclear meltdown, opening a dam to drown people, hacking into aeroplanes to make them crash, disabling train and shop controls so that they crash, and other such incidents.[822] The dispute about possible legal actions against the Estonian attacks emerges due to two standpoints.[823] As discussed previously regarding cyber space sovereignty, some argue all states need to accept and agree that cyberspace is an area where nations can exert their sovereignty by means of effective control doctrine.[824] This doctrine is based on the ruling in the Nicaragua case which recognised that a country is "in complete control" of, e.g., a mercenary group if the actors are completely dependent on the state.[825] The alternative position argues that cyberspace is considered a common heritage of mankind (like the deep seabed), so no one state can claim to have jurisdiction over it.[826] Nevertheless, the author would like to reiterate her argument from earlier, and underline that she follows the majority of the Group of Experts, and states like the US, and believes that the cyberspace belongs to the cyber territory of a state and that the state consequently has jurisdiction over it.

One of the problems of technological advancement is that hackers can cross into the domain and networks of other countries - since the net is seamless, they can mask their operations and activities, wreak destruction, and then disappear unscathed.[827] The entry point and origin remain hidden and masked with other IPs, and while the hardware for the internet is provided from somewhere, the information

[821] Ibid 6.

[822] Ibid.

[823] S Scott, 'From nuclear war to net war: analogizing cyber-attacks in international law. Berkeley Journal of International Law (2009) 27 1, 193.

[824] Ibid 193.

[825] Ibid 233.

[826] Ibid 211.

[827] J Thomson, 'State Sovereignty in International Relations: Bridging the Gap between Theory
and Empirical Research' International Studies Quarterly (1995) 39, 217.

transmitted is not under the control of the provider.[828] As seen in the Estonia attack, Russia denied being involved in the attack, though it conceded that some rogue hackers might have used their infrastructure to attack Estonia. The result is that when a crime is committed, proof of the crime is available; however, proof linking the crime to the organiser is not available.[829] This happened in the Estonia case.

However, the final point here is that Estonia has sovereignty over its cyber space territory. Its cyber space territory, just like its physical territory, is protected by international law principles. Therefore, the DDoS attack is a violating the cyber sovereignty of Estonia. On the question of whether the cyber-attack against Estonia is considered a use of force under international law, there are many academic authors who took a position in favour of this argument and others that did not. Buchan notes that the cyber-attack against Estonia is not a use of force because no physical damage has accrued, but he agreed it violated the principles of non-intervention and sovereignty.[830] Michael Gervais maintained the same position as Buchan and based his argument on the lack of severity under the Tallinn Manual criteria.[831] Tsagourias also noted that the attack is a violation of the principle of intervention, but not a use of force.[832] He stated that, "their severity (in view of the duration and scope of the attack) was limited, and their harmful effect was limited and containable; the invasiveness of the attack was superficial and whereas there were some direct consequences, other consequences– economic or financial – were rather remote."[833] A similar position is taken by Andres Henriksen when he added that the attack does not give Estonia the right to self-defence.[834] On the other hand,

---

[828] Ibid 218.

[829] Ibid 219.

[830] S Haataja, 'The 2007 cyber-attacks against Estonia and international law on the use of force:

an informational approach' Ibid, 171.

[831] Ibid.

[832] Ibid.

[833] Ibid. 172.

[834] Anders Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015) 84 Nordic

Journal of International Law 323, 327.

Schmitt's view on the attack on Estonia indicates that it constituted a use of force because it affects the Estonian social life and has an impact on the government services and Estonian economy.[835] Schmitt's criteria for analysis of cyberattacks is one of the most significant measurements for any cyber-attack based on international law rules. It uses eight points to evaluate a cyberattack.[836]

The criteria of severity refer to the extent of destruction, scope, severity, and intensity of the attack. E.g., defacing of a websites is not a use of force, whereas hacking a government, bank or defence websites is a use of force.[837] In the Estonia attack, all these attacks took place, and violated Article 2 (4) of the UN Charter of 1945.[838] The second criterion is imminency, which refers to the speed of attack and if there was time available for negotiation. The victim state should have irrefutable proof that the attacking state was involved.[839] In the Estonia cyber-attack case, the first wave of attacks occurred on 27 April 2007 and lasted until 8 May 2007. While Russian hackers and chat rooms were involved, there was no proof that the Russian state was involved or led the attack. Hence, Estonia could not approach NATO to invoke Art 5 and get collective defence support against Russia.[840] The directness refers to unexpected consequences and if the result of the attack led to death and

---

[835] S Haataja, 'The 2007 cyber-attacks against Estonia and international law on the use of force:
an informational approach' ,Ibid173.

[836] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework' , Ibid, 1998.

[837] Ibid.

[838] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective' (Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2008) https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePers pective.pdf (accessed 8 May 2019).

[839] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework' Columbia Journal of Transnational Law (1999) 37, 1998.

[840] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective' Ibid

injuries.[841] The attack on Estonia did not cause any deaths and injury. Estonia was unable to prove that a specific instance of an attack caused the failure of banks and other websites. Hence, the attacks cannot be legally considered as an act of war.[842] Regarding the invasiveness, there should be a movement of troops into the victim's territory, with the intention to overthrow the government.[843] In Estonia's case, there was no troop movement, and there was no effort to overthrow the government. Hence, the government could not consider the attack as an act of war.[844] The criterion of measurability requires the state to clearly state in economic terms the value of assets damaged beyond salvage.[845] In the case of Estonia, such metrics were not possible since the systems such as banks and the government were intact, and only their operational ability was degraded, but not destroyed. Hence, Estonia could not claim the attack as an act of war.[846]

According to the pre-emptive legitimacy criterion, a state can use computer networks as counter-defensive attacks, and self-defence is allowed when a credible threat is established.[847] In the case of Estonia, the government did not have

---

[841] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework' Columbia Journal of Transnational Law (1999) 37, 1992.

[842] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective', Ibid
pective.pdf (accessed 8 May 2019).

[843] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework', Ibid, 1992.

[844] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective' , Ibid

[845] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework' , Ibid, 1993.

[846] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective', Ibid.

[847] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on
a Normative Framework', Ibid, 1994.

irrefutable evidence that the Russian government was involved. Hence, it could not attack Russian networks.[848] If an attack from State R on State E has occurred and if State R has not sponsored the attacks, then State E can still ask State R to take steps to stop or prevent such attacks in the future. However, remote attackers can launch attacks from State R, and the state cannot be held responsible for it, as per the responsibility principle.[849] This process happened in Estonia and the Russian government admitted that some of its computers were used, but the government was not involved. The claim diluted the ability of Estonia to act against Russia.[850] There is an interesting description of the attack given by Sheng Li, who deemed it an "informational blockage". [851] It means the attack affects the well-being of Estonia and as a result, it should be considered as a use of force. Both sides of view are still under the umbrella of international law. Even though most of the authors classed the attack below the threshold of the use of force, they consider it a breach of the non-intervention principle. Therefore, it will allow the victim state to use countermeasures against the attacker.

Another criterion that has been suggested to analyse the Estonia attack is derived from an informational approach as proposed by Haataja[852] who argued that this type of harm would amount to the use of force.[853] In his opinion, it is "Virtually uncontested" a use of force if the resulting harm causes physical damage to entities

[848] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective' ,Ibid.

[849] Schmitt M 'Computer Network Attack and the Use of Force in International Law: Thoughts on

a Normative Framework' , Ibid,, 1995.

[850] R Ottis 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective', Ibid.

[851] Ibid.

[852] Haataja S, 'The 2007 cyber-attacks against Estonia and international law on the use of force:

an informational approach' , Ibid, 174.

[853] Ibid.

or injuries to persons.[854] This informational approach relied on three elements, informational ethics, state entity and informational violence.[855]

Floridi argued in a similar way when he described the ethics beyond the material environment as a "bio-centric".[856] Moreover, every state has a right to keep its information system protected as a part of its entity. Therefore, any cyber-attack that occurs against this entity will amount to violence and consequently, it will prove harmful for the state, thus, falling within the use of force area.[857] Rindall Dipert describes this cyber harm as "impairment or degradation" of the system function.[858] Such attacks are directed to piercing the morale of the victims by defacing sites, placing doctored images on the site, and spreading propaganda.[859] This is a type of informational warfare where the attacker focuses on spreading fear and unrest through posting messages and information.[860] Technology has allowed hackers to create informational warfare at a fraction of the cost needed for a military attack. The problem with such cyberattacks is that the fragility of social order is broken; they can create panic, uncertainty, destroy trust and confidence in the government and lead to mob mentality.[861]

There is another approach has been illustrated in the previous chapter when determining the use of force and the existence of an armed attack, which is the target-based approach. This approach considers any act targeting a national critical infrastructure based on its severity as a use of force or armed attack. In the Estonian context, Estonia has adopted the definition the European Union suggested which

---

[854] Roscini, Cyber Operations and the Use of Force in International Law , Ibid, 53.

[855] L Fluridi, Information: A very short introduction, Oxford University Press, (2010), 111.

[856] Ibid.

[857] Haataja S, 'The 2007 cyber-attacks against Estonia and international law on the use of force:
an informational approach' , Ibid, 175-181.

[858] R Dipert, 'The Ethics of Cyberwarfare', (2010), 9 Journal of Military Ethics 384, 386.

[859]A Jenik, 'Cyberwar in Estonia and the Middle East' Network Security (April 2009), 5

[860] ibid 6.

[861] S Beidlemen 'Defining and deterring cyber war' Strategy Research Project, U.S. Army War
College (2009), 16.

defines “critical infrastructure” as “an asset, system or part thereof, which is essential for the maintenance of vital societal functions, and the health, safety, security, economic or social well-being of people, and whose disruption or destruction would have a significant impact in a Member State as a result of the failure to maintain those functions.”[862] In the case of the DDoS attack, the state suffered from a massive denial-of-service attack which paralysed the state capability from providing services for people. Therefore, this cyber operation targeted a national critical infrastructure, which has a severe impact on their function. Based on the target-based approach, the DDoS attack would be considered a use of force. Moreover, it will amount to an armed attack because it is “directed against a State’s critical infrastructure, provided the cyber-attack had the potential to severely cripple a State’s ability to carry out and ensure the conducting of essential State functions.”[863] The author agrees with using the national critical infrastructure definition in assessing the armed attack, as illustrated in the previous Chapter.[864]

To reiterate, there are several possibilities to evaluate if an armed attack occurred. One could apply the “scale and effect” criterion, as suggested by the Tallinn Manual.[865] In this case, the intensity of the cyber operation against Estonia meets the required scale, as “Estonia's citizens enjoyed Wi-Fi coverage in 95% of the country; 99% of them used the Internet for banking and 86% completed their taxes online.”[866]Also, the consequences were huge and affected Estonia's financial and telecom sector and resulted in financial loss and economic collapse, as mentioned previously in the description of the attack section.

Hackers use the information to spread disinformation and doubts about the capability of the government to protect its citizens.[867] When the attacks prolong for

---

[862] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[863] Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defence in the Cyber Context, Ibid, 438

[864] See page 90.

[865] See page 82,83

[866] Kaeo M, Founder & Chief Network Security Architect, Double Shot Security, Presentation on Cyber-attacks on Estonia (2007).200

[867] ibid 17.

weeks and networks remain inaccessible, citizens develop more doubt about the government, and they may even accept regime changes, proposed by the attacker.[868] This was the case in Estonia, where the Russian hackers attempted to force their ideology on the citizens. Information wars can be very effective, at low acquisition costs, and without firing a shot.[869] The previous review shows that determining state responsibility in the cyber context remains rather vague. Further, a state can employ non-state actors to carry out attacks and deny any involvement in the attack. Tracing the perpetrators is difficult, and even if systems provided by the attacking state are identified, the state can claim to be an innocent victim and say that its systems were used and that it was unaware of these attacks.

4.2.3. Changes in Estonia after the cyberattack

After the 2007 cyber-attack, Estonia has brought out a number of changes, which will be briefly discussed in this section. The cyberattack on Estonia was unprecedented in terms of the scale of the attack, the speed of the attacks, and the damage it caused. One would expect that governments around the world would be prepared and would have hardened their systems. Nothing of that sort appears to have been done, and governments are still squabbling over the legal aspects.[870] In the aftermath of the Estonia cyberattack, Estonia and the Grand Duchy of Luxembourg entered into an agreement to host Estonian data in Luxembourg.[871] The two countries agreed to establish a data embassy which enjoys the same protection and privileges of a conventional embassy. An attack on the embassy would be an act of war, and entering the embassy unless permitted would be an incursion into

[868] ibid 18.

[869] Caso J, 'The Rules of Engagement for Cyber-Warfare and the Tallinn Manual: A Case Study' The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems June 4-7, 2014, Hong Kong, China, 53.

[870] S, Scott, "Estonia Three Years Later: A Progress Report on" Combating Cyber-attacks ,Ibid, 22.

[871] S Bartłomiej, 'The data embassy under public international law' ,Ibid, 226.

another country.[872] However, despite this agreement, the legal status and actual protection against cyber-attacks is not clear.[873]

As per the agreement signed in 2013, Estonian data will be hosted in the data embassy with assets such as data and information systems licences, telecommunication, and storage system.[874] Would or indeed must other states respect that arrangement, and is there such a thing as 'protection of data embassies' in international law? The data embassy was physically located in offices provided by Luxembourg.[875] As per the Vienna Convention on Diplomatic Relations, the immunities and privileges of a mission covering the buildings, land, and the residence head of the mission were considered as part of a state.[876] The premises must be used for the purpose of the mission, and the convention does not differentiate or define the full nature of the mission.[877] As per Article 22 (1), the premises, documents, archives, and private residence of the diplomatic agent are inviolable.[878] The state in which the embassy is located does not have any right to enter the premises, unless invited by the mission lead, and these principles are the foundation of long regime.[879] The implication is that the premises, the occupants, and the inside repository cannot be searched, attached, or requisitioned and expropriated. The state in which the embassy is located needs to prevent any intrusion or damage and provide 24-hour security and police guard.[880] In the event that the embassy is seized or invaded, the host state is obliged to restore the premises and provide reparation for any damage. Article 21(2) does not impose any

[872] Ibid , 227.

[873] Ibid.

[874] Ibid.

[875] Ibid 228.

[876] United Nations, 'Vienna Convention on Diplomatic Relations' United Nations, Treaty Series,
500, 95.

[877] Ibid.

[878] Ibid.

[879] The Diplomatic and Consular Premises Act 1987 (from 15th May 1987, Ch 46) at <https://www.legislation.gov.uk/ukpga/1987/46>. 57 Aust (n 52) 114.

[880] Charpak Chatterjee, International Law and Diplomacy, (Routledge 2007) 199.

obligation to provide assistance for the members of the mission to obtain accommodation, but it is considered in good spirit to offer the required help.[881]

However, as per the Vienna Convention, the premises and the consular offices should not be used in a manner that is incompatible with the exercise and duties of the consular office; therefore, end use is the key to the agreement, and the Vienna Convention does not specify any terms about hosting data.[882] In the agreement between Estonia and Luxembourg, Article 1(b) speaks of the premises as a dedicated data embassy with the main purpose of hosting Estonian data and IT systems.[883] There are further clarifications that Luxembourg will take all required steps to protect the premises against any threats, damage, and intrusion. The whole objective of the agreement was to afford data and IT systems of Estonia the same level of rigour and protection that an embassy has.[884] While the systems are guarded and protected, this does not guarantee that hackers cannot gain access to the data. It is true that the data centre could not be physically attacked without violating the Vienna Convention; however, the same convention cannot stop a hacker from using advanced technology to make a similar attempt. It appears that Estonia has undertaken a lot of expense and time for protection, and these attempts may not be successful. This form of warfare does not need missiles, expensive fighter aircraft – it requires just a computer, some specialised software, and tools that can be downloaded for free, an internet connection, and special skills.[885]

Estonia brought in some changes to its strategy and approach to handle similar events.[886] It brought into force the Estonian Information Society Strategy 2013 to promote the development of a knowledge-based economy and society, where

---

[881] Ibid, 202.

[882] Bartlomiej, 'The data embassy under public international law' ,235.

[883] Ibid 236.

[884] Ibid 238.

[885] Ibid.

[886] C Christian, R Ottis, and A Talihärm, 'Estonia after the 2007 cyber-attacks: Legal, strategic
and organisational changes in cyber security' International Journal of Cyber Warfare and Terrorism (2011) 1.1, 24.

risks from cyberattacks were given top priority.[887] The National Security Concept of Estonia was first published in 2004, back then, cybersecurity did not receive a high level of attention. In fact, the documents and briefs did not even mention cyber threats and retaliatory defensive actions that could be taken.[888] In 2007, the Estonia government developed a Cyber Security Strategy (CSS) that presented a comprehensive policy for responding to cyberattacks. Multi-stakeholder committee were formed with agencies from the private sector.[889] The strategy looks at cybersecurity as a national exercise to respond to the overpowering threats formed by cyber-attackers. CSS has five objectives, and these are the formation of large-scale security measures, increasing skills in cybersecurity, improving the legal framework, and increasing international cooperation on cybersecurity.[890] Estonia also developed a National Security Concept in 2010 where the increased reliance on IT systems is addressed, as well as rising concerns about cyber threats. It recognises that cyber-terrorists, criminals, and organised criminals need to be targeted. Agreed actions included reducing the vulnerabilities of critical systems and data centres that should remain operational even in the middle of an attack. Moreover, there was further development of the Guidelines for Development of Criminal Policy.[891]

It was envisaged that a sufficient number of IT specialists and experts should be inducted in law enforcement agencies. Estonia helped to increase awareness and concern in NATO, which resulted in developing a unified strategy against cyber threats. Estonia also helped to support a number of international organisations such as the Association of Southeast Asian Nations, Council of Europe, and helped to set up a task force on Developments in Information and Communication Technology in the Context of International Security.[892] Considering that cyber laws were weak and full of loopholes, Estonia brought in a number of changes to the legislation that governed cyber-crime, criminal law, crises management laws, private laws, public

[887] Ibid.

[888] Ibid 25.

[889] Ibid 26.

[890] Ibid 27.

[891] Ibid.

[892] Ibid 28.

administrative law, and wartime/national defence laws. These laws provided all the legal support at the local level, and a hacker based in Estonia could not carry out an attack without facing severe punishment. However, the laws do not apply to international actors who could be based in Russia or elsewhere and carry out attacks around the globe.[893]

Fig 2.1 (below) illustrates the various laws that Estonia created to support the fight against cyber-attacks. Because of the huge losses and the severe damages to many digital services, the Estonian government develops its laws to protect the cyber space.[894] This table indicates the changes that have been made by the Estonian parliament in the cyber legislation realm. It can be seen from this table that there are some amendments to existing laws like the Criminal Procedure Law as well as completely new laws such as the Personal Data Protection Law which entered into force in 2008. Changes in criminal law indicate that Estonia aims to harden the deterrence against cyber-attacks. Also, it shows that Estonian law provides more jurisdiction over these attacks; thus, crisis management has improved its protection strategy. Moreover, the development in armed conflict law is a very significant indicator because it means that Estonia admitted the existence of cyber war and the need to defend its cyber realm legally. The improvement in public and private law shows that Estonia ensures protection that covers individuals, companies and government entities.

