

**THE LEGALITY OF ANTICIPATORY SELF-DEFENCE AGAINST A
MARITIME CYBER-ATTACK**

by

FOLUKE MARY DARE

Submitted in fulfilment of the requirements for the degree

of

DOCTOR LEGUM (LL. D)

in the

FACULTY OF LAW

at the

NELSON MANDELA UNIVERSITY

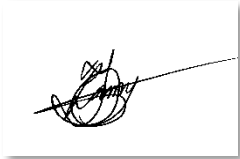
PROMOTER: PROF PHG VRANCKEN

CO-PROMOTER: PROF FRANS MARX

APRIL, 2022

DECLARATION

I, FOLUKE MARY DARE with student number s220013233, hereby declare that the thesis for LL. D (Public Law) to be awarded is my own work and that it has not previously been submitted for assessment or completion of any post graduate qualification to another University or for another qualification.



24th July 2022

.....
MRS. FOLUKE MARY DARE

.....
DATE

DEDICATION

To Almighty God.

ACKNOWLEDGEMENTS

I am filled with profound gratitude to God for the grace, good health, strength, courage, and wisdom to undertake this doctoral research.

My immense gratitude goes to my promoter, Prof Patrick Vrancken, for the privilege to learn and be guided by his wealth of knowledge. His patience, doggedness, and commitment to achieve excellence is worth emulating and is deeply appreciated. I am very grateful to my co-promoter, Prof Frans Marx, for his valuable observations, guidance, and support during my research.

I thank my family for their unflinching support, prayers and encouragement which fueled my determination to keep moving forward with my research despite life's challenges. My post humous appreciation goes to my late father, Sir J.S. Ajiboye Esq, JP, KSM, the architect of my career, for planting the seed to pursue this doctoral program in my heart before his demise. I am filled with great joy that our plan has come to fruition.

I must express my appreciation to Nelson Mandela University management for the student support I received through the National Research Foundation during my doctoral program. It enabled me to stay focused and carry out my research without distractions. I am deeply honoured to be a doctoral candidate at this prestigious university that has chosen to build a global research reputation in law of the sea and ocean sciences.

The following persons are worthy of being remembered for their support, mentorship, and encouragement: Dr. Tajudeen Sanni, Mr. Abdulkareem Azeez, Mrs. Fatimah Sanni, Dr. Tade Oyewunmi, and Ms. Tanya Stephens. God bless you all.

GLOSSARY/LIST OF ABBREVIATIONS

AIS – Automatic Identification Systems
AU – African Union
CyRiM – Cyber Risk Management
DOS – Denial of Service
DDOS – Distributed Denial of Service
DHS – Department of Homeland Security
GAO – Government Accountability Office
GPS – Global Positioning System
ICJ – International Court of Justice
ICT – Information and Communications Technology
IMO – International Maritime Organisation
MCA – Maritime Cyber-Attack
MCAA – Maritime Cyber Armed Attack
PC – Personal Computer
US – United States
UN – United Nations
UNCLOS – United Nations Convention on Law of the Sea

KEYWORDS

Maritime Cybersecurity, Maritime Cyber-Attack, Use of Force, Anticipatory Self-Defence, Maritime Security, Imminence, Maritime Cyber Threats.

SUMMARY

This research aims to determine how the principle of anticipatory self-defence, in line with article 51 of the UN Charter, can be applied to the context of maritime cybersecurity. Despite the debates by some scholars to clarify the international law position on anticipatory self-defence in the maritime context, there is no universally accepted legal provision for States to rely on in carrying out anticipatory self-defence against imminent maritime cyber-attacks. This raises the questions concerning the lawful steps States can take in self-defence against maritime cyber-attacks. This research shows the challenges facing States in their bid to comply with the provision of article 51 of the UN Charter to anticipatorily defend against an MCA. The recommendations made are intended to guide States in making policies and mapping our strategies to lawfully tackle the emerging threat of cyber-attacks against maritime security.

TABLE OF CONTENTS

DECLARATION	ii
ACKNOWLEDGEMENTS	iv
GLOSSARY/LIST OF ABBREVIATIONS	v
KEYWORDS	vi
SUMMARY	vii
TABLE OF CONTENTS	viii
CHAPTER 1: INTRODUCTION	1
1.1. Introduction	1
1.2. An Overview of Cyber Threat at Sea	4
<i>1.2.1. Classification of Cyber-attacks</i>	<i>7</i>
<i>1.2.2. Threats to Maritime Cyber Security</i>	<i>8</i>
1.2.2.1. Features of Maritime Cyber Threats	10
1.2.2.2. Unique Nature of Maritime Cyber-attacks	12
1.3. Defence Measures against Maritime Cyber-Attack	13
1.4. Research Focus	14
1.5. Research Structure	17
1.6. Limitations	19
CHAPTER 2: THE LEGAL CONTEXT OF MARITIME CYBER SECURITY	21
2.1. Introduction	21
2.2. International Legal Instruments on Maritime Cyber Security	23
<i>2.2.1. The United Nations Convention on Law of the Sea</i>	<i>24</i>
<i>2.2.2. Regional Laws on Cyber Security</i>	<i>28</i>
<i>2.2.3. Suppression of Unlawful Acts Against the Safety of Maritime Navigation Convention and its Additional Protocol</i>	<i>32</i>
<i>2.2.4. The International Maritime Organisation’s Guidelines on Maritime Cyber Security</i>	<i>34</i>

2.2.5. <i>The UN Charter and the Judicial Interpretation on the Use of Force and Armed Attack</i>	36
2.3. Domestic Laws	38
2.4. Scholarly Writings on Maritime Cyber Security	42
2.5. Conclusion	55
CHAPTER 3: MARITIME CYBER-ATTACK AS USE OF FORCE	57
3.1. Introduction	57
3.1.1. <i>Violent Acts in the Maritime Sector</i>	59
3.1.2. <i>Historical Background on the Use of Force</i>	61
3.2. Maritime Cyber Operation, Interference or Attack	63
3.2.1. <i>Maritime Cyber Operation</i>	63
3.2.2. <i>Maritime Cyber Interference</i>	64
3.2.3. <i>Maritime Cyber-Attack</i>	65
3.3. Use of Force in the Context of Maritime Cyber Security	74
3.3.1. <i>Meaning of Force</i>	74
3.3.2. <i>Maritime Cyber-Attack as a Type of Force</i>	77
3.3.3. <i>Maritime Cyber-attack as Unlawful Use of Force</i>	81
3.3.4. <i>Evolving Legal Norms on the Use of Force</i>	84
3.4. Conclusion	95
CHAPTER 4: MARITIME CYBER-ATTACK AS AN ARMED ATTACK	97
4.1. Introduction	97
4.2. The Right of Self-defence	98
4.3. Determining the Occurrence of an Armed Attack	102
4.3.1. <i>Assessment of the Attacker’s Act</i>	103
4.3.2. <i>The Gravity Threshold of the Attack</i>	105
4.3.3. <i>Identifying Critical Infrastructure</i>	106
4.3.4. <i>Armed Attack in the Maritime Context</i>	108
4.4. Cyber-Attack as Armed Attack	111
4.4.1. <i>Critical Analysis of Cyber Armed Attack</i>	112
4.4.2. <i>Scale and Effect Principle as Determinant of Cyber Armed Attack</i>	118

4.5. Qualifying Maritime Cyber-attack as Armed Attack	120
4.5.1. <i>Examples of Maritime Cyber-attacks</i>	121
4.5.2. <i>Legal Theory on Maritime Cyber Armed Attack</i>	123
4.5.3. <i>Maritime Cyber-attack and the Threshold of Armed Attack</i>	126
4.5.4. <i>Severity of Effect as a Determinant of Maritime Cyber Armed Attack.....</i>	129
4.6. Conclusion.....	130
CHAPTER 5: ANTICIPATORY SELF-DEFENCE AGAINST MARITIME CYBER-ATTACK	133
5.1. Introduction	133
5.2. Invoking Anticipatory Self-defence against MCAA	134
5.2.1. <i>Criteria for Anticipatory Self-defence against MCAA</i>	137
5.2.2. <i>Options Available in Self-defence against MCAA</i>	141
5.3. Conditions for Anticipatory Self-defence against MCAA	145
5.3.1. <i>The Legal Requirement of Imminence.....</i>	146
5.3.2. <i>The Legal Requirement of Necessity.....</i>	150
5.3.3. <i>The Legal requirement of Proportionality.....</i>	152
5.4. Challenges of Invoking ASD against MCAA	153
5.4.1. <i>Intent and Timeline of Attacker’s Act</i>	155
5.4.2. <i>Application of the Legal Requirements of Anticipatory Self-Defence to MCAA</i>	158
5.4.3. <i>Secrecy Surrounding MCAA Reports</i>	164
5.4.4. <i>Technology Capacity for Early Detection of MCAA.....</i>	165
5.4.5. <i>Attribution.....</i>	167
5.4.6. <i>Lack of Consensus in Treaty Provisions on MCAA.....</i>	170
5.4.7. <i>Lack of Universal Cyber Security Expertise.....</i>	171
5.4.8. <i>Defence against Non-State Actors without Violating Sovereignty.....</i>	172
5.5. Conclusion.....	173
CHAPTER 6: CONCLUSION.....	175
6.1. Introduction	175
6.2. Summary of Key Issues.....	175
6.3. Recommendations	180

TABLE OF INTERNATIONAL INSTRUMENTS	187
TABLE OF LEGISLATION	188
TABLE OF CASES	189
BIBLIOGRAPHY	190
<i>Books.....</i>	<i>190</i>
<i>Journal Articles</i>	<i>194</i>
<i>Conference Papers, Seminars, Symposia and Lectures</i>	<i>204</i>
<i>Reports, Policies and Draft Policies.....</i>	<i>206</i>
<i>Newspapers, Radio Broadcast and Newsletters.....</i>	<i>208</i>
<i>Websites.....</i>	<i>208</i>

CHAPTER 1: INTRODUCTION

1.1. Introduction

Understanding the technical nature of the Internet is vital in determining the security issues that arise from using it. The Internet connects various forms of specialised computing devices such as machines, satellite components, mobile phones, desktop, and laptop computers.¹ These devices possess unique addresses through which they interact by following the language of Internet communications known as protocols. Information is transferred across the globe through the Internet network as packets of data.²

The evolution of the Internet has been dominated by narratives that are interconnected in their accounts.³ Bory aptly explains this when he states that:

A group of pioneers...shared their visions about the future of networking technologies, and so assembled the conceptual frame of the Internet imaginary; the second narrative comprises the stories about the pioneers and founding fathers of the Internet and the Web that were told and spread starting from the 1990s. In this period not only academics, but also political and cultural actors, institutionalised the myth of the Internet's origins in Western culture.⁴

The 'group of pioneers' in the first narrative comprises the foremost computer scientists, namely: Vannevar Bush, Joseph Licklider, Douglas Engelbart, and Tim Berners-Lee, who invented the World Wide Web, which is not the Internet but a data-enabled service that runs within the Internet network.⁵

¹ Daigle "On the Nature of the Internet" in *Global Commission on Internet Governance Report A Universal Internet in a Bordered World* (2016), 17-20.

² *Ibid.*

³ Naughton "The Evolution of the Internet: From Military Experiment to General Purpose Technology" 2016 1(1) *Journal of Cyber Policy* 5-28, states that "Research on its design commenced in 1973 and the network became operational in January 1983. For the first two decades of its existence, it was the preserve of a technological, academic, and research elite; Bory *The Internet Myth: From the Internet Imaginary to Network Ideologies* (2020) 7-38.

⁴ Bory *The Internet Myth* 9-10.

⁵ Naughton 2016 *Journal of Cyber Policy* 5 6, states that: "...Thus, for example, many users think that the World Wide Web is 'the Internet'... But the words up to here are not suitable for a document of this nature the Web and Facebook are just particular examples of data-enabled services that run on the infrastructure that constitutes the Internet and mistaking them for the network is analogous to thinking that intercity trains, say, define the railway system." South Africa's section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines The Internet as "...the interconnected system of networks that connects computers around the world using the TCPIP (Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet) and includes future versions thereof".

One of the stories about the founding fathers in the second narrative is that the Internet was created for military purposes.⁶ The Internet's original purpose has metamorphosed from a medium of communication between scientists into easy and often anonymous worldwide access by and to computer systems of individuals, corporate bodies, and government institutions.⁷

The Internet was not created for a single purpose.⁸ Presently, Internet users with various purposes include adults, youths, graduates, manufacturing, transportation companies, and States for establishing and managing critical national infrastructure. The demography and diversity of purpose for Internet usage have brought to light some pertinent security issues.

The Internet has played a crucial role in developing maritime, aviation and land transportation systems in the modern era. The cyber aspect of maritime security, which is the focus of this research, has evolved over the years due to the existence of information technology. Maritime transport is very relevant to worldwide activities ranging from trade to security operations. Goods are shipped around the world and people are transported to various destinations. Apart from the commercial activities, the sea is seen as a very strategic avenue for military activities, which include the presence of naval aircraft carriers, missile launchers, attack submarines and other naval war equipment.

The ease and anonymity associated with Internet usage has created a platform for individuals to interfere, in a range of sophisticated ways, with individuals, companies, objects and States.⁹ The victims' hardware and software are open to cyber interference and other cyber actions. In this context, cyber interference refers to a nonconsensual cyber act that affects the control of a victim's software or hardware. The use of the term 'cyber-attack' becomes relevant when cyber interference meets the requirement of article 51 of the UN Charter.¹⁰ In this introduction, cyber

⁶ Bory *The Internet Myth* 5.

⁷ Gable "Cyber-Apocalypse Now: Securing the Internet against Cyber-terrorism and Using Universal Jurisdiction as a Deterrent" 2010 43 *Vanderbilt Journal of Transnational Law* 57 67; Lipson *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy* (2002) 13.

⁸ Daigle *Global Commission on Internet Governance Report* 17-20.

⁹ Stahl "The Unchartered Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cyber Security" 2011 40 *Georgia Journal of International and Comparative Law* 247 248.

¹⁰ Knopová and Knopová "The Third War in the Cyberspace? Cyber Warfare in the Middle East" 2014 3(1) *Acta Informatica Pragensia* 23, 25-26; "[a]ctually, cyber-attacks can be divided into

interference is deliberately used to explain cyber acts which target a victim's software or hardware without authorisation. Understanding the technical concept of an attack is crucial to applying the international law provision on anticipatory self-defence to maritime cyber security. This will be discussed thoroughly in chapter three after identifying the applicable laws in chapter two. Cyber interferences can originate from and target any destination on land, at sea or in the air. For this research, maritime cyber interference has occurred when cyber interferences affect marine vessels, coastal military port installations, oil rigs, and other sea installations¹¹ used to exploit marine resources. They can be channelled through several locations to evade being traced or detected.