[893] Estonian Government,'Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian)'. Estonian Government 2010, <http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise side muutmine seletuskiri(424).doc&file_size=31650&mnsensk=424+SE&fd=. (accessed 29 May 2019).

[894] Cyber Space definition, Please see Key terms.

Constitutional law				
Fundamental rights and freedoms; Organisation of the state; Execution of public authority				
Private law	Public administrative law	Criminal law	Crisis management law	War-time law / national defence law
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e-services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

Figure 2.1 Changes to Estonia's laws to fight cybercrime[895]

As can be seen from the above discussion, after the 2007 attack, Estonia took proactive measures to harden its infrastructure, focused on skill building to fight cyber-warfare, and brought policies with stronger laws to fight such attacks. They raised strong voices in NATO and other forums to highlight the danger of such events. Other nations should stop fighting amongst themselves and co-operate to strengthen the global fight against cyber-warfare. This is the lesson which needs to be learned by the Saudi government. Even though, Estonia suffered a massive cyber-attack which resulted in big losses, it developed its cyber capacity and utilised this attack to strengthen its cyber protection.

4.3. Stuxnet

The Estonian DoDs attack was just the beginning of a series of cyber-attacks around the world. Three years after the Estonian cyber-attack, a malware infiltrated Iranian systems at the nuclear facility Natanz. Stuxnet is a very sophisticated malware, this became evident when the attack resulted in kinetic damages. This helps, and arguably makes it easier, to assess the attack based on the use of force rules. By examining this attack and its consequences, it will challenge the application

[895] C Christian, R Ottis, and A Talihärm, 'Estonia after the 2007 cyber-attacks: Legal, strategic
and organisational changes in cyber security' Ibid,.1.

of jus ad bellum rules to the cyber-attacks. It is first necessary to contextualise this section's analysis with an understanding of Iran's cyber capabilities. This is because, even before the perpetration of the attack itself, the country had been quietly expanding its cyber capabilities' scope and mastery.[896] This is because the Iranian government considers the country's development of knowledge in the realm of cyber relations to be a key aspect of its larger strategy to provide for the defence and exportation of the Shia Islamic revolution initiated in 1979.[897] Therefore, even as the Iranian government is looking to take significant action to control the use of the Internet by its own citizens, the Iranian government is also looking to derive benefits from it, and actively invests in cyber safeguards with a view to expanding its capability to project its cyber power.[898]

4.3.1 The Attack

In November 2010, it was announced that Natanz's uranium enrichment plant had stopped on a number of occasions due to a number of significant technical issues associated with Stuxnet.[899] This is because a "serious nuclear accident" occurred at the site in 2009 that is believed to have forced the then head of Iran's Atomic Energy Organisation to resign.[900] Additionally, statistics that the Federation of American Scientists published show that Iran's number of operational enrichment

[896] Marc Johnson, 'The rising Iranian cyber threat' (The Buckley Club <https://thebuckleyclub.com/the-rising-iranian-cyber-threat-15028b76e0f9> (27 May 2019).

[897] Ibid.

[898] Ibid.

[899] Yossi Melman, 'Iran Pauses Uranium Enrichment at Natanz Nuclear Plant' (Haaretz, 23 November 2010) <https://www.haaretz.com/1.5143485> (accessed 27 May 2019)

[900] Babbage, 'The Stuxnet worm: A cyber-missile aimed at Iran?' (The Economist, 24 September 2010) <https://www.economist.com/babbage/2010/09/24/a-cyber-missile-aimed-at-iran> (accessed 27 May 2019).

centrifuges fell from approximately 4,700 to around 3,900 at the same time.[901] Furthermore, in a report from December 2010, the Institute for Science and International Security (ISIS) implied that the Stuxnet attack itself served as a reasonable explanation for the damage that has been apparently caused at Natanz to the centrifuges between November 2009 and the end of January 2010.[902] Indeed, the Stuxnet attack in Iran appears to have been –

> *"designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. If its goal was to quickly destroy all the centrifuges in the FEP [Fuel Enrichment Plant], Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily"*.[903]

On this basis, the Stuxnet worm operated by causing the infected Iranian IR-1 centrifuges to vary significantly in speed over a number of days for varying periods of time.[904] The stresses from the varying speeds caused the aluminium centrifugal tubes to expand so that they actually came into contact with one another, which then ultimately destroyed the machine.[905]

---

[901] David Albright and Jacqueline Shire, 'IAEA Report on Iran: Fordow enrichment plant at "advanced stage of construction;" decline in number P1 centrifuges enriching but P1 centrifuge
efficiency increases; discovery of previously unknown stock of heavy water' (Institute for Science and International Security, 16 November 2009)

[902] David Albright, Paul Brannan, and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? (22 Dec 2010) , ISIS Reports, 6

[903] Ibid.

[904] Holger Stark, 'Stuxnet virus opens new era of cyber war' (Der Spiegel Online, 8 August 2011) https://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html (accessed 27 May 2019).

[905] Ibid.

However, the reality is that the impact of the Stuxnet worm upon Iran's cyber infrastructure was always limited.[906] This is because Iranian technicians were able to quickly replace the damaged centrifuges so that it is likely that there was only a brief disruption of uranium enrichment.[907] Therefore, in February 2011, a report was released by the ISIS that concluded that, so long as caution is exercised by the Iranian government moving forward, Stuxnet is unlikely to destroy more Natanz centrifuges.[908] The reason for this is that Iran is likely to have cleaned its control systems so that they were free from malware.[909] Nevertheless, caution will still have to be exercised in view of the fact that so many computers in the country are still considered to contain Stuxnet, despite the fact that the worm did not reduce uranium's production after 2010.[910] Nonetheless, it is still necessary to investigate why Stuxnet destroyed only 1,000 centrifuges.[911] Likely, this is because it proofed significantly harder to be able to destroy centrifuges than had previously been believed through the perpetration of cyber-attacks.[912]

4.3.2 Legal aspects of the Stuxnet Attack and its international unlawfulness

Regarding the legal aspects of the Stuxnet attacks, especially the question of its international unlawfulness, there is a need to ascertain if the operation could be objectively labelled as a 'use of force' under Article 2 (4) of the United Nations Charter and according to customary international law. Based on the application of the Schmitt Framework, it was concluded by Foltz that the Stuxnet attack could be

---

[906] Joby Warrick, 'Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack' (The
Washington Post, 15 February 2011).

[907] Ibid.

[908] David Albright, Paul Brannan, and Christina Walrond, 'Stuxnet Malware and Natanz: Update
of ISIS December 22, 2010 Report' (15 February 2011).ISIS Report, 10-12.

[909] Ibid.

[910] Ibid.

[911] Ibid.

[912] Ibid.

considered to be an example of a use of force under international law.[913] This is because it was recognised by the International Court of Justice in the case of *Nicaragua v. USA*[914] that the distinction between the threat or use of force (including armed force) and an armed attack is based on the particular operations *"scale and effects"*.[915] It is Fultz's view that the Stuxnet attack could be labelled as a *"per se use of force because it caused physical damage"* in Iran.[916] However, the labelling of Stuxnet in this way and for this reason, may be considered to be a somewhat glib oversimplification of the application of Schmitt's severity criterion.[917] The *"scale and effects"* criterion which was applied in the Nicaragua case is called an effects-based model,[918] which assesses the final result of the attack and its implications on the victim state.[919] The effects-based model goes beyond the physical effects. It also includes direct and indirect effects.[920] The destructing of 10 percent of the Natanz centrifuges constitutes the required effect to reach the level of use of force which is prohibited by Article2 (4) and therefore should be considered an armed attack.[921]

Morton has put forward a relatively straightforward two-pronged definition of the use of force in the context of cyberspace that serves to combine intent with

---

[913] Lieutenant Colonel Andrew Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force'
Debate' (2012) 67(4) JFQ 40,43-47

[914] Nicaragua Case, para 195

[915] Ibid.

[916] Michael Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence and Armed Conflicts' in National Research Council, *Proceedings of a* Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US *Policy* (2010), The National Academies Press, 155.

[917] L Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force'
Debate' Ibid,42

[918] A Moore, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law
and Potential Models." (2015) *Naval L. Rev* 64 20.

[919] Ibid.

[920] Ibid.

[921] Ibid 24.

Schmitt's Framework.[922] Specifically, Morton provides that a cyberspace use of force refers to any operation in cyberspace that (a) is meant to damage property or cause injury or death to persons and (b) that involves a physical invasion of the target country's sovereignty via its cyberspace infrastructure.[923] On this basis, Morton argues that any cyberspace operation that serves to fulfil these two prerequisites will be deemed to be both a use of force and an armed attack under Articles 2(4) and 51 of the UN Charter 1945 respectively.[924] Based on the application of Morton's understanding of cyberspace use of force, the author's view regarding the Stuxnet attack is considered to be clear: it aimed to disrupt the nuclear program in Iran.[925] More specifically, the Stuxnet attack was meant to damage Iran's physical infrastructure.[926] It must also be noted that the infection of the target computers with the Stuxnet worm needed the Iranian scientists to unwittingly provide help.[927] This is because these scientists unknowingly inserted infected thumb drives into computers that were not actually connected to the internet.[928] Therefore, it would seem that these actions can be equated to Iran's sovereignty being physical invaded. Therefore, based on Morton's understanding of cyberspace use of force, Stuxnet was an example of a use of force contrary to Article 2(4).[929]

The key distinction that could be drawn between understanding cyberspace use of force and the Schmitt Framework is that Stuxnet would be considered to be a use of force, even if the Natanz centrifuges had not suffered any damage at all.[930]

---

[922] Lieutenant Colonel Grady Morton Jr, 'Cyberspace Operations, Stuxnet, jus ad bellum and jus in bello' (Air War College, Air University, 14 February 2013).

[923] Ibid.

[924] Ibid.

[925] Ibid.

[926] L Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force'
Debate' Ibid, 41-42

[927] Ibid.

[928] Ibid.

[929] Lieutenant Colonel Grady Morton Jr, 'Cyberspace Operations, Stuxnet, jus ad bellum and jus in bello' (Air War College, Air University, 14 February 2013).

[930] D Hollis, 'Is a Use of Force the Same as an Armed Attack in Cyberspace?' (Opinio Juris, 28

This is because, even where no actual damage arose, the intent to bring about some form of damage was considered to have existed in practice.[931] In addition, the national sovereignty of Iran, as an independent country, was clearly violated by its cyberspace infrastructure being penetrated physically.[932] Therefore, combined, these factors were considered to be sufficient for the attack to amount to a use of force contrary to Article 2(4) of the UN Charter 1945.[933]

At the same time, however, it is also pertinent to consider the application of the principle of distinction to the Stuxnet attack because the attack's target was the uranium-enriching centrifuges.[934] As long as these centrifuges enrich uranium for nuclear weapons, they would be considered to be a valid military target.[935] However, as they look to move significantly further away from the intended target, there is a growing possibility that the destinations that a virus needs to pass through on the way to their ultimate target will be civilian.[936] Therefore, it is most effective to consider the whole network that controls a targeted military industrial complex's infrastructure.[937] On this basis, the Stuxnet attack actually served to infect thousands of computers in at least another eleven countries.[938] Despite the fact that the worm did not damage most of those computers, there is a need to consider if these computers have been damaged just because a virus infected them that needed specialists' time and effort to detect and remove.[939] On this basis, the threshold problem in this regard requires us to ascertain if a use of force under Article 2(4) was

---

April 2012) <http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armedattack-in-
cyberspace> [accessed 27 May 2019].

[931] Ibid.

[932] Ibid.

[933] Ibid.

[934] David Albright, Paul Brannan, and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? (22 Dec 2010), Ibid, 4-6

[935] Ibid.

[936] Ibid.

[937] Ibid.

[938] Lukas Milevski, 'Stuxnet and Strategy: A Special Operation in Cyberspace?' (2011) 63(4) Joint Force Quarterly 64, 69.

[939] Ibid.

actually initiated against these countries as well.[940] This is because Stuxnet was actually written in a way to remain harmless against all computers that were not using the Siemens software, whilst the virus was also set to self-destruct in the summer of 2012.[941] Therefore, it would seem to be true to say that there was a lack of intent to cause damage to all of the other computers that it passed through, so that it could be concluded that the principle of distinction was adhered to. There was a lack of intent to damage any computers beyond Iran.[942] At the same time, however, there is still a need to recognise that there is a caveat to the intent-base rule because a reckless release of a virus, like Stuxnet, could bring about liability for the principle of discrimination's violation despite a lack of specific intent.[943] In this regard, Sharp's suggested a model called *"Similar to strict liability"*.[944] This model requires the attack to target a state's critical infrastructure to amount to a use of force and potentially an armed attack. [945]

The Stuxnet attack targeted Iranian critical infrastructure. Therefore, Stuxnet Malware according to this criterion is a use of force and armed attack.[946] The Tallinn Manual also considers the Stuxnet attack as an armed attack based on the scale and effect assessment. The Stuxnet attack has a high level of intensity which meets the required level of scale, and its consequences have affected a significant facility in Iran which is considered a substantial element in the state. The thesis therefore follows the Manual's view for these reasons.

From another perspective, Moore does not consider the Stuxnet attack as a use of force. He based his view on the state practice and the definition of "force" is

---

[940] Ibid.

[941] Ibid.

[942] Herbert Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4(1) Journal of National
Security Law and Policy 77.

[943] Ibid.

[944] W Sharp, 'Cyber Space and the Use of Force' (1999). Aegis Research Corporation 7, 28 .

[945] Ibid.

[946] Moore A, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law
and Potential Models." Ibid, 21.

Article 2(4). He describes the act of the attack as *"Coercive uses of the cyber instrument"*.[947] Therefore, it is not an act of force even though it brought physical damage to the Iranian complex.[948]

The Tallinn Manual lists eight factors to determine whether or not the cyber-attack reaches the level of the use of force or an armed attack.[949] These factors are almost the same factors used by Schmitt to evaluate any cyber-attack, which are (immediacy, severity, directness, invasiveness, measurability, military character, presumptive legitimately and state involvement).[950] Regarding immediacy: although most of the Tallinn Manual experts agreed that Stuxnet is a use of force, there are others with a contrary view.[951] The experts who consider it a use of force use the same assessment for characterising use of force and armed attack. However, the others distinguish between the definition of them. As a result, the latter group based their argument on the immediacy requirements. That means *"…the target state must identify operation, injury, or damage contemporaneously to satisfy the armed attack requirement."*[952]

During the Stuxnet attack, Iran did not realise the attack took place until the damage had already been accrued.[953] With regard to the directness, Stuxnet was designed to target the enrichment plant at Natanz, and it achieved its target successfully.[954] Also, Stuxnet satisfied the severity criteria because it caused physical damage to Iranian infrastructure. Stuxnet has infiltrated other Iranian systems to reach its target, which meets the invasiveness factor.[955] The enrichment

---

[947] Ibid 22.

[948] Ibid

[949] Ibid.

[950] Schmitt M, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' Ibid, 18,19

[951] Moore A, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law and Potential Models." Ibid, 23.

[952] Ibid.

[953] Ibid.

[954] Ibid.

[955] In this Regard, Schmitt has noted: "In the cyber context, this factor must be cautiously

plant at Natanz can be considered a military target, which makes the connection with the military operation criteria. The destructive impact of the Stuxnet malware makes the use of this cyber instrument presumptively illegitimate, both internationally and domestically, in Iran.[956] The state involvement criterion is satisfied because the target of the attack was a governmental property. This assessment is also known as an analogous-instruments model, which focuses on the injury or the damage to the property. This model, as Moore describes, “analogizes the commonalities of the consequences of the use of armed force with the consequences of the use of the cyber instrument”.[957] This model characterises Stuxnet as a use of force due to the result or the damage caused to Natanz centrifuges, the same damage could have been caused by a military weapon.[958] Another legal issue in the cyber realm is the attribution of the attack. In the Stuxnet case, Iranian officials have attributed this attack to the United States and Israel.[959] They based their report on many interviews originating 18 months before the attack which reveal their intent to slow the Iranian weapon capability production.[960] Therefore, Stuxnet launched from a state actor which triggered international responsibility.

---

applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the Target-State’s territory, as

in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.” M Schmitt, "Cyber operations in international law: The use of force, collective security, self-defence, and armed conflicts." Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy. Vol. 151 (2010) 156.

[956] Ibid.

[957] Ibid 18.

[958] Ibid 23.

[959] D. E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran: Officials Cite Wide Effort to Hinder Nuclear Work," *New York Times (1923-Current File),* (2012). pA1.

[960] Ibid.

4.3.3. Changes in Iran after the cyberattack

After the Stuxnet attack against the Iranian uranium enrichment program, Iran has started to develop its cyber capabilities. In March 2012, the Iranian Supreme Leader has announced the founding of the Supreme Cyberspace Council whose first mission was to plan a cyberspace strategy.[961] This strategy consists of offensive and defensive tools to maintain its cyber security. In the defensive area, Iran aims to defend its data and critical infrastructure against any cyber-attacks.[962] Additionally, it aims to defend its cyberspace against any anti-governmental activity or any Western ideas which are not acceptable to the Iranian government.[963] Furthermore, Iran built a Cyberspace Defence Command. Its aim is to "develop a comprehensive defensive doctrine for state institutions and infrastructures against cyber threats."[964] The Iranian Passive Defence Organisation Leader Jalali, has declared that "Iran plans to fight our enemies with abundant power in cyberspace and internet warfare."[965] Furthermore, The Communications and Information Technology Ministry founded the Centre for Information Security (MAHER).[966] This centre is responsible to act in the case of a cyber-attack, and also trains experts in the cyber field as well as develop an auto response by machines to any cyber-attack.[967] In addition, this centre aims to defend all governmental websites or private entities listed with the Communication Ministry.[968]

---

[961] Kronenfeld S, Siboni G., Iran and Cyberspace Warfare, Military and Strategic Affairs, Volume 4, No.3,(2012), 78.

[962] Ibid 79.

[963] Ibid.

[964] Ibid, 84.

[965] Amy Kellog, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'enemies'," Fox News, (14 Mar 2011), http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/ [Accessed on: 5 Feb 2023]

[966] Kronenfeld S, Siboni G., Iran and Cyberspace Warfare, (2012), 4(3) Military and Strategic Affairs, 84.

[967] Ibid.

[968] Ibid.