Unfortunately, the maritime industry has undergone security threats that adversely affect international trade and economic growth and State sovereignty in a non-kinetic way and with varying degrees of impact.¹² These threats include piracy, terrorism and other unlawful acts which can be perpetrated through nonconsensual cyber acts.¹³ Also, military ports, ships, oil rigs, and other sea installations used to exploit marine resources can be targeted. The consequences range from minor security lapses, enormous damage to property and pollution of the marine environment to loss of lives. Ships and submarines have become means through which weapons of mass destruction can be launched.¹⁴ For instance, this can occur when maritime cyberspace is used to launch a nuclear missile aboard ship through a cyber interference. This confirms the growing concern about maritime cyber security threats. Although these security threats have been the focus of the International

two categories – syntactic attacks that act directly, in other words malicious software, and semantic attacks that aim to modify data. Thus, semantic attacks focus on a user, whereas syntactic attacks direct onto IT facilities. Even though the damages caused by semantic attacks can be of considerable extent, ... syntactic attacks are used more often and cause more damages”.

¹¹ According to section 4 of Australia's Sea Installations Act of 1987, states that sea installations mean “any man-made structure that, when in, or brought into, physical contact with the seabed or when floating, can be used for an environment related activity”.

¹² Sakhuja “Security threats and challenges to maritime supply chains” (undated) https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2959.pdf (accessed on 2019-12-12).

¹³ Article 101 of 1833 UNTS 3, (1982) 21 ILM 1261. Adopted: 10.12.1982; EIF: 16.11.1994 (UNCLOS) defines piracy.

¹⁴ Bateman “Regional Maritime Security: Threats and Risk Assessments” in *Southeast Asia and the Rise of Chinese and Indian Naval Power: Between Rising Naval Powers* (2010) 99-113.

Maritime Organisation, a vital regulator of the maritime shipping industry¹⁵, maritime cyber-attacks have gained lesser attention.

1.2. An Overview of Cyber Threat at Sea

The sea is one of the natural resources on earth, collectively shared by States for commercial and military uses.¹⁶ According to Tangredi,

oceans and the airspace above them were the first internationally recognised global commons and the model for analysing the emerging space and cyberspace domains...Mitigating security threats to the maritime commons benefited all nations, even non-coastal states.¹⁷

The establishment of a legal framework for governing the sea aligned with the objective of mitigating security threats. The 1982 United Nations Convention on Law of the Sea¹⁸ emerged to regulate the freedoms at sea by providing for the rights and jurisdictions of States in the marine domain.¹⁹ Some of the protected rights include safety of life at sea, navigation, and communication onshore and offshore. These rights can be breached through cyber interference, which is the focus of this research, as well as piracy and terrorism.

Over the years, there has been a tremendous increase in maritime cyber interference, especially in the last decade. In 2011, cyber pirates targeted an Iranian

¹⁵ International Maritime Organization “Maritime Security and Piracy” (undated) <https://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx> (accessed 2020-11-11) “The IMO has within its mandate to make trade and travel by sea as safe and secure as possible. To manage and mitigate any threats with the potential to compromise maritime security the Organization develops suitable regulations and guidance through the Maritime Safety Committee (MSC) and with input from the Organization’s Facilitation Committee (FAL) and Legal Committee (LEG).” Also the International Ship and Port Facility Security (ISPS) Code which is contained in the 1974 International Convention for the Safety of Life at Sea (SOLAS) is an example of the IMO’s instrument which requires member States to maintain high standards of security at sea with no specific provision on the legality of self-defence against cyber-attack.

¹⁶ University of Strathclyde Glasgow “Law and Governance of the Global Commons Incubator” (undated) <https://www.strath.ac.uk/research/strathclydecentreenvironmentallawgovernance/ourwork/research/labsincubators/lawandgovernanceoftheglobalcommonsincubator/> (accessed on 2020-10-28); “International law defines traditionally five global commons: high seas, the deep-sea bed, the atmosphere, Antarctica and Outer Space”.

¹⁷ Tangredi “The Maritime Commons and Military Power” in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security* 2012 71-72.

¹⁸ UNCLOS

¹⁹ Koh *A Constitution of the World’s Oceans* Remarks of the President of the Third United Nations Conference on the Law of the Sea at the Conference at Montego Bay (December 1982) available at http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm “accessed on 2020-10-28.

supply line, IRISL, and their actions resulted in substantial financial loss.²⁰ The business operation of the supply line was interrupted when the pirates interfered with the servers. Also, they crashed the logistics system by altering information on the manifest and client-vendor data.²¹ In 2012, multiple systems on a commercial ship contracted by the U.S. military were compromised in a State-sponsored attack and the GPS signals of over 120 ships were maliciously jammed.²² This unlawful cyber operation put the ships' navigation system in jeopardy and threatened the safe passage of ships at sea.

In 2013, it was discovered that drug smugglers had breached cyber security at the port of Antwerp. They hacked the cargo tracking systems in order to avoid detection.²³ In 2014, the United States (U.S) Government Accountability Office (GAO) issued a report on maritime critical infrastructure protection, which emphasised the need for the Department of Homeland Security (DHS) to address port cyber security better.²⁴ In that report, it was observed that 24 major U.S. agencies had ineffective responses to cyber incidents.²⁵ They mainly were unsuccessful in their effort to repel or defend against cyber interferences. In the same year, the ship-to-shore cranes of a major U.S. port facility suffered a severe system disruption.²⁶ A.P. Moeller-Maersk lost more than USD200 million in 2017 when its cyber security system was breached.²⁷ In 2018, the main international ports of Spain and the U.S. experienced cyber-attacks. The internal IT systems of the ports of Barcelona and San Diego were targeted.²⁸ The probable consequence of such cyber-attacks on the international ports can adversely affect the global

²⁰ Ivezic "Defeating 21st Century Pirates: The Maritime Industry and Cyber-attacks" (8 January 2018) (available at www.csoonline.com (accessed on 2018-03-25)).

²¹ *Ibid.*

²² Krasny "Chinese hacked U.S. Military Contractors: Senate Panel" (18 September 2014) (available at www.reuters.com/article/us-usa-military-cyberspying/chinese-hacked-u-s-military-contractors-senate-panel-idUSKBN0HC1TA20140918 (accessed on 2018-03-25)).

²³ Cyber bits "Hackers Deployed to Facilitate Drugs Smuggling" (available at www.europol.europa.eu (accessed on 2018-03-25)).

²⁴ US GAO – Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cyber Security (available at www.gao.gov (accessed on 2018-03-25)).

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ Ivezic *supra*.

²⁸ Safety4sea "2018 Highlights: Major Cyber Attacks Reported in Maritime Industry" (26 December 2018) <https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/> (accessed 2019-12-14).

economy. Likewise, the Australian Defence shipbuilder, Austal,²⁹ was the victim of a ransomware attack by hackers who targeted its data management systems.³⁰ South Korean and Japanese shipping companies were also victims of a group of cyber criminals from Nigeria who targeted business emails in the global maritime industry to divert payments running to hundreds of thousands of dollars.³¹ These criminals impersonated employees of these companies and engaged in business dealings to fraudulently get paid huge sums of money.

In 2019, the IT network of the Kuwait transportation and shipping industry experienced cyber-attacks which allowed hackers to install malware as a backdoor tool.³² This malware provided the attacker with unauthorised and remote access to any compromised Personal Computer (PC) system. It was also reported that the US Coast Guards confirmed the use of malware by hackers to disrupt shipboard computer systems.³³ The shipboard computer system comprises of the network system for information, transmission, and processing. It has been described as:

a high-powered computer system that collects, processes, displays and archives data from the navigational and scientific sensors...on ships...which is vital to safe navigation and scientific applications...³⁴

It provides real-time information to the server from navigation, meteorological, oceanographic and fisheries sensors. Data collected from these sensors are crucial to the safe operation of a vessel and should not be interfered with. Also, in the same year, about 20 Chinese coastal sites experienced hostile Global Positioning System (GPS) spoofing which targeted the shipping industry, especially oil terminals.³⁵

It has been reported by the Cyber Risk Management (CyRiM) project³⁶ that a maritime cyber-attack can cause enormous economic damage and chaos in the

²⁹ Austal builds vessels for the Royal Navy of Oman, the Royal Australian Navy, and the US Navy.

³⁰ Safety4sea “2018 Highlights: Major Cyber Attacks Reported in Maritime Industry” (26 December 2018) <https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/> (accessed 2019-12-14).

³¹ *Ibid.*

³² Loock “Two Major Cyber-attacks Have Targeted Kuwait Transportation and Shipping Industry This Year” (1 October 2019) <http://www.marsecreview.com/2019/10/two-major-cyber-attacks-have-targetted-kuwait-transportation-and-shipping-industry-this-year/> (accessed 2019-12-16).

³³ *Ibid.*

³⁴ <http://137.75.108.144/technology/tools/scs/scs.html> (accessed 2019-12-19).

³⁵ The Maritime Executive “Patterns of GPS Spoofing at Chinese Ports” (accessed 2019-12-20).

³⁶ The Singapore-based public-private initiative.

global maritime supply chain. This report showcases a hypothetical maritime cyber-attack that infects the computer systems aboard a ship with a virus that:

originates in a ship management company's cargo management software, corrupting the manifests of all the ships it manages..., works its way through the port management system supply chain to disrupt the first port of call for each infected ship...and spreads through the port's cargo management network.³⁷

Based on these chronological events of the last decade, it is evident that maritime cyber-attacks pose a serious threat to maritime security. With the increasing reliance on technology in the shipping industry, challenges will continuously arise which require well-formed policies and legal actions by States to ensure the security of maritime cyberspace. Although many countries have various domestic laws on cyber infrastructures, States have no consensus on the universal approach to address self-defence issues arising from maritime cyber-attacks.

1.2.1. Classification of Cyber-attacks

The above instances of cyber-attacks can be categorised based on legal classification, interferer's purpose, the seriousness of interferer's participation, scope of the attack and type of network setting being attacked.³⁸ These categories overlap because a cyber-attack can fit into the description of one more of the categories. For instance, the legal classification of cyber-attacks refers to categorising them as active and passive cyber-attacks. Active cyber-attacks, such as denial of service, involve modification of data with the intent to corrupt or destroy the data and the victim's network. The active cyber-attacks encompass the scope of attacks involving malicious attacks, which is characterised by the extensive participation of the attacker in launching the attack over various types of networks.³⁹

Passive cyber-attacks, such as phishing scams entail eavesdropping, monitoring, and getting information from a victim's system without alteration of the data.⁴⁰ This legal classification of cyber-attacks into active and passive cyber-attacks is relevant in answering the questions in this research. For example, on the issue of whether Maritime Cyber Attack (MCA) can qualify as use of force or meet the threshold of an

³⁷ CyRiM Project "2009 Shen Attack: Cyber risk in Asia Pacific Ports 13" https://www.msig-asia.com/sites/msig_asia/files/downloads/CyRiM_ShenAttack_FinalReport.pdf (accessed on 2019-12-19).

³⁸ Uma and Padmavathi "A Survey on Various Cyber-attacks and Their Classification" 2013 15(5) *International Journal of Network Security* 390, 394.

³⁹ *Ibid.*

⁴⁰ *Ibid.*

armed attack, the severity and effect of the MCA will be considered. The decade-long history of cyber-attacks, as discussed above, whether passive or active, demonstrate that the growing impact and disastrous consequences of cyber interferences have been felt globally. Hence, there is a need to ensure that laws and enforcement mechanisms are globally agreed upon to identify and lawfully curb these maritime cyber security threats.

Also, the classification of 'interferer's purpose', which assesses the attacker's intent, consists of perceived hostile cyber operations and harmless cyber espionage.⁴¹ The hostile intent of a cyber-attacker can be implied when the foreseeable resultant consequence of the attack is perceived as grievous and destructive. Cyber espionage entails surveillance and gathering intelligence without causing extensive damage or destruction to property within the victim's cyberspace.⁴² There is a thin line between these categories because cyber espionage can be perceived as a hostile cyber operation if the attack's scope and network setting are critical to a State's national security. When the attacker's surveillance targets intelligence gathering about a State's security network, it can be interpreted as a serious breach of national security.

In addition, cyber-attacks can be classified based on illegality and attributability. When a computer network device is used unlawfully by a person or a group of people to breach maritime cybersecurity without State sponsorship, it can be categorised as a cybercrime.⁴³ This classification is based on the provisions of the cybercrime laws regulating the jurisdiction where the attack occurred. It is clear that in this instance, a cyber-attack can be described as a cybercrime.

1.2.2. Threats to Maritime Cyber Security

Maritime security is a crucial concept of maritime policy which is relevant to ocean governance and international security.⁴⁴ In the absence of a universal definition of maritime security, its description can depict a stable and peaceful usage of the sea

⁴¹ *Ibid.*

⁴² Abdyraeva *The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends* (2020) Report OIIP - Austrian Institute for International Affairs 32, 15: Here, Cyber espionage was defined as a tool a) To gather intelligence b) To strategically leak private information c) To alter stored information while Cyber-attacks/ cybercrime was defined as hacking into critical infrastructure, political organizations, politicians..."

⁴³ *Ibid.*

⁴⁴ Bueger "What is Maritime Security?" 2015 53 *Marine Policy* 159 159.

and its resources.⁴⁵ Actions such as cyber-attacks against ships, maritime piracy, smuggling of illicit cargo, human trafficking through the sea, illegal dumping, vessel discharge of pollutants, attacks by maritime militia, and sometimes naval forces can threaten maritime security.⁴⁶ The importance of securing the marine environment cannot be overemphasised. Understanding the possible forms of security challenges faced at sea and the legal implications is paramount to having a robust maritime security strategy.⁴⁷ Maritime cyber security can be breached illegally by an aggressor or legally by a victim-State while acting in self-defence.

A State is threatened when its population, territory, political authority, and capacity to enter into legal relations with other States face an imminent attack. Protecting these elements of statehood involves protecting a State's territorial rights of jurisdiction, resources, and control of movement through its borders.⁴⁸ Coastal States can exercise jurisdiction over activities within their territorial sea while recognising other States' right of innocent passage.⁴⁹ On the high seas, States enjoy jurisdiction over flagged ships⁵⁰ and other rights in accordance with the provisions of international law and particularly, the law of the sea. When these rights are threatened, States carry out security assessments to determine their next line of action. This assessment requires identification of the threat, perception of whether the attack is imminent and foresight of a reasonable consequence of the attack. This assessment guides the victim-State, which is under threat, to act in anticipatory self-defence within the confines of the law to thwart the imminent attack.

Ships, military ports, and sea installations being used to exploit marine resources are open to cyber interferences owing to their reliance on Information and Communications Technology (ICT). ICT has been defined as:

technology that is used to handle communications processes such as telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions.⁵¹

⁴⁵ Kraska and Pedrozo *International Maritime Security Law* (2013) 1.

⁴⁶ Ece "The Maritime Dimension of International Security: Piracy Attacks" in *Maritime Security and Defence against Terrorism* (2012) 11.

⁴⁷ *Ibid.*

⁴⁸ Simmons "On the Territorial Rights of States" 2001 11 *Philosophical Issues* 300 306.

⁴⁹ Article 19(2) of UNCLOS.

⁵⁰ Articles 91, 92, 94, and 97 of UNCLOS.