On the offensive front, Iran has invested more than $1 billion in technology, recruiting experts and criminals to serve their interest.[969] In addition, the Iranian government trained a cyber force.[970] Moreover, Iran has built the Iranian Cyber Army (ICA). Ebrahim Jabbari, head of Iranian Revolutionary Guard Corp's (IRGC) described it as the second-biggest cyber army in the world.[971] The ICA's main function is hacking sites.[972] Moreover, the Revolutionary Guards build an electronic warfare system which has the ability and the efficiency to blocking radar and communications.[973] Iran has a very sophisticated program intended to build a separate network which is isolated from the World Wide Web.[974] This network operates under the name "Halal" and functions as a national network which allows the government to control the content of the web and public browsing and keep its data and governmental services safe and protected from hacking.[975]

Iran gives considerable attention to its relations with China and Russia regarding the cyber realm. China has invested more than $1 billion in Iranian infrastructure, whereas Iran is the main oil supplier to China.[976] This partnership goes beyond the trade and energy sector to cyber security as a mutual interest.[977] A comprehensive deal with the value of $130 million between the Telecommunications Company of Iran and the Chinese ZTE Corp is proof of this partnership. Iran bought a full surveillance system from ZTE which allows the Iranian government to monitor

---

[969] Farwell J., What does Iran cybar cabaility measn for future conflict? (2013) The Whitehead journal
of Diplomacy and International Relation 52.

[970] Ibid 55.

[971] Iran Says It Welcomes Hackers Who Work For Islamic Republic, (07 Mar 2011), Persien Letters website, Available at: https://www.rferl.org/a/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html [Accessed on: 5 Feb 2023]

[972] Ibid.

[973] Ibid 85.

[974] Kronenfeld S, Siboni G., Iran and Cyberspace Warfare, Ibid, 82.

[975] Ibid 83.

[976] Farwell J., What does Iran cybar cabaility measn for future conflict?, The Whitehead journal of Diplomacy and International Relation,(2013) 58.

[977] Ibid.

telephone lines, text messages, cellular lines, and web surfing.[978] Russia as well has been an ally to Iran in many areas. Russia provides strong support to Iran with regard to the U.S sanction against Iran.[979] Moreover, the Russia's Foreign Ministry has announced in 2012 that "the sanction against Iran was undisguised blackmail."[980] Lewis J., a specialist on cyberspace security, has stated that "Iran was quicker in developing offensive capabilities and more daring in their use than anyone expected."[981] This is a very considerable statement which proves Iran's cyber capability. Knowing this, the Iranian capacity is a model for Saudi Arabia to strengthen its cyber defence and be fully prepared for any type of cyber-attack. As Saudi Arabia is the main case in this thesis, it is important to look into the biggest cyber-attack against Saudi Arabia. In order to get the full picture of the legal aspects of this cyber operation, there will be a description of the attack and its effects, followed by a legal analysis of the attack. Then, there will be a discussion about cyber development in Saudi Arabia after that incident.

4.4. The Saudi Aramco Attack

Saudi Aramco (Saudi Arabian Oil Company) is a state-owned company responsible for the production, refining and exporting of the oil. Aramco has the ability to pump 12.5 million bpd and boasting more than 260 billion barrels of proven reserves, much of it easily recovered for less than $3 per barrel. Therefore, it is known as the biggest oil company in the world.[982] It has a market value up to $10 trillion USD.[983] For these reasons, [984] any threat to Aramco could potentially put Saudi Arabian national security in danger. The Saudi government secures Aramco

[978] Kronenfeld S, Siboni G., Iran and Cyberspace Warfare, Ibid, 82.

[979] Ibid.

[980] Ibid.

[981] Ibid,92

[982] C. Helman, "The World's Biggest Oil Companies," Forbes, 07-Sep 2010.

[983] N Abokhodair,Z Dehlawi, Saudi Arabia's Response to Cyber Conflict: A case study of the Shamoon malware incident, (2013).IEEE, 4-7.

[984] Ibid.

with more than 33,000 soldiers and 5000 guards.[985] Nevertheless, this high security did not prevent the cyber-attack.

4.4.1. The Attack

In August 2012, a self-replicating computer virus hit about 30,000 Windows-based workstations within Aramco. This virus's function was to overwrite files on the hard disks of the targeted computers.[986] This virus acquired the name "Shamoon". It showed a fraction of an image of a burning American flag. The analyst of this cyber-attack noted that this type of virus required physical access to a computer on the Aramco network[987], which means there was someone present who commenced this attack.[988] Therefore, Saudi Aramco should reconsider not just their cyber security measures but also their employee's loyalty and physical security.

The Shamoon virus has conducted a two-stage attack using Seculert.[989] Which means the attacker needed a computer connected to the internet to gain control of it. Then, the attacker used this primary computer as a proxy to the external Command-and-Control (C2) server. After the virus spread to the other computers, the Shamoon malware wiped all traces of other malicious software from these computers.[990] After twelve days of Shamoon nightmare, Saudi Aramco was able to resume its work as usual and restored the main internal network services. The United States Computer Emergency Readiness Team described Shamoon functionality as "highly destructive"[991], it impacted Saudi Aramco's activity greatly.

---

[985] Ibid.

[986] Bronk, Christopher and Tikk-Ringas, Eneken. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict.", Ibid,3

[987] Jeffery Carr, Was Iran Responsible for Saudi Aramco's Network Attack, Digital Dao (2012).

[988] Nicole Perlroth, Connecting the Dots After Cyber-attack on Saudi Aramco, The New York Times, (2012)

[989] Seculert is a cloud-based cyber security technology company based in Israel. The company's technology is designed to detect breaches and Advanced Persistent Threats, attacking networks. https://en.wikipedia.org/wiki/Seculert

[990] Seculert, "Shamoon, a two-stage targeted attack", 2012.

[991] United States Computer Emergency Readiness Team, Joint Security Awareness Report,

The attacked computers were temporarily unusable, and the Saudi Aramco website went down. Moreover, Shamoon's impacts went beyond Aramco to other companies such as Santa Fe, Ocean and Schlumberger and the Exploration and Petroleum Engineering Centre.[992] The significant question here is who is behind this attack, which leads to the legal analysis of Aramco incident.

4.4.2. Legal aspects of Aramco Attack and the international unlawfulness

It remains undetermined whether any unauthorised cyber attack against a fully state-owned company would violate the state's sovereignty. Currently, there is no customary law specifically dealing with cyber incidents because it is a rather new phenomenon. Irrespective of this, there is of course general customary law which can (and must) be applied to cyber situations. The author believes that it is generally possible that such attacks can violate a state's sovereignty, but every incident must be analysed on a case by case basis. The method to do so is by the Schmitt's standards. Therefore, the Aramco attack will now be closely examined.[993]

There is only little existing legal analysis of Aramco attack. Most of the academics who wrote about one legal aspect, such as the attribution, did so without a full legal analysis of the entire attack. For example, Carr and Lewis have discussed that the attack most likely originated from Iran, based on the intensive relation between Saudi Arabia and the Iranian government.[994] Moreover, Iran has an advantage from the destruction of Aramco cyber function and from affecting its oil production because Iran is faced with many sanctions due to their production of

---

2012.

[992] Bronk, Christopher and Tikk-Ringas, Eneken. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict.", Ibid,20.

[993] See https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

[994] Carr J, Who's Responsible for the Saudi Aramco Network Attack?, Infosec Island, 2012. U.S. says Iran behind cyber-attack in Saudi Arabia, Alarabyia News, 2012.

nuclear weapons which will bring their oil and gas infrastructure offline.[995] With regard to attribution of the attack, the sufficiency and qualification of evidence burden depends on the actors. Whether the attack is state-on state or involves non-state actors is elementary. In the case of the Aramco attack, the burden of proof for the attribution lies on the Saudis.[996] That was confirmed by Bronk and Tikk-Ringas, who also took a position of applying the existing rules of armed conflict and state responsibility to cyber operations by saying that "it still to be restated".[997] This expression needs more clarification, as it is too vague. Restating the existing rules could mean that there is no need for new rules, however, rewriting the existing laws in this regard means to make them more compatible and applicable for cyber operations. Another explanation for this expression could be making new rules whilst keeping the existing rules as they are. The thesis does not support any of these hypotheses. It suggests that the existing rules are applicable to cyber operations. In the context of the Aramco attack, the Schmitt standards, which have been used for the analysis of previous cyber-attacks, are an important method for assessing these cyber-attacks and drawing the legal limits for the state response.

There is no Aramco attack analysis based on the Schmitt standards. The Tallinn Manual has stated eight factors to determine whether or not the cyber-attack reaches the level of the use of force or armed attack, which is the same as the Schmitt standards.[998] The first one is immediacy. In the Aramco attack, Saudi Arabia did not notice the attack until it had already happened. There was no room for dialogue and negotiation between the attacker and the target. Therefore, the threat was immediate, and the damage has accrued which justifies the requirement to act in self-defence.

The second is the directness, the Shamoon malware has targeted the Aramco computers and achieved its goal by showing a burned American flag on all screens. The third criterion is the level of destruction caused by the attack, which is known as

[995] Bronk, Christopher and Tikk-Ringas, Eneken. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict.", Ibid, 22.

[996] Ibid, 25

[997] Ibid.

[998] See Tallinn Manual on the international law applicable to cyber warfare 2013.

“severity”. The Shamoon attack affected about 30,000 computers, which can be considered as a severe destruction. In regard to the invasiveness, the Shamoon virus affected the sovereignty of Saudi Arabia and has spread beyond Saudi borders as Platts reported: “both drilling and production data were lost, including data provided by such drilling companies as Santa Fe, Ocean and Schlumberger … The virus hit the company’s management offices throughout the Kingdom. It also hit its offices in Houston and The Hague…”[999] Therefore, the invasiveness criterion has been met.

The measurability criterion means the ability to assess how much damage has been done. In the Aramco attack, the damages have been measured by many institutions, such as the US Department of Homeland Security’s computer emergency readiness team (US-CERT). The destructive impact of the Shamoon malware makes the use of the cyber instrument presumptively illegitimate internationally and domestically in Saudi Arabia. The last criterion is the state involvement criteria, which is satisfied because the target of the attack was an oil company owned by the state, located in the territory of Saudi Arabia. Moreover, the attack was clearly launched to hurt Saudi Arabia, not just a company. As stated above, the author believes that some attacks against state-owned companies can violate a state’s sovereignty. She believes this is what happened here. Based on these criteria, the Aramco attack could amount to a use of force and an armed attack which allows self-defence. That was the Schmitt assessment for any cyber operation to help place the attack in the scope of the use of force or not. After this step, the attribution issue remains very complicated because it is difficult to determine who the perpetrator is due to the nature of the cyber space, which makes it difficult to track the right source of the attack. Even though, the victim state can locate the place of the attack, the state cannot know the person or the company who launched this attack. The attribution matter is not conclusive and will impact other legal consequences such as determining state responsibility.

---

[999] John Roberts, ‘Cyber Threats to Energy Security, as Experienced by Saudi Arabia’, Platts,
27 November 2012, http://blogs.platts. com/2012/11/27/virus_threats/. [Accessed on 5 Feb 2023]

4.4.3. Changes in Saudi Arabia after the cyber-attack

The 2012 cyber-attack against Aramco, was a wake-up call for the Saudi government to focus on the Saudi cyber security capacity. The Ministry of Communication and Information Technology in Saudi Arabia started to work on a National Information Security Strategy, which published its seventh draft by 2013. This strategy addresses many important topics and issues, such establishing a National IS Policy and Directive Issuance System, establishing the National IS Risk Assessment Function (NRAF) and establishing the National Risk Process Management System (RPMS). The objective of this strategy is to increase and improve Information Security Education, increase and improve Information Security Training Expand and improve Information Security Awareness and promote and emphasise the concept of shared responsibility. Furthermore, it is designed to strengthen the Kingdom's National Technical Capabilities, Combat Cybercrime Objective and Expand Research and Innovation Through International Cooperation.

Dr Khan, founder and CEO of the Washington-based Global Foundation for Cyber Studies and Research, stated that: “While Saudi Arabia is improving its cybersecurity in leaps and bounds, it also needs to pay careful attention to providing mandatory awareness and training programs at a national level.”[1000] The cyber security market in Saudi Arabia is increasing vastly. The market value in 2020 reached $5 billion.[1001] Consequently, Saudi Arabia has established many institutions for maintaining Saudi cyber security. They established the National Cybersecurity Authority, the Saudi Federation for Cybersecurity, Programming and Drones, and the Prince Mohammed bin Salman College of Cybersecurity, Artificial Intelligence and Advanced Technologies. Furthermore, the Saudi Vision 2030 envisions secure and resilient digital infrastructure with high-speed internet access across the country, also the cyber security is part of its concerns and improvements.

[1000] https://www.arabnews.com/node/1483661/saudi-arabia.

[1001] Ibid.

4.5. Conclusion

The incidents which were examined in this chapter are the Estonia DDoS attacks, the Stuxnet Malware, and the Aramco hacking of the refineries and oil production centres. Attempting to apply Article 2 (4) and Article 51 of the UN charter alone to these attacks is not enough. Therefore, the academic authors cited in this chapter suggested different models to examine the cyber operation in the context of *jus ad bellum* such as the analogous-to-instrument, the effect-based, and the strict-liability models. These modules will be discussed in detail in the upcoming chapters. Furthermore, the Schmitt analysis, which was adopted by the Tallinn Manual, consists of seven factors to determine whether the cyber operation is a use of force or an armed attack. State practice also proves that states will treat Article 2 (4) as just one of several factors to consider when characterising cyber-attacks. Consequently, this causes a shift in the international paradigm regarding "use of force". This outcome will be used in analysing and studying the cyber operation in the context of applying the jus ad bellum and the related principles such as the non-intervention principle and sovereignty.

Each case illustrates the technical difficulties of attribution of malware in cyber-attacks, which leads to difficulties in determining international responsibility.[1002] Moreover, they show how difficult it is to use the right of self-defence since the actor of the cyber-attack remains anonymous. Furthermore, all these cases show a different method of technology and have a distinguished scenario. For example, in the Estonian DDoS attack, the hackers sent a large flood of connection requests and spam with malware to the victims' servers. Due to the huge service requests, the servers crashed, which brought the IT systems of Estonia to a standstill.[1003] This allowed the hackers to gain access to the server and internal networks, where they stole and deleted information, or defaced sites. On the other hand, the Stuxnet worm caused the infected Iranian IR-1 centrifuges to vary significantly in speed over a number of days for varying periods of time.[1004]

[1002] J Jason, Attribution, state responsibility y, and the duty to prevent malicious cyber-attacks in international law. (2017), PhD thesis m University of Glasgow 18.
[1003] J Lewis, 'Cyber-attacks Explained' ,Ibid, 1-2.

[1004] Holger Stark, 'Stuxnet virus opens new era of cyber war' (Der Spiegel Online, 8 August 2011) https://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-

Therefore, one can clearly see that the cyber operation technique is very different from case to case. Consequently, the legal analysis was different.

This chapter showed the variety of cyber-attacks around the world and suggested possible ways for international law to deal with each one individually. It has been demonstrated that the legal studies about the mentioned cases are limited. In the case of the Aramco attack, there was no available legal analysis based on jus ad bellum rules available. This thesis created an analysis for the Aramco attack based on the Schmitt standards. The common element in all these attacks is the relative ease with which a few hackers managed to penetrate secure systems, making them crash, and the lack of attribution proof to bring the alleged hackers to justice.

Simultaneously, this chapter supports the aim and objective of this thesis by showing that applying existing paradigms to those attacks does not give a conclusive answer to the ability of applying *jus ad bellum* to cyber-attacks. State practice was the only way to determine if the *jus ad bellum* rules are applicable in these cyber-attacks or not. By illustrating the type of the attack and its effect on the state's critical infrastructure or its national peace and security, it has become evident that cyber coercion is prohibited based on the international community's consensus. In the absence of an international treaty to regulate cyber operations, applying the current jus ad bellum rules was the only way for the states to characterise the act of the cyber operation as a use of force or an armed attack. Therefore, state practice has provided a route to apply the current rules of use of force, which just need more analysis to fill the gaps arising particularly from technical issues such as allocating the source of the attack. As it worked previously for these states, it will be effective to apply the jus ad bellum rules to any cyber operations hereafter. The state practice in this regard will guide Saudi Arabia while developing its policy and will help to adopt rules to regulate the cyber operations to protect its critical infrastructure and to maintain its cyber security. This is the main aim of this thesis. The next chapter will illustrate the UNSC's role in cyber operations and discuss the most significant legal issues regarding its powers under the UN Charter, including if they also apply to authorising cyber operations.

---

opens-new-era-of-cyber-war-a-778912.html (accessed 27 May 2019).

CHAPTER 5: THE UNSC'S ROLE AND CYBER OPERATIONS

5.1. Introduction

The aim of this chapter is to discuss the role of the United Nations Security Council (UNSC) in cyber operations and the possibility of using cyber operations as a tool to maintain peace and security. For this, the chapter will analyse the UNSC's general powers of intervention, as well as the duty to maintain peace and security as a general principle. Next to a grammatical interpretation of the UN Charter, the author will analyse and engage with the literature on the role of the UNSC. Moreover, the UNSC's responses to cyber-attacks will also be evaluated and situated within its powers under Chapter VII: how did the UNSC interpret the concepts of 'threat to the peace', 'breach of the peace' and 'act of aggression' in practice? The key part of this chapter will be the examination of how cyber-attacks could fit within the three aforementioned bases for action according to Chapter VII. In addition, the chapter examines more broadly the ability of the UNSC to use cyber operations as a sanction. Lastly, the author will briefly address the political realities and current composition of the Council, which features in its decision-making process.

To start, the author will provide an overview of the United National Security Council's (UNSC) role based on the UN Charter and literature because that forms the foundation of its role and powers.

5.2 The UNSC's power to intervene to maintain peace and security

Under the United Nations Charter, the Security Council has the primary mission to maintain international peace and security.[1005] The UNSC can even allow

[1005] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 39.

deployment of military forces whenever and wherever a peace operation is required to restore international peace and security.[1006] While the Secretary-General as well as the General Assembly play complementary and important roles within the United Nations,[1007] the Security Council is the only body that can determine if a certain situation constitutes a threat to the peace.[1008] The UNSC can also call the parties to a dispute to settle it in peaceful ways and suggests terms of settlement or methods of adjustment.

The Security Council follows the principles of international law and justice when settling or adjusting internal situations or disputes that lead to a breach of the peace.[1009] It also aims at establishing friendly relationships amid different nations on the basis of respect for the principle of self-determination and equal rights of people, and to take other suitable actions to strengthen peace universally.[1010] The Council and its Members are obliged to follow the principles enshrined in the UN Charter, which includes the principle of the sovereign equality of all its Members. It is important for the Members to fulfil all obligations in good faith to ensure the benefits and rights that result from membership.

Further, in order to maintain international peace and security, it is significant for all UN members to refrain in their international relations from the use of force or threat against the political independence and territorial integrity of any state, or in any other way that is not relevant to the purposes of the United Nations.[1011] They should also refrain from providing assistance to any state against which the organisation is taking enforcement or preventative action and should provide the Security Council with the help in any action it takes accruing to the current

[1006] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 42.