⁵¹ Information and Communications Technology "What Does Information and Communications Technology (ICT) Mean" (18 August 2020)

It has been relied upon for optimising operations such as the navigation system onboard the vessels, propulsion, freight management and traffic control communications.⁵² These operating systems utilise ICT features such as digital maps, radio, satellite communication and GPS.⁵³ These modern features of paperless navigation and automatic updates have increased the vulnerability of ships so much that⁵⁴ unauthorised Internet access by cyber-attackers can interfere with the ship's navigation, satellite communication, cargo tracking systems, marine radar systems and automatic identification systems (AIS).⁵⁵ All of these systems are critical to the safety of ships at sea. More specifically, Internet attackers can carry out grave attacks⁵⁶ such as attacking the shipboard network or sending false GPS information.⁵⁷ The communication signals of the engine controls and sensors, cargo controls, personal computers, payment systems, navigation systems, passenger and crew data can be blocked.⁵⁸ This suggests that remotely controlled and autonomous ships will be at greater risk of being targeted by hackers than the presently uncommon manually controlled ships due to their reliance on ICT.

1.2.2.1. Features of Maritime Cyber Threats

Cyber-attacks against a State can take various forms and can occur within its maritime zones. For this research, the relevant location for determining the occurrence of an attack is the marine location of the target. The origin of the attack can be from a server situated on the land or at sea. Identifying the origin of the attack is relevant for acting in self-defence. A breach of maritime cyber security refers to the intrusion against another network, whether in offence or defence.⁵⁹ The intrusion can

<https://www.techopedia.com/definition/24152/information-and-communications-technology-ict> accessed on 2020-10-14.

⁵² European Network and Information Security Agency (ENISA) 2011 Report on "Analysis of Cyber Security Aspects in the Maritime Sector" 1-2 https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport (accessed on 2018-03-12).

⁵³ *Ibid.*

⁵⁴ *Ibid.*

⁵⁵ Paganini "Hacking Ships: Maritime Shipping Industry at Risk" (31 March 2015) <http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html> (accessed on 2018-03-12).

⁵⁶ The attacks are very serious due to the gravity of damage attackers can cause under the cloak of anonymity; Lipson *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy* (2002) 13; Stevens "Internet War Crimes Tribunals and Security in an Interconnected World" 2009 18(3) *Transnational Law and Contemporary Problems* 657-720.

⁵⁷ UK Chamber of Shipping *A Master's Guide to Cyber Security* (2015) 2-6.

⁵⁸ *Ibid.*

⁵⁹ Article 49(1) Additional Protocol I to the Geneva Conventions of 1949.

vary in the light of recent technological advancements. It can be carried out with a variety of cyber weaponry. It can occur through the use of tangible or intangible weaponry and to cause a degree of damage or disruption to the target. The use of tangible weaponry can involve dropping bombs or missiles on computer devices that power other critical operating systems at sea. Cyber weapons can be intangible, such as using malicious computer software to target critical Internet-reliant sea installations to exploit marine resources, military ports, and critical infrastructures of ships. The use of malware⁶⁰ and other cyber activities to cause grievous bodily harm, to inflict financial losses, destruction, and damage to property, are examples of offensive cyber-attacks.⁶¹ They can be carried out by private individuals or by the State.

Cyber-attacks may be carried out through automated malware, denial of service (DOS) attacks and unauthorised remote intrusions into computer systems.⁶² These methods of interferences may be combined to create different types of cyber intrusion. The most effective and straightforward types of intrusion are DOS and malware interferences.⁶³ The malware can use a slaving mechanism that gives the intruder the ability to remotely control the victim's computers to do as he or she pleases.⁶⁴ It can affect its target by changing its programming function, while the DOS paralyses the functioning capacity of the target system. An example of introducing malicious software was seen in Iran, where the *Stuxnet* computer worm was used to attack its nuclear facility in 2010. The malware's capacity included replicating itself, hijacking and reprogramming to destroy the facility completely.⁶⁵ It can be introduced into a system without Internet through a universal serial bus (USB) computer port. In this case, attributing responsibility to and determining the intention of the attackers was difficult.⁶⁶ Consequently, the defence ability of the victim was impaired due to some impractical requirements of the rules of international law in

⁶⁰ Malicious Software delivered through the Internet.

⁶¹ Schmitt (ed.) *Tallinn Manual on the International Law Application to Cyber Warfare* 2ed (2017) 106.

⁶² Sklerov "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defences against States Who Neglect Their Duty to Prevent" 2009 201 *Military Law Review* 1 13

⁶³ Stahl 2011 *Georgia Journal of International and Comparative Law* 255.

⁶⁴ Norton "What is Malware and how can we prevent it?" http://us.norton.com/security_response/malware.jsp (accessed 2018-01-24).

⁶⁵ Glick "Column One: The lessons of Stuxnet" (1 October 2010) (<http://www.jpost.com/Opinion/Columnists/Article.aspx?id=189823> (accessed 2021-11-30).

⁶⁶ *Ibid.*

identifying the attacker.⁶⁷ This will be referred to and discussed in detail in the following chapters.

Both or either a DOS and malware interference on the operating and/or programming system of a ship is extremely dangerous. The operating system of a ship can be hijacked by an intruder and commanded to change course. The ship can be diverted or used as a weapon of destruction by crashing it into an oil rig or any other target. The operating system of the cargo section of the ship can be manipulated and used to smuggle hard drugs or weapons. Hence, due to the speed with which maritime cyber interferences are launched, gathering evidence to determine the effect, damage and identity of an intruder make it challenging to act within the boundaries of existing laws.

1.2.2.2. Unique Nature of Maritime Cyber-attacks

A maritime cyber-attack is unique in that; its impact poses a modern form of threat to maritime cyber security.⁶⁸ It is a unique form of artificial threat against the maritime industry because it is different from the usual threats of pirate attacks.⁶⁹ The platform of information technology on which it occurs is a critical infrastructure for maritime operations.⁷⁰ This is because navigation, communication and other systems of a ship are operated through cyberspace. Cyberspace provides less costly and quick access to the marine environment when compared to physical entry.⁷¹ As Russell aptly states,

Cyberspace allows information – and attacks – to travel almost instantaneously across vast distances. These attacks occur much faster than humans can react or respond to them...a complex system: one in which numerous independent elements continuously interact and spontaneously organise and reorganise themselves into more and more elaborate structures over time.⁷²

⁶⁷ Lipson *Tracking and Tracing Cyber-Attacks* 51.

⁶⁸ Dombrowski & Demchak "Cyber War, Cybered conflict and the Maritime Domain" 2014 67(2) *Naval War College Review* 70.

⁶⁹ Chronis Kapalidis "Cyber Security Challenges for the Maritime Industry" 30/07/2019. In this article, Chronis opined that Cyber security has been over the last years the first non-natural threat to the global risk landscape according to the World Economic Forum" <https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/> accessed on 22nd January, 2020.

⁷⁰ *Ibid.*

⁷¹ Russell *Cyber Blockades* 2014 12-13.

⁷² *Ibid.*

The uniqueness of its swift occurrence makes understanding, attributing, and reacting to cyber interference complicated.⁷³ It can be launched within split seconds and its impact is felt instantly. Since the shipping industry has embraced information technology, it is responsible for understanding the consequences of a cyber intrusion.

The unique factors of masking the intruder's identity can confuse the victim and intangibility through data modification can create a destructive effect on the target.⁷⁴ Interferers are skilled at hiding their identity by sitting behind a computer to cause havoc, sending their destructive codes through various servers, or erasing their tracks in cyberspace to avoid being traced. A disguise of the origin of the intrusion and various resultant effects of an attack are also responsible for the difficulty in understanding and attributing maritime cyber interference.⁷⁵ These unique features of maritime cyber-attacks need to be considered in determining specific policy guidelines or approaches to protect ships, ports, and oil rigs from imminent threats through anticipatory self-defence.

1.3. Defence Measures against Maritime Cyber-Attack

This refers to steps States can take to secure cyberspace in their territorial seas and within their jurisdiction on the high seas. These steps should comply with relevant international laws. Schmitt's "Tallinn Manual 2.0 on the International Law Application to Cyber Warfare", published in 2017 from a contribution by a renowned international group of experts, has provided a blueprint for applying international law principles on self-defence to maritime cyber security. Mueller and his co-authors published a book in 2006 titled "Striking First: Pre-emptive and Preventive Attack in U.S. National Security Policy", which explains the concept of anticipatory self-defence. They argued that anticipatory self-defence is the use of force by a State to repel a reasonably foreseeable threat or attack that meets the threshold of armed attack.⁷⁶ Some measures for early detection of impending grave cyber-attacks can help to thwart cyber interferences that can threaten States' interests at sea.

⁷³ Rid & Buchanan "Attributing Cyber-attacks" 2015 38 (1-2) *Journal of Strategic studies* 5-6; Brantly *The decision to attack: Military and intelligence cyber decision-making* 2016 89.

⁷⁴ Dinniss *Cyber Warfare and the Laws of War* 2012 Cambridge University Press 65.

⁷⁵ *Ibid.*

⁷⁶ Mueller, Castillo, Morgan, Pegahi and Rosen *Striking First: Pre-emptive and Preventive Attack in U.S. National Security Policy* (2006) 53.

Active cyber defence mechanisms may be employed to prevent looming cyber-attacks. During a Conference on Cyber Conflict in 2014, Dewar explained active cyber defence as proactive actions against the intruder's network to prevent a cyber threat from materialising.⁷⁷ This can be done by using cyber techniques that allow the victim to spot, evaluate, and diminish cyber threats as they arise.⁷⁸ Some of these techniques can be minimally or very aggressive. Hoffman and Levite's "Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyber space?" published in 2017, proposed examples of cyber defence techniques. Examples of minimally aggressive active cyber defence techniques include the use of intrusion-prevention systems, deception techniques to confuse attackers, and isolating the attacker with bait to prevent further intrusion.⁷⁹ Other more aggressive measures include disrupting the servers being used by the intruder, breaking botnets, and getting into the intruder's networks to recover, modify, or expunge stolen data.⁸⁰

Some of the issues that arise when States exercise the right to self-defence include attribution, State responsibility and compliance with the principle of imminence for the justification of anticipatory self-defence. Bruner, in a policy brief titled *Double Standard on Due Diligence in Cyberspace* published in July 2020, explained that:

[t]he principle of due diligence requires that one does not allow his/her cyber infrastructure to be used in a way that harms others.⁸¹

He explains the challenge in navigating through State responsibility when cyber-attacks are launched through State-owned cyber infrastructure especially when States deny sponsorship of the attack.⁸²

1.4. Research Focus

This research aims to determine that anticipatory self-defence can be lawfully invoked in certain instances of breaches of a State's maritime cybersecurity. Despite the debates by some scholars to clarify the international law position on anticipatory

⁷⁷ Dewar "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence" (6th Annual Conference on Cyber Conflict, 2014), NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf (accessed 2018-10-20).

⁷⁸ *Ibid.*

⁷⁹ Hoffman and Levite *Private Sector Cyber Defence: Can Active Measures Help Stabilize Cyber space?* (2017) 8.

⁸⁰ *Ibid.*

⁸¹ Bruner "Double Standard on Due Diligence in Cyberspace" 2020 *Peace Research Centre Prague Policy Brief* <https://www.jstor.org/stable/resrep25308> (accessed on 2020-10-31).

⁸² *Ibid.*

self-defence in the maritime context, there is no universally accepted legal provision for States to rely on in carrying out anticipatory self-defence against imminent maritime cyber-attacks.⁸³ It has been asserted that:

While the use of force in the cyber context poses the challenge of ‘how’ and ‘when’ the existing legal framework regulating the use of force can be applied, it is capable, in principle, of being applied to any type of force that can be qualified as such.⁸⁴

This assertion raises the question as to whether cyber-attacks can qualify as the use of force. It also triggers a debate on the modality of invoking anticipatory self-defence, which falls within the legal framework regulating the use of force.

The application of the right of self-defence in different contexts, including against a maritime cyber-attack (MCA), raises the issues of proportionality and necessity when determining the legitimate approach to invoking this right.⁸⁵ The efficiency of maritime cyber security laws depends heavily on the effective implementation of the laws without sacrificing the victims’ rights to repel an imminent attack. The legal requirements States need to comply with for enforcing their territorial rights should not jeopardise their right to anticipatorily defend against an MCA. Therefore, the main objective of this research is to assess the application of article 51 of the United Nations Charter in the context of maritime cyber law. In the following chapters, the following questions will be examined to achieve the research objective.

1. When does maritime cyber interference meet the requirements to qualify as an attack in terms of the provision of article 51 of the UN Charter?
2. When is a maritime cyber-attack imminent for the purpose of invoking anticipatory self-defence as stipulated by article 51 of the UN Charter and other international instruments on cyber security?
3. When are the requirements for necessity met in terms of satisfying the required conditions for invoking anticipatory self-defence in line with article 51

⁸³ Gill and Ducheine “Anticipatory Self-Defence in the Cyber Context” 2013 89 *International Law Studies* 438 438; Tsagourias “Cyber-attacks, Self-defence and the Problem of Attribution” 2012 *Journal of Conflict and Security Law* 229-244; Schmitt (ed) *Tallinn Manual 2.0 on the International Law Application to Cyber Warfare* (2017) 2ed.; McGhee “Hack, Attack or Whack: The Politics of Imprecision in Cyber Law” 2015 4 *Journal of Law and Cyber Warfare* 13-41.

⁸⁴ Gill and Ducheine 2013 *International Law Studies* 439.

⁸⁵ Kretzmer “The Inherent Right of Self-Defence and Proportionality in *Jus ad Bellum*” 2013 24 *European Journal of International Law* 235 282; the application of the right of self-defence in different contexts including MCA has been debated with the issues of proportionality and necessity arising in determining the legitimate approach to invoking this right.

of the UN Charter, the relevant provisions of the African Union (AU) Convention on Cyber Security and other international conventions on cyber security?

4. What form(s) of anticipatory self-defence against threats to maritime cyber security meet the requirement of proportionality in terms of the UN Charter and other international conventions on cyber security?

These questions will be discussed by focusing on the relevant international legal instruments, International Court of Justice, judgments, and scholarly writings. This research will argue that an MCA can qualify as a threat of armed attack in certain instances, which will permit States to act anticipatorily in self-defence. Since there is no exhaustive list in international law on the types of weapons that can be used to cause an armed attack, States have the right to anticipatorily defend against certain types of imminent MCAs, which can cause loss of lives and damage to property. The unique nature of MCAs to cause enormous damage within seconds while cloaking the attacker's identity will be studied to determine the conditions that should be fulfilled to invoke anticipatory self-defence lawfully. The International Court of Justice (ICJ) has interpreted the provision of article 51 by ruling that acts that cause loss of lives or enormous damage to property are armed attacks. Whether this ICJ's interpretation can be applied to attacks carried out through maritime cyberspace will also be discussed in the following chapters.

Despite the focus of this research being on MCAs launched by a State targeting another State, attacks by non-State actors will be discussed. The threat posed by non-State actors will be discussed regarding the possibility of whether their attacks are attributable to a State or meet the threshold of armed attack in the context of article 51. This discussion about cyber-attacks perpetrated by non-State actors will be limited to their relevance to the legal context of unlawful breach of cybersecurity which are categorised as cybercrimes.⁸⁶ Cybercrimes, in this context, constitutes of cyber-attacks carried out by individuals or a group of persons targeted at another person, a group or the State. The aspect of cybercrimes which falls within the scope of this research is limited to cybercrimes against the State. This includes cybercrimes which target government computer network systems at sea. Greater

⁸⁶ This will be discussed in section 2.3, particularly on pages 37- 41 and on page 101.

emphasis will be placed on the issues relating to when the unlawful conduct of a non-State actor is attributable to a State in chapter 5.