[1007] "What Is The Security Council? | United Nations Security Council". 2020. *Un.Org*. https://www.un.org/securitycouncil/content/what-security-council.

[1008] UN Charter of the United Nations and statute of the International Court of Justice. UN, 2015.

[1009] Bailliet, Cecilia M., and Simon O'Connor. "The good faith obligation to maintain international
peace and security and the pacific settlement of disputes." In *Research Handbook on International Law and Peace*. Edward Elgar Publishing, 2019.

[1010] Ibid 19.

[1011] Ibid 20.

Charter.[1012] The United Nations Security Council also makes sure that the states that are not members of the organisation act according to these principles, as it is needed for the maintenance of international peace and security. It is also significant to acknowledge that nothing contained in the current Charter allows the United Nations to intervene in concerns that are within the domestic jurisdiction of any state and that entail the members to submit such concerns to settlement. However, this principle should also not detriment the implementation of enforcement actions under Chapter VII.[1013]

Moreover, under Chapter VII Article 39, the Security Council has the responsibility to determine if any threat to the peace, breach of the peace, or act of aggression exists, and make suggestions or decide what implementations should be done according to Articles 41 and 42.[1014] While Article 41 allows the UNSC to use measures short of armed force, Article 42 explicitly includes the authorisation of land, sea, or air forces. However, Article 42 should only be used if measures under Article 41 either remain inadequate or have proven to be unsuccessful.

Enforcement actions to restore and maintain international peace and security can include, next to military action, also economic sanctions.[1015] This can include partial or complete interruption of economic relations and of radio, telegraphic, postal, air, sea, rail, and other means of communications, as well as the division of diplomatic relations.[1016] These Articles also suggest that if these measures are inadequate for the Security Council, they must take action by land forces, sea, or air to restore or maintain international peace and security. It can also include blockade, demonstrations, and other operations by those means of Members of the United

[1012] Ibid 11.

[1013] Ibid 8.

[1014] Cullen, Miriam. "Questioning the Criminal Justice Imperative: UN Security Council Procedure and the Downside of Chapter VII Decision Making for the Adjudication of International Crimes." Global Governance: A Review of Multilateralism and International Organizations 25, no. 2 (2019): 327-350.

[1015] Gray C. *International law and the use of force*. Oxford University Press, 2018.

[1016] Galand, Alexandre Skander. "Was the Residual Mechanism's Creation Falling Squarely within the Chapter VII Power of the Security Council?." *Questions of International Law* 40 (2017).

Nations.[1017] Furthermore, the Security Council has also developed special political missions, known as Peacekeeping Operations.[1018]

However, the composition of the Council and the lack of reform since the foundation of the UN has been criticised by many scholars. The five permanent members (P-5) of the Council, China, France, Russia, the UK and the US all have a veto which, once used, automatically blocks any attempt of making a decision. The veto power has been vastly criticised. Some scholars, like Mohamad Ali et al. criticise the mere existence of the veto powers, arguing there should be a majority rule decision instead.[1019] Koester points out that the main problem is that the use of the veto blocks the UNSC and makes decision-taking impossible.[1020] This was not only evident in the Cold War, it is also evident today. Therefore, the UN's most powerful organ is not actually functioning. This point is also supported by Papalia who criticises the 'unqualified veto' which means a veto given for singular national interests.[1021]

Further, the Council is not representative of the international community (no less the P-5), they also have occasionally been accused of overstepping their mandate. There are no checks-and-balances, Efekthar Jaromi and Hajani underline

[1017] Green, Leslie C. "United Nations operations." In *The contemporary law of armed conflict*. (2018)

Manchester University Press, 318-326

[1018] "Maintain International Peace And Security". 2014. *Un.Org*. https://www.un.org/en/sections/what-we-do/maintain-international-peace-and-security/index.html#:~:text=The%20UN%20does%20this%20by,peace%20to%20hold%20and%20flourish.&text=The%20UN%20Security%20Council%20has,for%20international%20peace%20and%20security. [Accessed on: 5 Feb 2023], 11

[1019] Mohamad Ali, Mohamad Syazwan Shah, Megat Mahathir Megat Tharih Afendi, and Noor Azizi Abdul Aziz. "A criticism on the UNSC veto power and the introduction of majority rule as an alternative." (2012).

[1020] She goes on to explore different options for the international community to act, like R2P. Koester, Chelsea. "Looking Beyond R2P for an Answer to inaction in the Security Council." Fla. J. Int'l L. 27 (2015): 377.

[1021] Papalia, Giorgia. "A critique of the unqualified veto power." Perth ILJ 2 (2017) 55.

this point by arguing the UNSC should be legally responsible for its actions.[1022] The UNSC's action or inaction will be further explored in the next section. However, this should already give an idea about the political realities of the Council.

Nevertheless, the idea of the UN Charter is that the United Nations maintain international peace and security through the UNSC by using peacekeeping, peace building, counter-terrorism, disarmament, and preventative diplomacy and mediation. Peace-making is one of the most effective techniques that are available to the United Nations. It helps host countries detect the difficult way from conflict to peace. The multidimensional function of peacekeeping today is called upon to not just maintain international peace and security, but also promote and protect human rights and help in extending legitimate state authority and restoring the rule of law, support constitutional processes and the organisation of elections. Measures can also include the reintegration and demobilisation of former combatants, assisting in disarmament, protecting civilians, and facilitating political processes.

The Secretary-General introduced the Action for Peacekeeping Initiative in 2019, in order to revamp the mutual political commitment to the operations of peacekeeping. The peace building activities in the United Nations aim at laying the ground for sustainable peace and development, decreasing the risk of relapsing into conflict, and helping countries emerge from conflict.[1023] The United Nations peace building architecture consists of the peace building Support Office, the Peace building Fund, and the Peace building Commission. The Peace building Support Office provides support and assistance to the Peace building Commission with policy guidance and strategic advice, administers the Peace building Fund and serves the Secretary General in collaborating with the agencies of the United Nations in their peace building efforts.[1024] The United Nations also co-ordinates the global fight against terrorism to maintain international peace and security.[1025]

[1022] Eftekhar Jahromi, Goudarz, and Ali Hajiani. "The United Nations Security Council Performance under Criticism and Objective Monitoring." *International Law Review* 34.56 (2017): 37-60.

[1023] Ibid.

[1024] Ibid 10.

[1025] Ibid 9.

In 2006, the United Nations Global Counter Terrorism Strategy was founded. This was the first time UN member states agreed to a shared operational and strategic framework to fight terrorism. Further, the General Assembly and other bodies belonging to the United Nations that are supported by the Office for Disarmament Affairs worked to promote international peace and security with the help of removing nuclear weapons along with other weapons that lead to mass destruction and the regulation of conventional arms. One of the most effective ways to eliminate massive economic costs of conflicts and human suffering along with the aftermath is to prevent conflicts initially.[1026]

One important concern the United Nations emphasise is the action on those who are responsible for the practices and policies involving punishment by the international community, while decreasing the effect of the measures considered on other parts of the economy and population.[1027] The United Nations exists to provide support to the preservation of international peace and security, as well as to provide help to the peoples and Governments in developing a world, in which freedom from want and fear is the reality for all. The lessons of the past seventy-two years have demonstrated that these goals are fundamentally interlaced, which the human rights, development, and security are being the preconditions for sustainable peace.[1028] The member states are the main providers of security that grant the protection of sustainable development and human rights. The task of the United Nations is to support the national actors in accomplishing their development goals along with peace and security.

Having said that, the establishment of accountable and effective security institutions on the basis of full respect for human rights, without discrimination, and the rule of law are crucial. Further, the United Nations have been involved for decades and play a critical role in helping the national actors to re-establish or improve security at the request of national Governments or in response to the General Assembly or United Nations Security Council mandates, specifically in the aftermath of conflict. Irrespective of this extensive experience, support for the sector

[1026] Ibid 10.

[1027] Ibid 11.

[1028] Ibid.

reform of security has remained largely an expedient undertaking.[1029] The United Nations Security Council has elaborated on the standards and principles to guide its support for the national actors in re-establishing and improving security.[1030] It uses a system-wide approach to provide coherent United Nations help in those contexts where it has resources to deliver effective support and stay active to the national authorities.[1031]

Further, according to the Article 40 of Chapter VII of the Charter, it is important to prevent an inflammation of a situation and the Security Council has the responsibility to make suggestions and decisions on the measures mentioned in Article 29. Therefore, it is important for the members to call upon the concerned parties and abide by provisional measures as it deems desirable and needed. It is important to understand that these measures should be in the absence of prejudice to the position, claims, and rights of the concerned parties.

Article 43 propounds that all Members of the United Nations should be available for the Security Council when called upon, with assistance, armed forces, agreements, and facilities that are needed to maintain international peace and security. It is also significant that the agreements should control the types and numbers of forces along with the general location, their level of readiness, and the nature of the assistance and facilities to be delivered.[1032] The agreement should also be negotiated as soon as possible on the initiative of the United Nations Security Council. Article 44 proposes that when the Security Council decides to use force, it

[1029] Roscini, Marco. "Cyber operations as a use of force." Research Paper No. 16-05, University of Westminster, (2015), Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631078 [Accessed on 5 Feb 2023]. Published in :Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 233-254

[1030] Wood, Michael. "International Law and the Use of Force: What Happens in Practice?." (2013), 53 Indian journal of international law, 345-367.

[1031] Ibid.

[1032] COL, Louis H. Jordan. Report: "Arms Control and European Security."(2012), Strategic Studies Institute Monograph. Available at: https://www.globalsecurity.org/wmd/library/report/2012/ssi_blank-jordan.htm [Accessed on 5 Feb 2023].

should invite the member, provided that the member is interested, to take part in the decisions of the Security Council.[1033]

As per Article 45, members should hold a national air force contingent available for unified enforcement action in order to allow the United Nations to take military measures urgently.[1034] It is also essential that the degree of readiness and strength of these plans and contingents is determined in accordance with the agreements stated in Article 43. According to Article 46, these plans should be created by the Security Council by taking assistance of the Military Staff Committee. In this case, Article 47 advises that an established Military Staff Committee should exist in order to provide assistance on all questions regarding military requirements for preserving international peace and security, possible disarmament, the regulation of armaments, and the command and employment of forces placed at its transfer.[1035] This Article also suggests that the Military Staff Committee should comprise of Security Council Chief of Staff of the permanent members or their representatives.[1036] The Military Staff Committee also has the responsibility for the strategic direction of any armed forces at the transfer of the Security Council and to develop regional subcommittees.[1037] In Article 48, the action entailed to implement the decisions for maintaining international peace and security is important to be

---

[1033] Basu, Soumita. "Gender as national interest at the UN Security Council." (2016), 92(2) *International*
Affairs, 255-273.

[1034] Thakur, Ramesh. The United Nations, peace and security: from collective security to the responsibility to protect. (2016),Cambridge University Press, 35

[1035] Novosseloff, Alexandra. The UN military staff committee: Recreating a missing capacity, (2018),
Routledge,.First part.

[1036] Zhou, Jian. "Main Content of International Military Law." (2019), In *Fundamentals of Military Law*,
pp. 549-564..

[1037] Schneiker, Andrea, Anne Jenichen, and Jutta Joachim. "Situating the Gender Mainstreaming Norm in Regional Organisations: Comparing the Incorporation of UN Security Council Resolution 1325 in the EU and OSCE." In *Rethinking Gender Equality in Global Governance*, (2019), Palgrave Macmillan, 97-120.,.

taken into account for all members of the United Nations.[1038] Such decisions are implemented either by the United Nations or through their action in the suitable international agencies, of which they are members.

Articles 49 and 50 also indicate that the members of the United Nations should take mutual assistance in implementing measures that are decided by the Security Council.[1039] Under the Article 51 of Chapter VII of the Charter, nothing in the present Charter should damage the right to collective self-defence or the inherent right of individual self-defence if there is an armed attack against any member of the United Nations.[1040] This is important until the Security Council has considered taking measures in order to restore international peace and security.[1041] The measures considered by the affected member should also be reported to the Security Council and should not have an impact on its responsibility and authority under the current Charter at any time.

At times, radical change also leads to a response of crisis or conflict that threatens the security and peace of people or shows shortcomings in the arrangements that exist. The peace and security sector reform defines a process of implementation, review, an assessment along with evaluation and monitoring, which is led by national authorities that have as their goals the improvements of accountable and effective peace and security for the state and its peoples with full respect and without discrimination for the rule of law and human rights.

Making sure that there is international peace and security rests an unsettling challenge for the United Nations. Regardless of the efforts of the past seventy-two years, violence and conflict continue to pose a threat to the peoples and the member

---

[1038] Melling, Graham, and Anne Dennett. "The Security Council veto and Syria: responding to mass atrocities through the “Uniting for Peace” resolution." (2017), 57(3) *Indian Journal of International*
Law 285-307.

[1039] Ibid 40.

[1040] Baladze, Mariam, Legal Ground of Using Armed Forces in Modern International Law.264. Available at: http://dspace.wunu.edu.ua/bitstream/316497/34392/1/264.pdf [accessed on 5 Feb 2022]

[1041] Rhoads, Emily Paddon. Taking sides in peacekeeping: impartiality and the future of the United Nations 2016. Oxford University Press,.

states, freedom from want and fear rests evasive for many. Having said that, the United Nations Security Council continues to search for effective responses to highlight insecurity based on its Charter.[1042] There are two important themes that have emerged. The first one is that development, human rights, and security are mutually reinforcing and independence conditions for sustainable peace. Whereas the second is that the identification of these key components can only be accomplished within a broad framework of the rule of law. The member states and their organisations are also the main providers of security, and this is their sovereign responsibility and right.[1043]

How the United Nations can support member states in improving and preserving their capacity to meet this responsibility within a wider framework of respect for human rights and the rule of law has become a major concern for the United Nations Security Council. In recent years, the Security Council has also made important progress in providing technical help and describing a normative framework in this critical area.[1044] Yet, there is more to be implemented, and the United Nations Security Council stands ready to enlarge its support for peoples and the member states in communicating more sustainable and comprehensive strategies on the basis of national ownership. The early establishment of mechanisms and structures to regulate and protect the economy and public administration is an important step for building confidence. The existing agency mechanisms assist to make sure that the security considerations are highlighted at initial stages. Adding to that, the Peace building Commission also plays an important role in providing support for the national strategies to sustain and consolidate peace[1045].

[1042] Schia, Niels Nagelhus. Horseshoe and catwalk: Power, complexity and consensus-making
in the United Nations Security Council. 2017,Cambridge University Press,.

[1043] Liaropoulos, Andrew N. "Cyberspace governance and state sovereignty." In *Democracy and*
an Open-Economy World Order, (2017), Springer, Cham, 25-35..

[1044] Thakur, Ramesh. "The nuclear ban treaty: Recasting a normative framework for disarmament." (2017), 40(4)*The Washington Quarterly* ,71-95.

[1045] Ibid.

Indeed, the UNSC's power to intervene to maintain international peace and security can arguably also include threats posed by a cyber operation. The problem seems rather, that the likelihood of it not acting, due to veto is very high. Irrespective of that, it becomes more and more likely that cyber-attacks can amount to a threat which then authorises the Security Council to act with its measures. Such a scenario will be analysed and discussed in the next part.

5.3 UNSC's Role and powers relating to Cyber Operations

This chapter will evaluate the UNSC's possible responses to cyber-attacks and how responses can be situated within its powers under Chapter VII: how did the UNSC interpret the concepts of 'threat to the peace', 'breach of the peace' and 'act of aggression' in practice? The key part of this chapter will be the examination of how cyber-attacks could fit within the three aforementioned bases for action according to Chapter VII. In addition, the chapter examines more broadly the ability of the UNSC to use cyber operations as a sanction. Lastly, the author will briefly address the political realities and current composition of the Council, which features in its decision-making process.

While the key question for this section directly relates to the past practice of the UNSC, it is interesting to note that so far, no P5 country introduced cyber security to the agenda of the United National Security Council (UNSC). While the non-permanent members the Netherlands and Lithuania thought about introducing the topic to the Council, they have not done so during their time of membership.[1046] Nevertheless, despite not having discussed it as a stand-alone topic or as of principle, the Council could at any time change this. Moreover, the argues that cyber operations can in certain circumstances, as discussed in the previous chapters, constitute the use of force. If they do, it seems reasonable to assume the UNSC will

[1046] Tikk, Eneken, and Niels Nagelhus Schia. "The role of the UN Security Council in cybersecurity: International peace and security in the digital age." *Routledge Handbook of International Cybersecurity*. Taylor & Francis, 2020 2.

classify them as a threat against peace, breach of peace or an act of aggression according to Article 39.[1047]

As mentioned above, it is very possible that cyber matters fall within the mandate of the Council. To reiterate, Giegerich has mentioned that the Security Council is one of the six organs of the UN developed by the UN Charter.[1048] While various UN bodies may make propositions, the Security Council is the only UN body that can make binding decisions under Chapter VII of the charter. As Article 39 says: 'The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.' The essential mandate of the Security Council therefore does not only relate to universal peace and security, it also gives the Council the power to determine what is a threat to international peace and security. The Security Council uses procedures including making understandings, investigating and interceding, and, when indispensable, dispatching military/peacekeeping forces and requesting monetary endorsements. However, security also includes technology as identified by the principles of the UNSC.[1049] This is especially discussed in the literature. Emanuilov has e.g. stated that even though the UNSC has not given a single objective endorsement of the usage of cyber ambushes, on 7th June a social occasion of authorities agreed on a critical report to then UN Secretary-General Ban Ki-moon, under the title of "On the Developments in the Field of Information and Telecommunications in the Context of International Security".[1050] Upon the appearance of the report, the Secretary-General called a meeting of 15 experts from the five permanent UNSC members with the extension of experts from Argentina, Australia, Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to request the UN General Assembly to "study possible

[1047] Valuch, Jozef. "USE OF FORCE IN CYBERSPACE." International & Comparative Law Review/Mezinárodní a Srovnávací Právní Revue 20.2 (2020) 176.

[1048] Emanuilov, Ivo. "International (Cyber) security of the Global Aviation Critical Infrastructure as a Community Interest." (2019): 299-342.

[1049] Ibid.

[1050] Giegerich, Thomas. "Article 57." In the *Vienna Convention on the Law of Treaties*, pp. 1061-1068. Springer, Berlin, Heidelberg, 2018.

accommodating measures in having a tendency to existing and anticipated threats."[1051]

There are therefore two questions here: 1) Can the use of cyber operations be a threat to international peace and security?, and 2) Can cyber means be used as measures under Article 42 of the charter?