1.5. Research Structure

This thesis is divided into six chapters. Cyber activities that threaten maritime cyber infrastructure will be generally referred to as MCAs. This introductory chapter to the thesis has provided an overview of cyber interference in the marine environment. It has depicted the threat to maritime cyber security in this era by highlighting the increase in and complexity of maritime cyber interferences. The meaning and unique nature of threats to maritime cyber security have been examined with reference to relevant laws. The parameter of this study has been stated pertaining to analysing anticipatory self-defence against an MCA from the *jus ad bellum* perspective. During the analysis, the use of technical terminology on cyber security will be limited to those relevant to the discussion and which can be defined or described. To answer the above research questions, it is important to thoroughly discuss the relevant legal provisions in addressing the issues identified in this chapter.

Chapter two will examine the legal framework of maritime cyber security. It will explain the international legal instruments that are relevant to the subject of maritime cyber security. This lays the foundation for investigating the efficiency and effectiveness of States' application of the provisions of these legal instruments to thwart MCAs. Customary International law on anticipatory self-defence against MCAs will be discussed by assessing State practices on anticipatory self-defence and the relevant decisions of the ICJ. Understanding the position of law that regulates a State's rights, duties, or responsibilities with regard to maritime security, self-defence and related issues such as cyber security, use of force and armed attack, provides the basis for critically analysing legitimate anticipatory defence mechanisms against MCAs.

One of the main issues identified from the discussion in chapter two on the legal framework on maritime cyber security is the use of force. In chapter three, the position of international law on this issue will be applied to the context of maritime cyber security. The relationship between cyber acts and force, as stated in article 2(4) of the UN Charter, will be examined. The scope of MCA will be evaluated as well as how force can be exercised through cyber means. It will be determined

whether these unlawful cyber activities, whether passive or active, can be described as the use of force and a violation of a State's maritime cyber security despite varying degrees of probable or actual damage or losses that are caused.

Chapter four will analyse the issue of armed attack as identified when discussing the legal framework on maritime cyber security from chapter two and MCA as use of force in chapter three. The concept of use of force and armed attack are not mutually exclusive. Despite their seemingly overlap in discussing them because they are provided for by separate sections of the UN Charter and interpreted with reference to each other, the result of their interpretation births different legal implications. This is so because not all use of force amounts to an armed attack, but an armed attack has the element of the use of force. In this chapter, the principles of armed attack will be applied to the concept of maritime cyber-attack. The possibility of classifying maritime cyber-attack as an armed attack will be determined. It will assess how MCAs meet the threshold of being classified as "imminent attack". It will analyse how unlawful cyber incidents at sea that threaten cyber security (by attempting to acquire, obliterate, change, eliminate, embed, and divulge information without authorised access) may be qualified as armed attacks.

After identifying the laws and analysing the security issues of use of force and armed attack, it is necessary to discuss the legitimate options available to States in self-defence. A critical examination of the kind of measures that can be legally taken in self-defence and anticipatory self-defence will be done in chapter five by focusing on those involving the use of force and other active and passive means of defending ships against MCAs. It will discuss the lawful forms of individual and collective self-defence against MCA. It will discuss possible limitations by article 51 of the UN Charter on invoking anticipatory self-defence against maritime cyber-attack. An analysis of State practices pertaining to interpretation, implementation and compliance with existing maritime cyber security regulations, treaties and best practices will be done. The challenges faced by States during implementation and compliance will be examined. The analysis will focus on the legal requirements of imminence, necessity, and proportionality in defending against an imminent 'maritime cyber armed attack' (MCAA). It will examine specific challenges that can be faced by States when invoking anticipatory self-defence against cyber-attacks on ships, especially on the issues of attribution and jurisdiction.

Chapter six will articulate the key findings of this thesis in line with the research questions. Recommendations will be made regarding the amendment of existing laws and practice directives in the light of the discussions in the preceding chapters of this thesis.

1.6. Limitations

To understand the nature of maritime cyber-attack with the intent of lawfully repelling them anticipatorily, it is necessary to determine whether it constitutes a form of armed attack. From the *jus ad bellum* perspective, an armed attack is seen as a circumstance that may arise to activate the right to self-defence⁸⁷ which includes anticipatory self-defence.⁸⁸ It is the right of a State to use force as a necessity to defend itself against an armed attack. The *jus ad bellum* principle requires an assessment of a current security situation of a State in order to justify the right to act. In exploring this principle, this research will focus on anticipatory self-defence from the perspective of *jus ad bellum* with regard to determining whether MCAs can amount to an armed attack. The focus of this study will be mainly on *jus ad bellum* with limited reference to *jus in bello* on the principle of proportionality and necessity. The legal requirements of proportionality and necessity are relevant to how anticipatory self-defence should be carried out to remain legitimate. This limited reference will guide States on how to exercise their right to defend their territorial integrity lawfully. Also, the technical nature of the Internet will not be discussed in detail, but reference will be made to technical terms which are relevant to this research.

Attacks by non-State actors which are not attributable to a State will be discussed as types of unlawful cyber operations classified as crimes. As previously stated,⁸⁹ cybercrimes are types of cyber-attacks perpetrated by non-State actors which fall within the scope of my research to the extent that the target of the attack is the State.

⁸⁷ Schmitt "Attack as a Term of Art in International Law: The Cyber Operations Context" 2012 *4th International Conference on Cyber Conflict*, 285.

⁸⁸ Schmitt 2012 *4th International Conference on Cyber Conflict* 286; notably, the international law principles on anticipatory self-defence are centered on proportionality, necessity, and imminence.

⁸⁹ Section 1.4 Research Focus.

Therefore, the main discussion on non-State actors will entail when their cybercrimes are attributable to a State, targeted at a State, and the options available to States in anticipatory self-defence.

CHAPTER 2: THE LEGAL CONTEXT OF MARITIME CYBER SECURITY

2.1. Introduction

Anticipatory self-defence against a threat to the maritime cyber infrastructure of a State is one aspect of maritime security that requires more investigation. This investigation requires an understanding of maritime cyber security, its significance to national security, and the legal framework regulating it. In this chapter, the legal framework of maritime cyber security will be studied by assessing the international legal instruments relevant to maritime cyber security. This will be done by identifying and discussing the legal provisions and State practices and their relevance to determining the legality of anticipatory self-defence against a cyber-attack. The identified legal provisions relevant to maritime cyber security will be evaluated in the subsequent chapters to determine whether States have the right to anticipatory self-defence against maritime cyber-attacks (MCAs). It will be established that international law principles on self-defence can be applied to maritime cyber security.

The content of this chapter lays the foundation for examining the main research questions about viewing maritime cyber-attack as the use of force and an armed attack in the subsequent chapters. The judicial interpretation of the legal instruments identified below and scholarly debates about the legality and challenges of anticipatorily defending against a maritime cyber-attack will be analysed in chapters four and five, respectively. In this chapter, the laws and guidelines that are relevant to maritime cyber security will be identified. The identified provisions of these instruments will be explained to portray their relevance to defending the maritime cyber security of a State.

The UN Charter, the Convention on Law of the Sea, International Maritime Organisation guidelines, Budapest Convention on Cyber Crime, European Union General Data Protection Regulation, the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) Convention and the African Union Convention on Cyber Security and Personal Data Protection will be discussed. Customary International law on anticipatory self-defence will also be identified as a source of law for regulating maritime cyber security. As discussed in the following chapters, identifying these relevant legal instruments and rules of customary international law as sources of maritime cyber security laws will provide legal knowledge for

discussing whether and how States can anticipatorily defend against a maritime cyber-attack.