As discussed in chapter four, state practice has provided a route to apply the current rules of use of force to cyber operations. As Valuch says “It may be any threat or use of force that is directed against the territ or political independence of a state or is otherwise incompatible with the UN objectives.”[1052] Therefore, one can conclude that “a cyber operation which poses a threat or the use of force against the territorial integrity or political independence of a state, or which is otherwise incompatible with the objectives of the United Nations, is also contrary to the principle in concern.”[1053]

The author assumes that, similar to the use of regular force, there are two exceptions for using force in cyberspace. One is self-defence as mentioned in Article 51 of the UN Charter, the other is a mandate authorised by the Security Council. The latter situation will be discussed in detail below. This Chapter will examine the role of the Security Council based on Chapter VII of the United Nation Charter. It will discuss how the Security Council could intervene in the case of a cyber-threat to international peace and security.

To gather what responses to cyber-attacks are possible, it will be evaluated and situated within its powers under Chapter VII: how did the UNSC interpret the concepts of ‘threat to the peace’, ‘breach of the peace’ and ‘act of aggression’ in practice? The key part of this chapter will be the examination of how cyber-attacks could fit within the three aforementioned bases for action according to Chapter VII.

As discussed in the previous section, the UNSC has the authority to use measures short of force and measures involving force when there is a threat to

[1051] Ibid.

[1052] Valuch, Jozef. "USE OF FORCE IN CYBERSPACE." International & Comparative Law Review/Mezinárodní a Srovnávací Právní Revue 20.2 (2020) 177.

[1053] Ibid, 178.

international peace. As per Article 41 of the UN Charter, “The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.”[1054] In the past, the Council has considered a threat to the peace in several cases. In a presidential statement in 1992, threat to the peace was defined as ‘humanitarian emergencies, the overthrow of democratically elected leaders, extreme repression of civilian populations and cross-border refugee flows threatening regional security, and failure to hold perpetrators of major atrocities accountable’.[1055] Over time, the Council included Illicit trafficking in small arms and light weapons: UN Doc S/PRST/2006/38 (West Africa), international terrorism: UNSC Res 1368 (12 September 2001), and Proliferation of weapons of mass destruction and their means of delivery: UNSC Res 1467 (18 March 2003).

Likewise, the Council has only sporadically confirmed a breach of the peace under Art. 39 of the Charter. The Council confirmed a breach of the peace in cases of aggression, concerning the invasion of the Falkland Islands, concerning the Iran/Iraq war and concerning the invasion of Kuwait.[1056] This means, the Council only considers a threat to the peace or breach of the peace if there was an armed attack or act of aggression or the potential threat of mass destruction. Aggression alone has also been mentioned in relation to Art. 39. Most prominently and frequently regarding the case of

[1054] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 41.

[1055] Presidential statement of 31 January 1992 (UN Doc S/23500).

[1056] United Nations Security Council Resolution 82 (1950) on the calling upon the North Korean authorities to withdraw their armed forces to the 38th parallel (United Nations Security Council [UNSC]) UN Doc S/RES/82(1950), United Nations Security Council Resolution 505 (1982) requesting the Secretary-General to undertake a renewed mission of good offices for the Falkland Islands (Malvinas) (United Nations Security Council [UNSC]), United Nations Security Council Resolution 598 (1987) requesting the Secretary-General to dispatch observers to supervise the cease-fire between Iraq and the Islamic Republic of Iran (United Nations Security Council [UNSC]) UN Doc S/RES/598(1987), SCOR 42nd year, 5, United Nations Security Council Resolution 660 (1990) on the Iraqi invasion of Kuwait (United Nations Security Council [UNSC]) UN Doc S/RES/660(1990), SCOR 45th Year 19.

South African incursions against Angola.[1057] So how can we use this assessment for cyber?

From practice, it can be understood that the UNSC considers itself to have the authority to use force in situations which involve international terrorism, and the proliferation of weapons of mass destruction.[1058] With regard to cyber operations, the Security Council has decided that some cyber acts constitute a threat to peace and security or an act of aggression.[1059] At the UN, cybersecurity issues are discussed in the UN General Assembly Committee on Disarmament and International Security (DISEC) and in two working groups of governmental experts. The first one, which was created through the initiative of the United Kingdom, is closed. 25 experts are members of the group, including all permanent members of the UN Security Council. The second group, which was created at the behest of Russia as a response to the 'non-transparent' UK group, is open to all interested UN countries. James Lewis, CSIS, of the Washington-based Centre for Strategic and International Studies, told Voice of America's Russian Service that cybersecurity has been neglected by the UN. This topic, especially the issue of holding states accountable for cyberattacks, is 'politically sensitive.' Lewis noted that those permanent members of the UN Security Council with veto power do not want to raise this issue in formal meetings: 'This is why such informal processes are so valuable.'[1060]

For the aim of this thesis, three issues need to be examined. First, when does the Security Council consider a cyber operation to be a 'threat to the peace,

---

[1057] United Nation Security Council Resolution 475 (1980) Angola-South Africa (United Nations Security Council [UNSC]) UN Doc S/RES/475(1980), SCOR 35th Year 21, United Nations Security Council Resolution 546 (1984) on South Africa's military attacks on Angola (United Nations Security Council [UNSC]) UN Doc S/RES/546(1984), SCOR 39th Year 1, United Nations Security Council Resolution 567 (1985) Angola-South Africa (United Nations Security Council [UNSC]).

[1058] SC Res. 1373, UN Doc. S/RES/2001 (28 September 2001). And SC Res. 1540, UN Doc. S/RES/1540 (28 April 2004).

[1059] Tallinn Manual ,(2017), 357.

[1060] Maria Tolppa, International Cyber Stability Framework at the United Nations Security Council, NATO CCDCOE Law Branch, Available at: https://ccdcoe.org/library/publications/internationalcyber-stability-framework-at-the-united-nations-security-council/.

breach of the peace, or act of aggression'? Second, under what circumstances might measures authorised by the Security Council under Chapter VII include cyber operations? Third, is there a possibility of using cyber-attacks as measures by the Security Council against cyber or kinetic threats?

Regarding the first matter, Article 39 of the UN Charter states that 'The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken…'[1061] Therefore, the Security Council has discretionary authority to determine if certain acts constitute threats to peace and security. These acts could be threats to the peace during internal conflicts, such as those in Liberia, Rwanda, Sierra Leone, and East Timor[1062]; violations of human rights and humanitarian law in Somalia, Rwanda, and Eastern Zaire; violations of democratic principles in Haiti and Sierra Leone;[1063] terrorism; nuclear proliferation; and failure to cooperate with international prosecutions.[1064] However, when commenting on the Security Council's power to classify any act, Frowein stated that this does not mean that the Security Council has unlimited authority in that matter but that a threat to peace may occur 'when, in a particular situation, a danger of the use of force on a considerable scale arises.'[1065] Although Frowein made an important point when he stated that the Security Council does not possess "limitless" power, the ordinary meaning of Article 39 indicates that the Security Council has broad authority in determining what constitutes a threat to the peace. This argument is sufficient to classify cyber operations as a threat to peace and security. Dinniss argued that a cyber-attack would constitute a threat 'where it is of sufficient gravity that a state is likely to respond to it with force, regardless of whether it is categorised as an armed attack, or where the type of attack indicates further violence to follow, whether

[1061] United Nations, Charter of the United Nations, Ibid, Art. 39.

[1062] SC Res 794, 3 December 1992 on Somalia; SC Res 929, 22 June 1994 on Rwanda; SC Res 1078, 9 November 1996 on Zaire.

[1063] For Haiti: SC Res 841, 16 June 1993; SC Res 917, 6 May 1994; SC Res 940, 31 July 1994 and most recently SC Res 1529, 29 February 2004. For Sierra Leone: SC Res 1132, 8 October 1997; SC Res 1270, 22 October 1999; SC Res 1289, 7 February 2000; SC Res 1306, 5 July 2000.

[1064] SC Res 1172, 6 June 1998 on nuclear proliferation; SC Res 748, 31 March 1992 on Libya's failure to cooperate with prosecution of the Lockerbie bombers.

[1065] Jochen Frowein, 'Article 39' in B. Simma (ed.), The Charter of the United Nations: A Commentary (2nd edn, Oxford University Press, 2002) 717, 722.

electronically or by kinetic means.'[1066] It is clear that any assessment of cyber operations will be based on their severity and potential impact on the peace and security.

With regard to the second issue which need to be examined, Article 41 of the UN Charter, which grants the Security Council the authority to implement measures, states that 'The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.'[1067] Further, Article 42 states 'Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.'[1068] Therefore, the Security Council can use both forceful and non-forceful measures, including cyber means. For instance, if a state develops nuclear capacity and ignores the Security Council's requests to terminate that activity, the Security Council may authorise another state to interrupt the weapons programme by conducting a cyber operation.[1069] Moreover, the Security Council has the authority to use all 'necessary measures,' which indicates that it may use cyber operations as measures in the use of force level; the Security Council can also use kinetic measures against a cyber activity.[1070]

Dinniss has argued that cyber measures taken by the Security Council could be the 'equivalent of a blockade,' which is already included in Article 42 as a forceable measure.[1071] Dinniss also emphasised that 'Electronic measures under Article 41 could arguably also encompass denial-of-service attacks launched against

[1066] H. Dinniss, Cyber Warfare and the Laws of War, Ibid, 110

[1067] United Nations, Charter of the United Nations, Ibid, Art. 41.

[1068] Ibid, Art. 42.

[1069] Tallinn Manual 2.0., (2017), 359.

[1070] Ibid.

[1071] H. Dinniss, Cyber Warfare and the Laws of War, ibid, 111.

the media, banking and telecommunications infrastructure of a state.'[1072] These are some examples of the cyber measures that could be adopted by the Security Council and which comply with Article 41.

To assess the third issue, namely the probability of the Security Council to respond to a cyber or kinetic threats by cyber means, one must study past Security Council resolutions. For instance, from 2006 to 2010, the Security Council passed a number of resolutions and reports about the 'proliferation risks presented by the Iranian nuclear programme'.[1073] The Council stated that 'it is acting under Article 41 of Chapter VII of the Charter, and each resolution calls for member states to implement a series of specific non-forceful measures against Iran.'[1074] Therefore, while the Security Council may use cyber means in response to a threat to international peace and security, these must be within a specific scope and limit, and must also be in accordance with Articles 41 and 42 of the UN Charter.

As a general matter in international law, the Security Council must comply with the *jus cogens* rules when exercising its authority to use force. However, it may disregard other international law rules. In the context of a cyber operation, the Tallinn Manual provides an example by considering that the Security Council may target a civilian object which usually would be forbidden to be targeted by armed conflict law; yet, the UNSC could ignore the principle of distinction if such an act would achieve international peace and security.[1075] However, this example is not accurate in such a context because targeting civilian objects constitutes a fundamental breach of international humanitarian law and Rules 82 and 83 of the Tallinn Manual state that peace operations must comply with the rules of armed conflict.[1076] Therefore, that example is not in the right place. The rules of armed conflict—such as respecting civilian objects — bind any state and the Security Council itself during any armed conflict. It is worth mentioning that local laws should comply with the Security Council resolution regarding the use of cyber means, such as Internet service provider

[1072] Ibid.

[1073] SC Res 1929 (2010); SC Res 1803 (2008); SC Res 1747 (2007); SC Res 1737 (2006).

[1074] Ibid.

[1075] Ibid 360.

[1076] Tallinn Manual 2.0., (2017), 357.

regulations, amending them to comply with the UNSC resolution.[1077] However, cyber operations conducted by a peace force must respect local rules and laws.[1078]

Another significant matter that must be taken into account involves the arrangements between the Security Council and regional organisations. Rule 77 in the Tallinn Manual states that 'International organisations, arrangements, or agencies of a regional character may conduct enforcement actions, involving or in response to cyber operations, pursuant to a mandate from, or authorisation by, the United Nations Security Council.'[1079] It can be seen that the rule used the term mandate and authorised by the UNSC. The terms 'mandate' and 'authorisation by the UNSC' have distinct meanings. When the Security Council mandates a measure, it indicates that it designates a specific entity to conduct operations. Security Council authorisation means that a state or regional organisation conducts an operation pursuant to the Security Council authorisation,[1080] such as the measures taken by an ad hoc coalition according to the Security Council authorisation.[1081]

In the context of authorising force, it is significant to distinguish between the UNSC's 'peacekeeping' and 'peace enforcement' operations.[1082] A peacekeeping operation needs to meet several conditions.[1083] First, the territorial state must provide consent. Second, the impartiality principle must be implemented, particularly when it involves more than one state, such as in the monitoring of a ceasefire.[1084] The peace operation needs to be within the scope of the mandate or authorisation of the operation and its object and purpose.[1085] For instance, if the operation's scope is to monitor a ceasefire, the scope will be exceeded if a cyber operation is conducted

[1077] Ibid 358.

[1078] Ibid 368.

[1079] Ibid 360.

[1080] Ibid 361.

[1081] Ibid.

[1082] Ibid.

[1083] Ibid.

[1084] Report of the Special Committee on Peacekeeping, UN Doc. A/57/767, para. 46 (29 March
2003).

[1085] Tallinn Manual 2.0., (2017), 362.

on behalf of one state against another.[1086] On the other hand, in the case of peace enforcement, none of the three conditions are required. However, forceful measures authorised or mandated by the UNSC need to be necessary to achieve the mission's objective.[1087] Moreover, any cyber operation necessary to achieve the Security Council's mandate or authorisation will be lawful.[1088] For example, the use of a cyber operation to pinpoint targets in a peace enforcement operation would be legal. Another issue may arise in regard to either the scope of the mandate or authorisation if the Security Council does not expressly permit the use of force yet, the peace force needs to initiate a cyber operation — an operation that may rise to the level of use of force. As an example, a group, in social media, indicates violence against another ethnic group and the peace force needs to use cyber means against them.[1089]

The Tallinn Manual states that all United Nations force installations, materials, units, and vehicles should be protected and are not permitted to be targeted by cyber-attacks.[1090] Moreover, the Manual also notes that 'Other personnel, installations, material, units, or vehicles, including computers and computer networks, involved in a humanitarian assistance or peacekeeping mission in accordance with the United Nations Charter are protected against cyber-attack under the same conditions.'[1091] These statements also apply to a non-United Nations force that is providing assistance to a United Nations peace force, as the non-UN force is supporting the UNSC in achieving its peace force objective.

[1086] Ibid.

[1087] Ibid.

[1088] Ibid 364.

[1089] Ibid 365.

[1090] Ibid Rule 79, 368.

[1091] Ibid.

5.4 The UNSC's political realities and implications for cyber

Having established what the founding document of the United Nations, the UN Charter, envisioned for its most powerful organ, and how the Council could both react and use cyber, it remains to be analysed how this could work in practice.

While cyber-operations could easily be considered a threat to the peach, breach of the peace or act of aggression if they have the same kinetic energy of destruction like more conventional weapons, political realities also come into play. The Council with its five veto powers is vulnerable to the veto and indecision. While the veto had already been controversial at the 1945 San Francisco conference, it remains enshrined in the Charter and arguably complicates the work of the Council.[1092]

Both during the Cold War, and – after a brief period of action in the 1990s and early 2000s, the Council mostly was locked down due to the veto and political interests of the countries holding it. The veto could only be reformed if all permanent members agree – hence, it has not happened yet. Unsurprisingly, no current P5 member state wishes to lose its status and power.[1093]

So, how are the interests of the P5 affected by cyber? Most notably, three of the five permanent members, China, Russia, and the USA have their own interests and are themselves actively engaging in cyber operations. Since 2020, Chinese state-linked hackers have been actively exploiting US networks and continue to consistently engage in offensive cyber-operations. Costello, former US chief of staff, Office of the National Cyber Director, in an interview with Atlantic Council said: 'As reported by the Director of National Intelligence in the last few years, China has increasingly turned towards targeting US critical infrastructure, particular natural gas pipelines. This is an evolution, though whether it is 'learning by doing, 'operational preparation of the battlespace, or nascent ventures by a more operationally focused Strategic

[1092] Christian Wenaweser & Sina Alavi, Innovating to Restrain the Use of the Veto in the United Nations Security Council, 52 Case W. Res. J. INT'l L. 65 (2020) 65.

[1093] Ibid.

Support Force (reorganization into a Space and Cyber Corps from 2015-17) is unclear.'[1094]

However, the US has its own interests relating to cyber. Most successfully, it used cyber-means to infiltrate ISIS and brought parts of their online network down in August 2015.[1095] The US has enormous military and civilian cyber capabilities, having cyber units in all branches of their military, as well as in their police and security services. In its 2023 Annual Threat Assessment of the U.S. Intelligence Community, it identified China, Russia, Iran, and North Korea as threats. For all four countries, it also identified possible cyber threats.[1096] Not least due to this, the US is likely wary to commit to any rules or issue any resolutions that could inhibit its own capabilities against identified threats.

Russia, the last P5 with an increased interest in cyber, has most notably used cyber means in its aggressive war against Ukraine and demonstrated how cyber can be used to supplement conventional military means.[1097] NATO Stratcom identifies Russian cyber interests as: "From the Russian perspective, cyber warfare or the Russian equivalent 'information- technological warfare,' is only a part of the overarching concept of "information confrontation" (informatsionnoe protivoborstvo). The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence.'[1098] Russia has for years used cyber terms to influence elections in western countries and also during warfare. Not only in Ukraine, but also in the Second

[1094] https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

[1095] https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

[1096] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[1097] https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command.

[1098] https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

Chechen War in 1999, and the Russo-Georgian War in 2008.[1099] It is clear, therefore, that Russia has used cyber against other states for years for their own political interests. It should not be surprising that it does not want any decisive UNSC resolution defining, prohibiting, or limiting cyber means.

5.5 Conclusion

With reference to the discussion in this chapter concerning Security Council interventions, it should be noted that maintaining international peace and security may require the use of both forceful and non-forceful measures. Moreover, the UNSC has broad authority to classify any situation as a threat pursuant to Article 39 of the UN Charter. After classifying an act as a threat, the Security Council may choose appropriate measures to intervene, including economic, political, or military interventions. Militarily, this could involve the authorisation of peacekeeping forces or an international or regional organisation appointed by a member state. Regarding cyber operations, the classification of the cyber act depends on its severity and its impact on peace and security. As per Article 41 of the UN Charter, the Security Council has the authority to decide the 'necessary measures,' meaning that the Council could use cyber operations to maintain the required peace and security. Based on the discussion earlier, it should be noted that the Security Council has not yet determined expressly that cyber-attacks are a threat to the peace and security. However, because of its authority, the Council could do so any time. Moreover, the severe consequences that may result from a cyber operation, such as compromised power grids, water supplies, and disrupted flight signals, would undoubtedly constitute a threat. Furthermore, the Security Council could mandate or authorise the use of such measures by a regional organisation; while these could be cyber measures, the organisation should respect the mandate or authorisation scope and work within it. Irrespective whether the measures are taken by the Security Council itself or by a regional organisation, it is necessary to comply with human rights rules

[1099] Ibid.

and international humanitarian law. The experts in the Tallinn Manual concluded that any cyber measures should comply with the object and purpose of the mandate or authorisation. All in all, the Security Council can use a cyber operation as a measure as required by the situation, whether the international threat is a cyber threat or a kinetic threat achieved by cyber means. This answers one of the main questions of this thesis: the possibility that the Security Council may use a cyber operation as a measure to maintain peace and security. However, as section 5.4 showed, most prominently China, Russia, and the US have their own political interests that make it due to the veto unlikely that the Council will take any decisive action in relation to cyber.

CHAPTER 6: CONCLUSION AND FINAL FINDINGS

6.1 Conclusion

Even though the cyber domain is a new battlefield which comes with new challenges and requires an urgent attention at the international level, I would argue that, in the absence of formal UN regulations on cyber warfare and cyber operations, the thesis proved that countries can apply the traditional rules for determining whether an armed conflict exists (*jus ad bellum*) to this new act. This thesis provided a detailed study on how to apply the law on the use of force (*jus ad bellum*), specifically Articles 2 (4) and 51 of the UN Charter, to cyber operations. The thesis focused on how international law can address cyber conflict in the light of the meaning of 'use of force' in Article 2 (4), and how, based on Article 51, states could act in self-defence against cyber-attacks.

It has been demonstrated in Chapter Two that the prohibition of the use of force has many related principles such as the right to self-defence which is an exemption of the prohibition of the use of force. Even though, the right of self-defence is a natural right, there are some conditions that need to be met which have been discussed in said Chapter. Furthermore, it has been observed that even an authorised use of force is not permitted without some restrictions which show how international law aims to limit the use of force as far as possible, even in otherwise lawful ways. Moreover, Chapter Two showed that anticipatory self-defence has not been approved by international law. However, the state practice determined the opposite, especially in the states' fights against terrorism. In regard to the non-intervention principle, any contravention of the use of force will also include a non-intervention violation, but not every contravention of the non-intervention principle will be an armed attack or even a use of force. Chapter Two therefore provided an overview of the current international law in regard to the legality of use of force, and it demonstrated also many states positions about this matter. A focus, according to the thesis' scope, was laid on Saudi Arabia.

Most important was Chapter Three, which determined that cyber operations which cause injury or death to humans or physical damage to property violate the prohibition of the use of force. The thesis was in favour of following the target-based

approach when deciding the force character because Saudi Arabia and many other states have a clear definition of it. The author favoured this approach because a clear definition leaves no room for misunderstanding, which ensures that every state can apply this approach in the same way. While the Tallinn Manual and some authors such as Schmitt agreed on the consequences-based approach which relies on the effect of the cyber operation, the uncertainty of this approach seems less favourable. Chapter Three further demonstrated that the weapons used in cyber space are malware and viruses. While all of them are virtual and not physical weapons, they can still meet the definition of 'weapon'. This deduction has been reached by the ICJ when the court concluded that it will consider any weapon currently available or those who will come available in the future as war equipment, this clearly applies to cyber methods.

Chapter Three further argued that to trigger the right of self-defence against a cyber operation can only be triggered against an act that is equivalent to an armed attack based on the scope and effect criteria. This means that any use of force that injures or kills persons or damages or destroys property is an armed attack. On the other hand, non-destructive cyber operations, such as cyber theft or intelligence gathering, do not rise to the level of an armed attack and consequently cannot trigger the right to use self-defence. When a cyber-attack is launched in several small-scale operations, the thesis argued in favour of classifying this as an armed attack as long as these cyber-attacks combined cause the same damage and effect to the state as one individual cyber-attack. As a result, to protect the state from such cyber operations and provide the legal grounds for the state to respond, it has the right to use self-defence because the accumulation of cyber-attacks constitutes an armed attack as well. Also, this chapter determined that a cyber-attack launched by a non-state actor would amount to an armed attack if it is directed by or on behalf of a state, except in the case of terrorist involvement which has some disagreement about it.

For the aim of this thesis, the author supports in Chapter Three "the last window of opportunity" standard for assessing the imminence of the cyber operation. The reason for favouring this standard is that it allows anticipatory self-defence against the cyber-attacks. The author believes anticipatory self-defence is necessary for any meaningful and effective defence in the cyberspace. Any state needs to be able to

defend itself against a cyber-operation that could happen in seconds. Despite all the criticism of cyber anticipatory self-defence, there is still a need for it because the targeted state will find itself in a situation in which it has no choice but to respond by anticipatory self-defence to protect its infrastructure or its territory as a whole.

Chapter Three demonstrated that cyber acts which do not rise to the use of force and armed attack could still be considered a violation of international law when it violates the non-intervention principle. The cyber operation amounts to an intervention whenever it satisfies the coercion element. The non-intervention principle is deeply connected with the state sovereignty principle. It has been argued in this chapter that the cyber space is also protected by state sovereignty. The chapter concluded that the state has a sovereign authority over its cyber space, which allows the state to regulate the cyber activity on its territory and take measures to protect that territory. That protection also comes from the due diligence obligation, which requires the state to take whatever measures needed to maintain its territory and guarantee it to not be used illegally.

It can be noted that international law principles are like a chain – one element follows another. When the act violates the use of force or non-intervention, it will also violate sovereignty. As a result, there will be an international responsibility. Afterwards, the state can respond with self-defence or countermeasures. And in all cases if the state is a non-state actor, there will be an assessment for state involvement based on the “unable or unwilling” criterion. If a state does not carry out its due diligence obligations, the state will be found responsible even if the perpetrator is a non-state actor. Consequently, the victim state can use countermeasures to pursue that state to honour its obligation to prevent its territory from being used illegally. As demonstrated in Chapter Three, countermeasures are the most suitable way to act immediately against a cyber-attack because they do not rise to the level of use of force and can protect the state infrastructure from the fast and immediate effect of the cyber operation without any delays.

Moreover, Chapter Three concluded that if the state’s “essential interest” face “grave and imminent peril” and the sole means of averting that peril is temporary non-compliance by the State with its international obligations of “lesser weight or urgency”, the victim state is allowed to rely on the plea of necessity to protect its

interests from cyber operations. The plea of necessity is available in exceptional circumstances when the state's interests are in danger. Therefore, the use of force could be available in the case of cyber operations against a state's interests when the use of force is the only option to protect the state's interests and when there will be a huge harmful effect to the state if the state does not use force to defend its interests.[1100] This is because acting in response is an inevitable act to protect the state from harm, but acting before the harmful cyber operation has been launched to make sure the state's territory is not used in any illegal manner is an instance of correct due diligence. In other words, the right to respond is a mirror of the obligation to prevent.

State practice proves that states will treat Article 2 (4) as just one of several factors to consider when characterising cyber-attacks. Consequently, that creates a shift in the international paradigm regarding the "use of force". This study identified a number of examples of State practice regarding cyber-attacks and analysed them in Chapter Four based on the international legal principles which have been illustrated in chapters two and three. These cyber incidents were the Estonia DDoS attacks, the Stuxnet Malware incident, and the Aramco hacking of the refineries and oil production centres. They have presented an overview of how to apply international law rules to these cyber-attacks. Each case illustrates the technical difficulties of attribution of malware in cyber-attacks, which leads to difficulties in determining the international responsibility. Furthermore, state practice has provided a guidance to apply the current rules of use of force, which, however, needs more analysing and examining to fill in the gaps which arise particularly from technical issues such as allocating the source of the attack. By examining the type of the attack and its effect on the state's critical infrastructure or its national peace and security, it is evident that the cyber coercion is prohibited based on international community consensus.

Furthermore, the thesis deduced from examining Security Council interventions in Chapter Five that as per Articles 41 and 42 of the UN Charter, the Security Council has the authority to decide the 'necessary measures,' meaning that the

[1100] Gill, Terry D. and Tibori-Szabó, Kinga, Twelve Key Questions on Self-Defence against Non-
State Actors – and Some Answers, Ibid, 494 et seq.

Council could use cyber operations to maintain the required peace and security. The assessment of the cyber act is based on its severity and its impact on peace and security. Even though the Security Council has not determined expressly that the cyber-attack is a threat to international peace and security, they could do so on any occasion. The harsh consequences that may result from a cyber operation, such as compromised power grids, water supplies, and disrupted flight signals, would undoubtedly constitute a threat to international peace and security. The thesis's finding is therefore that the Security Council can use a cyber operation as a measure if required by the situation. Whether the international threat is a cyber threat or a kinetic threat achieved by cyber means is immaterial, as the UNSC's powers apply to either situation.

The thesis concluded that to start applying *jus ad bellum* in the cyber context, every state should at first develop a clear position about the relevant principles and provisions related to *jus ad bellum* such as the coercion scope, infrastructure definition, anticipatory self-defence and the imminency level required to invoke a plea of necessity and much more which is clarified in the thesis. Moreover, every state should work to find a way to correctly attribute cyber-attacks, which cannot be done without professional technical efforts. The thesis reached more findings in regard to Saudi Arabia's cyber strategy, which will be presented below.

6.2. Required Improvement in Cyber Security Strategy of Saudi Arabia

After the Aramco cyber-attack in 2012, Saudi Arabia began developing its cyber capability. It started with re-formulating a National Information Security Strategy.[1101] Besides many other improvements in the cyber field, Saudi Arabia has established many institutions for maintaining Saudi cyber security. These include a newly established National Cybersecurity Authority, the Saudi Federation for Cybersecurity, Programming and Drones, and the Prince Mohammed bin Salman College of Cybersecurity, Artificial Intelligence and Advanced Technologies. This strategy addresses many important topics and issues, such as establishing a National IS

[1101] Developing National Information Security Strategy for the Kingdom of Saudi Arabia NISS, DRAFT 7, (2011),

Policy and Directive Issuance System the National IS Risk Assessment Function (NRAF) and the National Risk Process Management System (RPMS). The objective of this strategy is to increase and improve information security education, as well as information security training. Further, its goal is to expand and improve information security awareness and promote and emphasise the concept of shared responsibility. Furthermore, it is aimed at strengthening the Kingdom's national technical capabilities, combating cyber-crime, and expanding research and innovation through international co-operation.

The strategy includes a “policy gap analysis process” to comply with Saudi laws and regulation in the cyber domain.[1102] Following an analysis, the Saudi government concludes that there are some challenges in this regard which are:

“1) Emerging threats against the Kingdom’s critical infrastructures and key resources that expand gaps against intended security objectives, as well as the policies and laws put into place to close those gaps.

2) Constant monitoring of new threats against in-place and emerging policy issues is essential to maintaining a secure environment…”[1103]

To illustrate, the strategy has been explained in a detailed table, which can be found below.

[1102] Ibid, 31.

[1103] Ibid

Compliance Requirement	National-Level Considerations	Corresponding KSA Law or Regulation	Suggested Action
Incident Response Policy and Procedures	Baseline incident response procedures involving national level reporting (e.g. National Level Incident Reporting Database)	Cabinet Circulate 16-5-1432	Define and disseminate incident reporting of cyber-events to a National level database. Ensure data is shared throughout KSA Agencies to prevent attack, or reduce the impact of an attack.
The Arab League Convention To Combat Cyber Crimes	Adherence to and participation in the International Cyber Crimes Convention	Anti-Cyber Crime Law	Ensure cyber-crime laws are consistent with international standards, and that co-operative agreements are in place with other Nations to ensure cyber criminals are captured and brought to justice

Table 2 : High-level Gap Analysis of National Level Policies, Laws and Regulations

The strategy contains a long and detailed table on the "High-level Gap Analysis of National Level Policies, Laws and Regulations".[1104] For the aims of this thesis, and in the current context, just two elements thereof have been quoted. The first one is the incident response policy and procedures, which is regulated by a Cabinet Circulate. However, this regulation does not mention which cyber-attack invites a legal response, nor how to classify the cyber operation as an attack . It just explains

[1104] Ibid, 26-29

the procedures to follow in the case of a cyber-attack.[1105] The second element is complying with the international cyber-crime regulations and participating in convention about cyber-crimes either internationally or regionally in the Middle East.

To fill the gaps, Saudi Arabia could get some inspiration from the United States, as they have similar approaches to their interpretation of cyber-attacks, and other similar legal classifications (as was discussed previously). The US Department of Defence adopted a cyber strategy which states that "The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law and consider economic sanctions."[1106] The United States' strategy makes it clear how they intend to respond, and it takes into account both the timing and the instrument used.

As mentioned before, Saudi Arabia does not have a separate strategy for cyber-defence. Moreover, it did not include any statement in the National Cyber Strategy about the legal response to a cyber-attack or an explicit phrase with regard to the Saudi intention – however, their response would likely be similar to the US. This underlines again that the Saudi government would benefit from using the US strategy as a guide. Furthermore, the United States DOD cyber strategy illustrates the importance of solving attribution issues in cyber operations due to the anonymity of state and non-state actors in tracking cyber-attack origin. It explains the significance of investing in "all source collection, analysis, and dissemination capabilities."[1107] The reason for making attribution a priority concern is because it is vital "to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics techniques, and procedures."[1108] This explains why it is also necessary to include a similar provision in the Saudi Cyber Strategy. Additionally, the US DOD cyber strategy views cyber operation in some situations as reasonable grounds to respond with military force.[1109] Also, it allows for the possibility to respond

[1105] Cabinet Circulate 2984 /M B, 1432 Hijrah.

[1106] The US Department of Defence Cyber Strategy, (2015), 11.

[1107] Ibid 11-12.

[1108] Ibid.

[1109] Ibid.

in non-military ways depending on the situation and the degree of the threat to the national security, such as diplomatic action or economic sanctions.[1110]

To illustrate how well the US's cyber strategy works, the author will briefly discuss a cyber incident against the US: the United States detected a Chinese espionage operation, which led to some intellectual property theft by China. By using attributable data, the US found out that China is the origin of those thefts. To deter any further data theft, the United States Justice Department "indicted five members of the People's Liberation Army for stealing U.S. intellectual property to directly benefit Chinese companies."[1111] Moreover, these measures helped the United Stated and China to have "consultative talks" which will reduce cyber risks in the future. The aim is to "bring greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace."[1112] That step will build trust in the cyber domain between the US and China. This is certainly a better way forward than the situation deteriorating in cyber conflict.

Such a strategy could also be adopted between Saudi Arabia and Iran, as they also have a cyber history between each other. This is true, especially after the Aramco attack, which has been illustrated previously in the thesis.[1113] However, Saudi Arabia needs to use more attribution sources and tools to confirm the origin of the cyber-attack. Then, Saudi Arabia should start to have "consultative talks" with the Iranian side. This could be a diplomatic method to develop a safer cyber space between the two countries. The DOD cyber strategy sets the goal for this: "The goal of this work is to reduce the risks of misperception and miscalculation that could contribute to escalation and instability."[1114] This can be used as guidance for Saudi Arabia to improve its strategy, as it still has not adopted one yet.

Another challenge facing states in the cyber security field, are "transnational criminal groups". Such groups are defined as organised criminals which are co-ordinated across national borders, involving groups or markets of individuals working

[1110] Ibid.

[1111] Ibid.

[1112] Ibid.

[1113] See page 178

[1114] The US Department of Defence Cyber Strategy, 13.

in more than one country to plan and execute illegal business ventures."[1115] Cyber tools make it easy for such a group to undertake its criminal activities because of the nature of cyber operation, which can be launched remotely from abroad. Therefore, the United States National Cyber Strategy stated that "The Administration will advocate for law enforcement to have effective legal tools to investigate and prosecute such groups and modernized organised crime statutes for use against this threat."[1116] Then, the strategy explained how to do that and hot to facilitate international co-operation to protect its national security from those criminals. It states that:

"The United States will continue to identify gaps and potential mechanisms for bringing foreign based cyber criminals to justice. The United States Government will also increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests."[1117]

It is clear from that statement that the United States have a restricted approach to fighting transnational crime groups because some of them have a sophisticated capability which can be similar to state capability. These groups could conduct a massive breach to the financial system, steal classified information, conduct intellectual property theft and much more.[1118] This issue has not been included in the Saudi Cyber Strategy at all. Due to the threat coming from organised criminal groups, it is highly recommended to include a similar policy in the Saudi strategy.

From the above-mentioned comparison, Saudi Arabia's unique and distinct challenges are as follows:

[1115] Yuriy A. Voronin (2000). "Measures to Control Transnational Organized Crime, Summary" .
National Criminal Justice Reference Service (NCJRS). U.S. Department of Justice. Document
No. NCJ 184773.

[1116] National Cyber Strategy of the United States of America, 2018, 21.

[1117] Ibid 11.

[1118] Ibid.

1. Anonymity and attribution – there is no clear policy for tracking and attributing cyber-attacks

2. The sensitive nature of information within each ministry, development of a trusting environment to share specific information about vulnerabilities, incidents and practices will require strong collaboration

3. High level of confidentiality, which makes it hard to improve and study the cyber-attacks against Saudi infrastructure

4. Isolated technical experts without input from legal experts

5. The improvement plans exist more on papers than in practice

6. There is no official document which lists the cyber-attacks and how Saudi would respond to them

Moreover, Saudi Arabia does not have a clear position about cyber warfare or the use of force in this cyber context. Also, there is a lack of legal statements and regulation in the Saudi Cyber Strategy. As it stands, it is all about co-operation between the private and governmental sector and how to do risk management and implement some administration and technical strategies.

It has been suggested above that the Saudi Cyber Strategy needs more improvement in legal terms. Moreover, Saudi Arabia needs to draft a distinct cyber defensive strategy.

6.3. Recommendations

Following the previous analysis, it can be concluded that there are several recommendations for Saudi Arabia's government. These are:

- Saudi Arabia has a very sophisticated technology and has the ability to protect and deter its infrastructure sufficiently, but all that cannot be done without a clear legal framework and cyber strategy.

- The Ministry of Defence in Saudi Arabia needs to work on a cyber strategy, especially concerning legal defensive rules, which must comply with the international law rules and regulations in the context of the right of self-defence. Moreover, short of using self-defence, the strategy must address using the countermeasures to protect the Saudi infrastructure from cyber-attacks.

- The Ministry of Defence in Saudi Arabia must clarify its position regarding anticipatory self-defence in the cyber context.

- The co-ordination between technological and legal experts is urgently required. Only such co-operation can solve legal issues while keeping appraised of technical facts and capabilities. An example is the attribution problem in the case of a cyber-attack.

- The Saudi government should issue a periodic legal report about cyber-attacks which attack Saudi infrastructure. It will help the national legislature in adopting any cyber rules and will clarify many legal issues for the researchers. Moreover, it will serve as a reference of state practice to be used internationally or in the event of developing a new cyber treaty.

- Further research on the attribution issue for cyber-attack incidents is necessary. Moreover, studying the requirements and the criteria to classify cyber-attacks according to the international law rules also needs to be done.