Maritime cyber security laws can be identified by reviewing some legal instruments and scholarly writings which provide the legal requirements for addressing the complex issue of regulating maritime cyber security threats. There is no universal treaty that specifically regulates maritime cyber security. States must rely on provisions from several legal instruments to formulate policies on the legal requirement for determining and invoking their right to self-defence.⁹⁰ These legal instruments are all relevant sources of arguments in understanding the legal framework for regulating maritime cyber security. These instruments can be referred to as international laws because they regulate the relationships between States. Despite the interconnection between States in cyberspace, some scholars argue that international law has nothing to do with cyberspace.⁹¹ According to Mary O'Connell,

The vast majority of cyber-attacks are not carried out by government-sponsored hackers but by criminals intending to steal business secrets and financial information. Therefore, there have been strong attempts to discourage governments characterising the Internet as being seen a war-fighting problem.⁹²

This view downplays the necessity of applying international law to cyberspace. It argues for reliance on domestic laws and sees unlawful activities in cyberspace as crimes. It does not consider other types of cyber-attack targeting critical operating systems, including navigation and communication systems aboard a flagship. It is submitted that O'Connell's opinion does not acknowledge cyber warfare as an aspect of international law that can trigger the right to self-defence. It focuses on domestic laws as a source of maritime cyber security.

⁹⁰ The sources of maritime cyber security laws include the UNCLOS; United Nations Charter, International Court of Justice rulings; International Maritime Organization; Schmitt (ed) *Tallinn Manual 2.0 on the International Law Application to Cyber Warfare* (2017) 2ed ; Sofaer *et al* "Cyber Security and International Agreements' Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy" <http://www.nap.edu/catalog/12997.html> (accessed 2018-02-20).

⁹¹ O'Connell "Cyber Mania" in *Cyber Security and International Law: Meeting Summary 2012* Chatham House <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf> (accessed 2019-02-19) .

⁹² O'Connell <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf> 3.

From another perspective, Egan sees cyberspace as a battleground that can be regulated by international law and recognises the inherent right of States to defend against attacks in cyberspace.⁹³ He acknowledges the applicability of the principles of international law, especially on the use of force and self-defence.⁹⁴ Although States can differ in their approach on specific cyber security issues such as MCAs, it is submitted that maritime cyber security is a subject that can affect the relationship between States due to the blurriness of territorial demarcation in cyberspace. Egan argues that:

Recognising the applicability of existing international law as a general matter, however, is the easy part, at least for most like-minded nations. Identifying how that law applies to specific cyber activities is more challenging, and States rarely articulate their views on this subject publicly.⁹⁵

This argument confirms the lack of universal clarity on the interpretation of the legal framework regulating maritime cyber-attacks. It is submitted that despite the existence of laws that can be adapted to address maritime cyber-attacks, the words of these instruments appear to allow their flexible application to suit various national interests.

2.2. International Legal Instruments on Maritime Cyber Security

International legal instruments refer to international laws regulating the maritime cyber relations between States, such as the United Nations Convention on Law of the Sea, Budapest Convention on Cyber Crime, European Union General Data Protection Regulation. Some domestic laws also make provisions that can be applied to maritime cyber incidents. Although they are not the direct focus of this discussion, their significance stems from the translation of their core values as from developed States based on the provision of article 38(1)(c) of the 1945 Statute of the International Court of Justice on sources of law in international laws.⁹⁶ Although these listed international legal instruments are not specifically international laws on maritime cyber security, they have formed the basis for adaptation to the evolving

⁹³ United Nations General Assembly “United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” (2015) <https://undocs.org/A/70/174> (accessed 2020-06-03) 12.

⁹⁴ Egan “International Law and Stability in Cyberspace” 2017 35 *Berkeley Journal of International Law* 169170-171.

⁹⁵ *Ibid.*

⁹⁶ Article 38 (1)(c) of the Statute of the International Court of Justice 1945, available at <https://www.icj-cij.org/en/statute> (accessed 2020-07-26)).

contemporary threat of cyber-attack against maritime infrastructures.⁹⁷ Some judicial decisions and scholarly writings by renowned scholars⁹⁸ can also serve as sources of international law on maritime cyber security.

2.2.1. The United Nations Convention on Law of the Sea

The United Nations Convention on Law of the Sea (UNCLOS)⁹⁹ regulates State responsibilities, duties, and rights in the maritime domain. It was intended to contribute immensely to the development and evolution of the law of the sea by being comprehensive in scope.¹⁰⁰ It is referred to as ‘the constitution for the oceans’.¹⁰¹ In line with its objectives and purpose as can be deduced from its preamble, the UNCLOS provides for the legal rights and duties required by States when carrying out maritime activities to ensure peace and security at sea.¹⁰² Its provisions address various issues arising within the maritime jurisdiction of States. The issues include general provisions on the legal status¹⁰³ and limits of the territorial sea,¹⁰⁴ the rules applicable for innocent passage of all ships¹⁰⁵, and specific rules that apply to merchant ships, commercial government ships,¹⁰⁶ warships, and non-commercial ships.¹⁰⁷ It also makes provisions for issues relating to exclusive economic zone¹⁰⁸, continental shelf¹⁰⁹ and the high seas.¹¹⁰ Some of these provisions can be relevant in determining incidental issues arising when States take steps to defend against MCA. Such issues can include perception of a maritime

⁹⁷ Lotrionte “Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law” 2018 3(2) *The Cyber Defence Review* 73 75.

⁹⁸ Article 38 (1)(d) of the Statute of the International Court of Justice of 1945, available at <https://www.icj-cij.org/en/statute> accessed 2020-07-26).

⁹⁹ 1833 UNTS 3, (1982) 21 ILM 1261. Adopted: 10.12.1982; EIF: 16.11.1994.

¹⁰⁰ Boyle “Further Development of the Law of the Sea Convention: Mechanisms for Change” 2005 54(3) *The International and Comparative Law Quarterly* 563 563.

¹⁰¹ Remarks by Koh, reproduced in UN *The Law of the Sea: Official Text of the UNCLOS* (London 1983) xxxiii; Analysis by Scott “The UNCLOS as an International Regime”, a paper given at the 3rd Verzijl Symposium, Utrecht, (2004).

¹⁰² Hulme “Preambles in Treaty Interpretation” 2016 164(5) *University of Pennsylvania Law Review* 1281 1300: “...preambles are more frequently cited as sources or evidence of a treaty’s object and purpose”

¹⁰³ Article 2 of UNCLOS.

¹⁰⁴ Articles 3-16 of UNCLOS.

¹⁰⁵ Articles 17-26 of UNCLOS.

¹⁰⁶ Articles 27-28 of UNCLOS.

¹⁰⁷ Article 29-32 of UNCLOS.

¹⁰⁸ Part V of UNCLOS.

¹⁰⁹ Part VI of UNCLOS.

¹¹⁰ Part VII of UNCLOS.

security threat, use of forceful or non-forceful means to repel the threats and attribution of MCAs to States.

Article 17 provides for the right of innocent passage through a State's territorial sea. This provision is in line with the principle of customary international law on the right to allow peaceful passage of ships of all States through the territorial sea of coastal States.¹¹¹ This right is explained in subsequent sections, which can be relied upon when determining which acts do not amount to 'peaceful passage'. It includes incidents that can be classified as a threat or use of force against the coastal State's sovereignty, territorial integrity, or political independence.¹¹² These incidents include the use of any kind of weapon to violate the territorial integrity of the coastal State.¹¹³ Hostile acts that threaten maritime security are stated in article 19(2) as:

(a) any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or ...violation of the principles of international law embodied in the Charter of the United Nations; (b) any exercise or practice with weapons of any kind; (c) any act aimed at collecting information to the prejudice of the defence or security of the coastal State; (d) any act of propaganda aimed at affecting the defence or security of the coastal State; ... (j) the carrying out of research or survey activities; (k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.¹¹⁴

It is submitted that the above provision can