6.4. Further Research

- Is an “attempted threat “prohibited by the intervention principle? This would lead us to an “attempted use of force” which is of a higher degree than the attempted threat. This area of concern has neither been discussed in the Tallinn Manuals nor amongst Scholars. Therefore, this needs to be elaborated on.
- It has been noted that the criterion to identify an armed attack which is drawn from Rule 71 is “the scale and effect”.[1119] This criterion was derived

[1119] Nicaragua Case, 195.

from the ICJ judgement in Nicaragua, as identified previously.[1120] The Group of Experts in the Tallinn Manual adopted this view when assessing the concept of armed attacks in cyber operations, and they consider this criterion as an unsettled matter.[1121] Therefore, this needs further research.

- The definition of 'critical infrastructure' is not universal. However, a commonly agreed upon definition is essential. Therefore this needs to be elaborated on.[1122]
- One aspect of coercion which still has not been settled is the causality of the coercion effect. The majority of the Experts are in favour of the view that the existence of a casual nexus between the act and the effect is sufficient for it to be considered an intervention within internal or external affairs. This needs more research.
- There is no consensus on what level of imminency needs to exist to invoke a plea of necessity, and therefore further research is necessary.
- More studies about solutions for the attribution problem in the cyber domain are urgently needed.

[1120] Ibid.

[1121] Tallinn Manual 2.0.,341.

[1122] The GGE report also recognises this without defining critical infrastructure: Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (2021), 7.

APPENDIX

Constitutional law				
Fundamental rights and freedoms; Organisation of the state; Execution of public authority				
Private law	Public administrative law	Criminal law	Crisis management law	War-time law / national defence law
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e-services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

Compliance Requirement	National-Level Considerations	Corresponding KSA Law or Regulation	Suggested Action
Incident Response Policy and Procedures	Baseline incident response procedures involving national level reporting (e.g. National Level Incident Reporting Database)	Cabinet Circulate 16-5-1432	Define and disseminate incident reporting of cyber-events to a National level database. Ensure data is shared throughout KSA agencies to prevent attack, or reduce impact of an attack.
The Arab League Convention To Combat Cyber Crimes	Adherence to and participation in the International Cyber Crimes Convention	Anti-Cyber Crime Law	Ensure cyber-crime laws are consistent with international standards, and that cooperative agreements are in place with other Nations to ensure cyber criminals are captured and brought to justice

Table 2 : High-level Gap Analysis of National Level Policies, Laws and Regulations

BIBLIOGRAPHY

Laws

Committee on Offensive Information Warfare, The Legal Framework Governing Cyberattack.

Diplomatic and Consular Premises Act 1987 (from 15th May 1987, Ch 46) at https://www.legislation.gov.uk/ukpga/1987/46

Developing National Information Security Strategy for the Kingdom of Saudi Arabia, NISS draft 7

Estonian Government, 'Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian)'. Estonian Government 2010. <http://www.riigikogu.ee/page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise side muutmine seletuskiri (424).doc&file_size=31650&mnsensk=424+SE&fd=

French Ministry of the Armies, International Law Applied to Operations in Cyberspace, (2019)

Treaties

Alabama claims of the United States of America against Great Britain, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Volume XXIX, pp. 125-134,130

Draft Convention on the international responsibility of states for injuries to aliens, Reprinted in Louis B. Sohn & RR

General Treaty on the Renunciation of War as an Instrument of National Policy (1928)

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10),

chp.IV.E.1, available at: https://www.refworld.org/docid/3ddb8f804.html [accessed 14 November 2019]

NATO, Cyber Defence North Atlantic Treaty Organization (16 July 2018) https://www.nato.int/cps/en/natohq/topics_78170.htm

UN, Charter of the United Nations and statute of the International Court of Justice (2015)

Vienna Convention on the Law of Treaties, Article 31(1), 1155 U.N.T.S. 331, (1969)

Cases

Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 July 2004, available at: https://www.refworld.org/cases,ICJ,414ad9a719.html

Advisory Opinion Concerning the Legality of the Threat or Use of Nuclear Weapons (Request for Advisory Opinion by the General Assembly of the United Nations)' (1996) ICJ https://www.refworld.org/cases,ICJ,3ae6b67f14.html

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits, Judgement of 19 December 2005 [2005] ICJ Rep

Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America) (2003) ICJ https://www.refworld.org/cases,ICJ,414b00604.html

Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Yugoslavia), ICJ (1996)

Corfu Channel, 'United Kingdom v Albania, Judgement, Merits' (1949) ICJ

Gabčikovo-Nagymaros Project, Hungary v Slovakia, Judgement, Merits, ICJ GL No 92, (1997)

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) (1996) 35 ILM 809

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement of 27 June 1986 [1986] ICJ Rep 14 Nicaragua v. USA [1986] ICJ Rep 14

Philippines v China, PCA case no 2013-19, (12 July 2016)

Société Commerciale de Belgique (Belg. v. Greece), Judgement, 1939 P.C.I.J. (ser. A/B) No. 78, at 160 (June 15).

UN Documents & other legal documents and reports

'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations' (1970) COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Definition of Aggression On 14 December 1974, the General Assembly adopted by consensus resolution 3314 (XXIX)

Deutscher Bundestag, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE", BT-Drs. 18/6989, (2015)

Developing National Information Security Strategy for the Kingdom of Saudi Arabia (NISS draft 7)

General Assembly 35th session, U.N. Doc. A/35/10 (Supplement No. 10), at 84 (1980)

Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace, 26 September 2019

ILC commentary on the Articles on State Responsibility

Office of General Counsel, An Assessment on International Legal Issues in Information Operations, United States Department of Defence (1999) www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

Office of The President, International Strategy for cyberspace, (2011)

President of Estonia, Kersti Kaljulaid, 'President of the Republic at the opening of CyCon 2019' (29.05.2019)

QATAR National Cyber Security Strategy (May 2014)

Report of the Special Committee on Peacekeeping, UN Doc. A/57/767, (29 March 2003)

Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly, (June 7, 2013) http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

SC Res 1078 (1996)

SC Res 1172, 6 June 1998 on nuclear proliferation

SC Res 1737 (2006)

SC Res 1747 (2007)

SC Res 1803 (2008)

SC Res 1929 (2010)

SC Res 748 (1992)

SC Res 793 (1992)

SC Res 929 (1994)

SC Res 1373

SC Res 1540

Security Council 2491st Meeting (1983)

Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations (Cambridge 2017)

Tallinn Manual on the international law applicable to cyber warfare 2013 (2013

The Charter of the United Nation: A commentary

UN Doc. S/RES/1540 (28 April 2004)

UN Doc. S/RES/2001 (28 September 2001)

United Kingdom Foreign, Commonwealth & Development Office, Application of international law to states' conduct in cyberspace: UK statement, 3 June 2021

United Nations, 'Identical letters dated 19 May 2015 from the Permanent Representative of Qatar to the United Nations addressed to the Secretary-General and the President of the Security Council' (2015)

Literature

Abokhodair N and Z Dehlawi, Saudi Arabia's Response to Cyber Conflict: A case study of the Shamoon malware incident (IEEE 2013)

Albright D and J Shire, 'IAEA Report on Iran: Fordow enrichment plant at "advanced stage of construction;" decline in number P1 centrifuges enriching but P1 centrifuge efficiency increases; discovery of previously unknown stock of heavy water' (Institute for Science and International Security, 16 November 2009)

Albright D, P Brannan, and C Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?' (Institute for Science and International Security, 22 December 2010)

Albright D, P Brannan, and C Walrond, 'Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report' (Institute for Science and International Security, 15 February 2011)

Andrzej K, 'Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan' European Scientific Journal (2014), 10.7, 238

Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF U.S. PRACTICE IN INTERNATIONAL LAW, ch 18, § A(3), at 13, https://www.state.gov/documents/organization/244486.pdf [https://perma.cc/5VDX-2M7X]

Aynalem F and K Vibhute, Legal Research Methods (JLSRI 2009)

Babbage, ‘The Stuxnet worm: A cyber-missile aimed at Iran?’ (The Economist, 24 September 2010) https://www.economist.com/babbage/2010/09/24/a-cyber-missile-aimed-at-iran
Bailliet CM and S O’Connor, ‘The good faith obligation to maintain international peace and security and the pacific settlement of disputes’ In Research Handbook on International Law and Peace (Edward Elgar Publishing 2019)
Baladze M, "LEGAL GROUNDS OF USING ARMED FORCES IN MODERN INTERNATIONAL LAW."
Banks W, ‘State Responsibility and Attribution of Cyber Intrusions after Tallinn’ (2017) 95 Tex L Rev 1487
Bannelier-Christakis, K, Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, Baltic Yearbook of International Law, Vol. 14 (2014)
Baradaran A and H Habibi, 'Cyber Warfare and Self-Defence from the Perspective of International Law' (2017) 10 J Pol & L 40
Bartelson J, A Genealogy of Sovereignty (Cambridge University Press, 1995)
Basu S, "Gender as national interest at the UN Security Council." International Affairs 92, no. 2 (2016): 255-273.
Baxter, Responsibility of states for injuries to the economic interests of aliens 55 AM. .J.INT’L L. 548
Beidlemen S, Defining and deterring cyber war' Strategy Research Project (U.S. Army War College 2009)
Bergwik, M., Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0, UPPSALA Universitet, Mater Thesis, 2020
Bethlehem D, ‘Principles Relevant to the Scope of a State’s Right of Self-Defence Against an Imminent or Actual Armed Attack by Non-State Actors’ (2012) 106 AJIL 5
Bethlehem D., Self-Defence Against an Imminent or Actual Armed Attack by Nonstate Actors, 106 AM. J. INT’L L.
Bright A, ‘Estonia accuses Russia of ‘cyberattack’ The Christian Monitor 1 November 2016) http://www.csmonitor.com/2007/0517/p99s01-duts.html
Bronk C and E Tikk-Ringas, ‘The Cyber-Attack on Saudi Aramco’ (April 2013) IISS www.iiss.org/en/publications/survival/sections/201394b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08bronkandtikk-ringas-e272
Byers M, ‘Terrorism and international law after 11 September’ (2002) 15 ICLQ 406
Camilla Gambarini, ‘Due Diligence,’ (Jus Mundi, 4 June 2021). < https://jusmundi.com/en/document/wiki/en-due-diligence-1>
Carr J, Was Iran Responsible for Saudi Aramco’s Network Attack, Digital Dao, (2012)

Carr J, Who's Responsible for the Saudi Aramco Network Attack?, Infosec Island, 2012.
U.S. says Iran behind cyber-attack in Saudi Arabia, Alarabyia News, 2012.
Caso J, 'The Rules of Engagement for Cyber-Warfare and the Tallinn Manual: A Case Study' The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems June 4-7, 2014, Hong Kong, China
Charpak C, International Law and Diplomacy (Routledge 2007)
Chatham House, 'Principles of International Law on the Use of Force by States in Self-Defence ' (2005) 31
Christian C, R Ottis, and A Talihärm, 'Estonia after the 2007 cyber-attacks: Legal, strategic and organisational changes in cyber security' International Journal of Cyber Warfare and Terrorism (2011) 1.1, 24
Courtney M, 'States of cyber-warfare' (2017) 12 ET 22
Crawford J, Brownlie's Principles of Public International Law (9th Edn, Oxford University Press 2019)
Crawford JR, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries (Cambridge University Press 2002)
CSIS, 'Significant Cyber Incidents' (Center for Strategic and International Studies, 2019) <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity>
Cullen M, "Questioning the Criminal Justice Imperative: UN Security Council Procedure and the Downside of Chapter VII Decision Making for the Adjudication of International Crimes." Global Governance: A Review of Multilateralism and International Organizations 25, no. 2 (2019): 327-350
Czossek C., Ottis R. and Ziolkowski K. (eds),4th International Conference on Cyber Conflict Proceedings (NATO CCD COE Publications: Tallinn, 295–309, (2012).
Developing National Information Security Strategy for the Kingdom of Saudi Arabia (NISS draft 7)
Dinniss H, Cyber Warfare and the Laws of War (Cambridge University Press 2012)
Dinstein Y., Computer Network Attack as a Use of Force under Article 2(4), in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell, International Law Studies , Vol.76, (2002)
Dong Y, (2019). The "jus ad bellum" in cyberspace: Where are we now and what next? New Zealand Journal of Public and International Law, 17(1), 41, 41-42
Dubay C, 'A Refresher on the Principle of Non-Intervention' (2014) IJM <http://www.judicialmonitor.org/archive_spring2014/generalprinciples.html>
E Nakashima and S Harris, 'How the Russians hacked the DNC passed its emails to WikiLeaks' (The Washington Post, 13 July 2018).

<https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/>
Ella S, Applicability of International law on Cyber Espionage Intrusions (Stokholm University 2015)
Ellen H, The Regime for the Exploitation of the Transboundary Marine Fisheries Resources: The United Nations Law of the Sea Convention Cooperation between States (Martinus Nijhoff Publishers 1989)
Emanuilov, Ivo. "International (Cyber) security of the Global Aviation Critical Infrastructure as a Community Interest." (2019): 299-342
Farwell J., What does Iran cybar cabaility measn for future conflict?, The Whitehead journal of Diplomacy and International Relation,(2013).52
Fluridi L, Information: A very short introduction (Oxford University Press (2010)
Foltz A, 'Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate' (2012) 67(4) JFQ 40
Forsberg T, Beyond Sovereignty, Within Territoriality: Mapping the Space of Late-Modern (Geo)Politics. Cooperation and Conflict, 31(4), 355-386. (1996)
Frakes J, "The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?" Wisconsin International Law Journal 21, no. 2 (2003): 409-434
Frowein J, Article 39' in B. Simma (ed.), The Charter of the United Nations: A Commentary (2nd edn, Oxford University Press 2002)
Galand, AS. "Was the Residual Mechanism's Creation Falling Squarely within the Chapter VII Power of the Security Council?." Questions of International Law 40 (2017)
Gangale T, How High the Sky? The Definition and Delimitation of Outer Space and Territorial Airspace in International Law, (Brill, 2018), 32.
Giegerich T, Article 57: In the Vienna Convention on the Law of Treaties, (Springer 2018)
Gill TD and PAL Duchene, 'Anticipatory Self-Defence in the Cyber Context' (2013) 89 Int'l L. Stud. 438
Goodman R, 'Cyber Operations and the U.S. Definition of "Armed Attack"' (2018) https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/
Gosnell Handler S (2012), The New Cyber Face of Battle: Developing a Legal Approach to Accomodate Emerging Trends in Warfare, Stanford Journal of International Law
Gray C, International Law and the Use of Force, 4th Ed. (Oxford University Press 2018)
Green JA, Cyber Warfare: A Multidisciplinary Analysis (Routledge 2015)
Green JA, The International Court of Justice and Self-Defence in International Law (Bloomsbury Publishing Plc 2009)

Green LC, United Nations operations: In The contemporary law of armed conflict (Manchester University Press 2018)
Greenwood C, ‘International Law and the Pre-Emptive Use of Force: Afghanistan, Al-Qaida, and Iraq’ (2003) 4 San Diego Int’l L.J. 7
Greenwood C, ‘International Law and United States Air Operations against Libya’ 89 West Virginia LR 933
Grosswald L, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, 36 Brook. J. Int'l L. (2011).Available at: https://brooklynworks.brooklaw.edu/bjil/vol36/iss3/11
Haataja S, ‘The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach’ Law Innovation and Technology (2017), 9 2
Hankinson, O, Due Diligence and the Gray Zones of International Cyberspace Laws, Michigan Journal of International Law, Volume 39 (2017), Available at: http://www.mjilonline.org/due-diligence-and-the-gray-zones-ofinternational-cyberspace-laws/#_ftn16
Heathcote S, Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity, in J Crawford, A Pellet & S Olleson (ed.), The Law of International Responsibility (Oxford University Press 2010)
Heintschel von Heinegg W, "Territorial sovereignty and neutrality in cyberspace." International Law Studies 89.1 (2013): 17
Helal M, ‘Clouds of War Over the Persian Gulf – A Jus ad Bellum Analysis (Part I)’ (2019) http://opiniojuris.org/2019/06/04/clouds-of-war-over-the-persian-gulf-a-jus-ad-bellum-analysis-part-i/
Helman C, “The World’s Biggest Oil Companies,” Forbes, 07-Sep 2010
Henriksen A, ‘Lawful State Responses to Low-Level Cyber-Attacks’ (2015) 84 Nordic Journal of International Law 323
Hoisington M, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence, 32 B.C. Int'l & Comp. L. Rev. 439 (2009)
Hollis D, Is a Use of Force the Same as an Armed Attack in Cyberspace? (Opinio Juris 2012) <http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armedattack-in-cyberspace>
Hsiu-lien L et al., Case Studies of Contemporary Neutrality Advocacy, in H.R. Reginbogin & P. Lottaz, eds., Permanent Neutrality: A Model for Peace, Security, and Justice (Lexington Books 2020)
Hunter D, "Cyberspace as Place and the Tragedy of the Digital Anticommons." California Law Review 91, no. 2 (2003): 439-519
J Thomson, ‘State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research’ International Studies Quarterly (1995) 39, 217

Jackson J, Sovereignty-Modern: A New Approach to an Outdated Concept, 97 AM. J. INT'L L 782, 785 (2003)
Jamnejad M and M Wood, 'The Principle of Non-intervention' (2009) 22 LJIL 345
Jang-Jaccard J and S Nepal, ‘A survey of Emerging Threats in Cybersecurity’ (2014) 1JCSS 973
Jason J, Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law. (2017), PhD thesis University of Glasgow
Jenik A, 'Cyberwar in Estonia and the Middle East' Network Security (April 2009), 5
Jennings R and Watts A, Oppenheim’s International Law (9th edn, Oxford University Press 1992)
Jensen E, Cyber Sovereignty: A Way Ahead, Ibid, 298–299, V Heinegg, Territorial sovereignty and Neutrality in Cyberspace, 89 International Law Studies 123, 127 (2013)
Jensen E, ‘Cyber Sovereignty: The Way Ahead,’ Texas International Law Journal, 50 (2), (2014), 279
Jiuyong S, ‘Prohibition of Use of Force in International Law’ (2018) 17 CJIL 1
Johnson MC, “The Rising Iranian Cyber Threat” (MediumMarch 23, 2017) <https://medium.com/the-buckley-club/the-rising-iranian-cyber-threat-15028b76e0f9>
Jordan LH, Arms Control and European Security
Kaczorowska-Ireland A, Public International Law, (5th edn., Routledge, 2015), 184
Kaeo M, Founder & Chief Network Security Architect, Double Shot Security, Presentation on Cyber-attacks on Estonia (2007)
Kammerhofer J, The Resilience of the Restrictive Rules on Self-Defence in Marc Weller (ed.), The Oxford Handbook on the Use of Force in International Law (Oxford, OUP 2015)
Kelsen H, ‘Sovereignty and International Law,’ The Georgetown Law Journal, 48 (4), (1960), 627
Kenneth NW, Reductionist and Systematic Theories,’ in Robert Keohane, ed., Neorealism and its Critics (Columbia University Press 1986)
Kittrich J, The Right of Individual Self-Defence in Public International Law, (Logos Verlag, 2008), 177.
Koh H, ‘Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012’ (2012) Harvard International Law Journal 54
Kronenfeld S, Siboni G., Iran and Cyberspace Warfare, Military and Strategic Affairs, Volume 4, No.3, (2012)
Kulesza J, Due Diligence in International Law, (Brill, 2016), 262
Lewis J, ‘Cyber-attacks Explained’ Centre for Strategic and International Studies (2007)

Li S, ‘When Does Internet Denial Trigger the Right of Armed Self-Defence ?’ (2013) 38 Yale Journal of International Law 179
Liaropoulos AN, Cyberspace governance and state sovereignty: Democracy and an Open-Economy World Order (Springer 2017)
Lin H, ‘Offensive Cyber Operations and the Use of Force’ (2010) 4 Journal of National Security Law and Policy 77
Liu, IY, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, 4(2) The Indonesian Journal of International and Comparative Law 191-260 (Forthcoming), Monash University Faculty of Law Legal Studies Research Paper No. 2907662, (January 30, 2017)
Lotrionte C., Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law Author(s), The Cyber Defence Review , Vol. 3, No. 2 (SUMMER 2018)
Lubell N, The Problem of Imminence in an Uncertain World, in The Oxford Handbook of the Use of Force In International Law (2015)
Manthorpe J, Forbidden Nation: A History of Taiwan (St Martin’s Press 2008)
Maogoto J, Rushing To Break the Law? The 'Bush Doctrine' of Pre-Emptive Strikes and the UN Charter on the Use of Force (University of Western Sydney 2003)
Melling G and A Dennett. "The Security Council veto and Syria: responding to mass atrocities through the “Uniting for Peace” resolution." Indian Journal of International Law 57, no. 3 (2017): 285-307
Melman Y, ‘Iran Pauses Uranium Enrichment at Natanz Nuclear Plant’ (Haaretz, 23 November 2010) https://www.haaretz.com/1.5143485
Milevski L, ‘Stuxnet and Strategy: A Special Operation in Cyberspace?’ (2011) 63(4) Joint Force Quarterly 69
Moore A, "Stuxnet and Article 2 (4)'s Prohibition against the Use of Force: Customary Law and Potential Models." Naval L. Rev 64 (2015)
Morgenthau HJ and Thompson KW, Politics among Nations: The Struggle for Power and Peace (Knopf 1985)
Morton Jr LCG, Cyberspace Operations, Stuxnet, jus ad bellum and jus in bello (Air War College, Air University 2013)
Müllerson R, Self-defence against Armed Attacks by Non-State Actors, Chinese Journal of International Law, Volume 18, Issue 4, December 2019
Müllerson R. ‘Self-Defence against Armed Attacks by Non-State Actors’ (2019) CJIL 751
Novosseloff A, The UN military staff committee: Recreating a missing capacity (Routledge 2018)
Ohlin J, Cyber Casuation, in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) Cyber War: Law and Ethics for Virtual Conflicts (Oxford University Press 2015)

Paganini P, ‘Iran Suspected for the Attack on the Saudi Aramco’ (20 Aug. 2012) www.securityaffairs.co/wordpress/8300/malware/iran-suspected-for-the-attack-on-thesaudi-aramco.html
Pank S, ‘What is the scope of legal self-defence in International Law? Jus ad bellum with a special view to new frontiers for self-defence’ (2014)
Pawar MV and J Anuradha, ‘Network Security and Types of Attacks in Network’ (2015) 48 PCS 503
Perlroth N, “Connecting the Dots After Cyber-Attack on Saudi Aramco” (The New York Times2012) <https://www.nytimes.com/by/nicole-perlroth> accessed January 28, 2023
Dipert R, ‘The Ethics of Cyberwarfare’, (2010), 9 Journal of Military Ethics 384
Kertu R, ‘Cyber War I: Estonia Attacked from Russia’ (2008) 9 1-2, European Affairs, 6
Ottis R 'Analysis of the 2007 Cyber-attacks Against Estonia from the Information Warfare Perspective' (Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2008) https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
Radim P and Dan JB, Svantesson, Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law (Edward Elgar 2017)
Raff A, “Shamoon, a Two-Stage Targeted Attack” (Seculert Blog on Advanced Persistent Threats and MalwareAugust 16, 2012) <https://www.avivraff.com/seculert/test/2012/08/shamoon-two-stage-targeted-attack.html>
Rhoads EP, Taking sides in peacekeeping: impartiality and the future of the United Nations (Oxford University Press 2016)
Rid T and Buchanan B, “Attributing Cyber Attacks” (2014) 38 Journal of Strategic Studies 4
Riesman W and J Baker, Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law (Yale University Press 1992)
Roberts A and R Guelff, Documents on the laws of war (3rd edn, Oxford University Press 2000)
Roberts J, ‘Cyber Threats to Energy Security, as Experienced by Saudi Arabia’, Platts, 27 November 2012, http://blogs.platts. com/2012/11/27/virus_threats
Roguski P, France’s Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I (Opinio Juris 2019)
Roscini M, Cyber Operations and the Use of Force in International Law (Oxford University Press 2014)
Roscini M, Cyber operations as a use of force: Research Handbook on International Law and Cyberspace (Edward Elgar Publishing 2015)
Rowe N, The attribution of cyber warfare (Routledge 2015)
Russell A, Cyber Blockades (Georgetown University Press 2014)

Ruys T and L Ferro, ‘Weathering the Storm: Legality and Legal Implications of the Saudi-Led Military Intervention in Yemen’ (2016) 65 ICLQ 61
Ryan DJ, International Cyberlaw: A Normative Approach, 42 Geo. J. Int’l L. 1161, 1185 (2011)
Bartłomiej S, ‘The data embassy under public international law’ International & Comparative Law Quarterly (2019), 68 1, 226
Michael S 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' Columbia Journal of Transnational Law (1999) 37, 1998
Scott S, ‘From nuclear war to net war: analogizing cyber-attacks in international law. Berkeley Journal of International Law (2009) 27 1, 193
Sucharitkul S, State Responsibility and International Liability under International Law, 18 Loy. L.A. Int'l & Comp. L. Rev. 823
Scott S, “Estonia Three Years Later: A Progress Report on” Combating Cyber-attacks (2010), Journal of Internet Law, Feb (2010), 22
Sanger DE, "Obama Order Sped Up Wave of Cyberattacks Against Iran: Officials Cite Wide Effort to Hinder Nuclear Work," New York Times (1923-Current File), (2012). pA1
Schachter O, 'The Right of States to Use Armed Force' (1984) 82 Mich L Rev 1620
Schachter O, ‘In Defence of International Rules on the Use of Force’ (1986) 53 U. CHI. L. REV. 113
Schachter O, ‘Self-Help in International Law: U.S. Action in the Iranian Hostage Crisis’ (1984) 37 J. INTL. AFF. 231
Schaller C., Beyond Self-Defence and Countermeasures A Critical Assessment of the Tallinn Manual’s Conception of Necessity, Vol. 95 – ISS. 7, 2017
Schia NN, “Horseshoe and Catwalk: Power, Complexity, and Consensus-Making in the United Nations Security Council” [2017] Palaces of Hope 55
Schmitt M, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey
Schmitt M, ‘Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’ (1999) 37 CJTL
Schmitt M, Cyber Operations and the Jud Ad Bellum Revisited, 56 Vill. L. Rev. 569 (2011)
Schmitt M, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence and Armed Conflicts’ in National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy (The National Academies Press 2010)
Schmitt M, Essays on Law and War at the Fault Lines,3, previously published in Foreign Cyber Interference in Elections, 97 INT’L L. STUD. 739 (2021)
Schmitt M, Tallinn Manual on the International Law Applicable to Cyber Operations (Cambridge University Press 2013)

Schmitt M, The Law Of Cyber Warfare: Quo Vadis?, Stanford Law & Policy Review [Vol. 25:269], (2014)
Schmitt M, Computer Network Attack: The Normative Software", Yearbook of International Humanitarian Law, vol.4, (2001)
Schmitt M., Foreign Cyber Interference in Elections, 97 INT'L L. STUD. 739 (2021)
Schmitt M, In Defence of Due Diligence in Cyberspace, THE YALE LAW JOURNAL FORUM, (2015)
Schneiker A, A Jenichen and J Joachim, Situating the Gender Mainstreaming Norm in Regional Organisations: Comparing the Incorporation of UN Security Council Resolution 1325 in the EU and OSCE: In Rethinking Gender Equality in Global Governance (Palgrave Macmillan 2019)
Scott J., Shackelford, From Nuclear War to Net War: Analogizing Cyber-attacks in International Law, Berkley Journal of International Law (BJIL), Vol. 25, No. 3, (2009)
Shackelford SJ, and RB Andres. 'State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem.' Geo J Int'l L 42 (2010) 986
Sharp WG, 'Cyberspace and the Use of Force' (1999) ARC
Sheng L, 'When Does Internet Denial Trigger the Right of Armed Self-Defence?' ,38 Yale Journal of International Law (2013) 179, 200
Shubert A, 'Cyber warfare: A different way to attack Iran's reactors' (CNN.com, 8 November 2011) <http://www.cnn.com/2011/11/08/tech/iran-stuxnet/>
Silver D, Computer Network Attack as a Use of Force under Article 2(4), in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell, International Law Studies , Vol.76, (2002)
Sklerov M, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defences against States Who Neglect Their Duty to Prevent', Military Law Review 201 (2009)
Sloane R., On the Use and Abuse of Necessity in the Law of State Responsibility, 106 AM. J. INT'L L. 447, 454 (2012)
Stark H, 'Stuxnet virus opens new era of cyber war' (Der Spiegel Online, 8 August 2011) https://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html
Stevens C, 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet.' *Contemporary Security Policy* 41, no. 1 (2020): 129-152
Taagepera R, *Estonia: Return to Independence* (Boulder, Westview Press 1993)

Talbot Jensen E, (2002), Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of self-defence, Stanford Journal of International Law, p. 234

Talmon S, 'German Constitutional Court Considers Self-Defence Against Nonstate Actors a Tenable Interpretation of Article 51 of the Un Charter.' GPIL-German Practice in International Law (2019)

Tardy T, The European Union and UN Peace Operations: What Global–Regional Peace and Security Partnership? In United Nations Peace Operations in a Changing Global Order (Palgrave Macmillan 2019)

Terry DG and K Tibori-Szabó, 'Twelve Key Questions on Self-Defence against Non-State Actors' (2019) 95 INT'L L. STUD. 467

Thakur R, The United Nations, peace and security: From collective security to the responsibility to protect (Cambridge University Press, 2016)

Thakur R, "The nuclear ban treaty: Recasting a normative framework for disarmament." *The Washington Quarterly* 40, no. 4 (2017): 71-95.

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

Thomson J, State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research, 39 INT'L STUDIES Q. 213,225 (1995)

Tolppa M, International Cyber Stability Framework at the United Nations Security Council, NATO CCDCOE Law Branch, https://ccdcoe.org/library/publications/international-cyber-stability-framework-at-the-united-nations-security-council/

Trachtman JP, Global Cyberterrorism, Jurisdiction, and International Organization' in M F. Grady & F Parisi (eds), The Law and Economics of Cybersecurity (1st edn, Cambridge University Press 2005)

Trapp K, State Responsibility for International Terrorism, 65, (2011)

Tsagourias N, Cyber-attacks, Self-Defence and the Problem of Attribution (July 24, 2012). Journal of Conflict & Security Law (2012), Vol. 17 No. 2, 229–244, Available at SSRN: https://ssrn.com/abstract=2538271.

United Nations, *Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression* (Repertory of Practice of United Nations Organs 2016) <http://legal.un.org/repertory/art51.shtml>

Valentinas M, Estonia: Attacks Seen As First Case Of 'Cyberwar' (30 May 2007) , <https://www.rferl.org/a/1076805.html >

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

Vermeer Z, ‘The Jus ad Bellum and the Airstrikes in Yemen: Double Standards for Decamping Presidents?’ (2015) Blog of the European Journal of International Law https://www.ejiltalk.org/the-jus-ad-bellum-and-the-airstrikes-in-yemen-double-standards-for-decamping-presidents/

W Sharp, ‘Cyber Space and the Use of Force’ (1999). Aegis Research Corporation 7, 28

Warrick J, ‘Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack’ (The Washington Post, 15 February 2011)

Watkins D and M Burton, *Research Methods in Law* (Routledge 2013)

Watts S, Low-intensity Cyber Operations and the Principle of Non-intervention, 1-2.

Waxman MC, ‘Cyber-attacks as Force under UN Charter Article 2(4)’ 87 ILS 15

Wight M, *Power Politics,* (Leicester University Press 1978)

William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council, (2009)

Willis H, The Doctrine of Sovereignty Under the United States Constitution, 15 No. 5 VA L. REV. 437 (1929)

Wilmshurst E., The Chatham House Principles of International Law on the Use of Force in Self-Defence , 55 INT’L & COMP. L.Q. 963, 967–68 (2006)

Wolff HH, Legal Implications of Territorial Sovereignty in Cyberspace, in Proceedings of the 4th International Conference on Cyber Conflict 9-10, 15 (2012)

Wood M, "International Law and the Use of Force: What Happens in Practice?." *Indian journal of international law* 53 (2013): 345-367.

Wright J, Cyber and International Law in the 21st Century, Speech of the The Attorney General Jeremy Wright QC MP in Chatham House Conference,(May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-internationallaw-in-the-21st-century

Xiao A, RESPONDING TO ELECTION MEDDLING IN THE CYBERSPACE: AN INTERNATIONAL LAW CASE STUDY ON THE RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION, in: DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW Vol 30:349

Zhou J, Main Content of International Military Law: Fundamentals of Military Law (Springer 2019)

Online Resources

"Maintain International Peace And Security". 2014. *Un.Org*. https://www.un.org/en/sections/what-we-do/maintain-international-peace-and-security/index.html#:~:text=The%20UN%20does%20this%20by,peace%20to%20hold%20and%20flourish.&text=The%20UN%20Security%20Council%20has,for%20international%20peace%20and%20security.

"What Is The Security Council? | United Nations Security Council". 2020. *Un.Org*. https://www.un.org/securitycouncil/content/what-security-council.

(*Hacktivismo - CCN-stic 401*) <http://www.dit.upm.es/~pepe/401/4660.htm#!-alone> accessed February 14, 2023

[MPEPIL] retrieved from < https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e252>

“Computer Virus” (*Computer Virus - an overview | ScienceDirect Topics*) <https://www.sciencedirect.com/topics/engineering/computer-virus> accessed February 15, 2023

“Cyberspace” (*Cyberspace - CIPedia*) <https://websites.fraunhofer.de/CIPedia/index.php/Cyberspace> accessed February 14, 2023

“UK says it supports Saudi Arabia's 'self-defence ' in Yemen”, The New Arab (2018)

“What Is a Distributed Denial-of-Service (Ddos) Attack? - Cloudflare” <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> accessed February 14, 2023

“What Is a Server? - Definition from Techopedia” (*Techopedia.com*) <https://www.techopedia.com/definition/2282/server> accessed February 14, 2023

"What Is Phishing: Attack Techniques & Scam Examples: Imperva" (*Learning Center*June 17, 2020) <https://www.imperva.com/learn/application-security/phishing-attack-scam/> accessed February 14, 2023

"What Is Software in Computer? Types and Examples - Javatpoint" (*www.javatpoint.com*) <https://www.javatpoint.com/what-is-software> accessed February 15, 2023

"WIFI Definition and Meaning" (*Washington Technology Solutions*) <https://watech.wa.gov/WiFi-definition-and-meaning> accessed February 19, 2023

Beal V, "What Is Cyber?" (*Webopedia*June 23, 2021) <https://www.webopedia.com/definitions/cyber/> accessed February 14, 2023

Bedell C, Loshin P and Hanna KT, "What Is a Computer Worm and How Does It Work?" (*Security*September 13, 2022) <https://www.techtarget.com/searchsecurity/definition/worm> accessed February 20, 2023

Declaration of the Minister of Foreign Affairs of the Republic of Estonia' (Republic of Estonia Government, 1 May 2007) https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia

Editor CSRCC, "Critical Infrastructure - Glossary: CSRC" (*CSRC Content Editor*) <https://csrc.nist.gov/glossary/term/critical_infrastructure> accessed February 14, 2023

Editor CSRCC, "Cyberspace Operations (CO) - Glossary: CSRC" (*CSRC Content Editor*) <https://csrc.nist.gov/glossary/term/cyberspace_operations> accessed February 14, 2023

Editorial SS, "What Is a Website & How Does It Work? (Easy Beginner's Guide)" (*SiteSaga*September 26, 2022) <https://www.sitesaga.com/what-is-a-website/> accessed February 19, 2023

Folger J, “What Is Spoofing? How Scam Works and How to Protect Yourself” (*Investopedia*November 3, 2022) <https://www.investopedia.com/terms/s/spoofing.asp> accessed February 15, 2023

Gillis AS, “What Is a Computer Network?” (*Networking*December 20, 2019) <https://www.techtarget.com/searchnetworking/definition/network> accessed February 13, 2023

Hanna KT, Lutkevich B and Wright R, “What Is Botnet?” (*Security*March 30, 2021) <https://www.techtarget.com/searchsecurity/definition/botnet> accessed February 13, 2023

International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition (2019), pp. 209-224, 210

Internet Corporation for Assigned Names and Numbers (ICANN), Homepage, http://www.icann.org/tr/english.html

J P. Barlow, ‘A Declaration of the Independence of Cyberspace’ (1998) <https://projects.eff.org/~barlow/Declaration-Final.html>

National Crime Agengy Website, ‘Cyber Crime’ https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

National Crime Agengy Website, ‘Cyber Crime’ https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Pickle B and Christensson P, “Data” (*Definition*December 13, 2022) <https://techterms.com/definition/data> accessed February 14, 2023

read 3min., “What Is a Denial of Service Attack (Dos) ?” (*Palo Alto Networks*) <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos> accessed February 14, 2023

Russian Federation, Ministry of Foreign Affairs, 'Comment by the Foreign Ministry on the Situation in Yemen' (2015) http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/20ca325c9ebff5d943257el40048cd74!OpenDocument

Sullivan P, “What Is CERT?” (*WhatIs.com*March 18, 2021)

<https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team> accessed February 13, 2023

The Economist, ‘Marching off to cyberwar’ The Economist 4 December 2008 www.economist.com/node/ 12673385

Toomas Hendrik Ilves, ‘Address by the President of Estonia’ (67th Session of the United Nations General Assembly, New York, 26 September 2012) https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-unitednations-general-assembly-un-headquarters-new-york-september-2012/

U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber-attack, May 12, 2009, https://www.nti.org/gsn/Article/us-general-reserves-right-to-use-force-even-nuclear-in-response-to-cyber-attack/

What is a botnet? < https://www.microsoft.com/en-us/security/pc-security/botnet.aspx>

What is a Ping (ICMP) flood attack? < https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ >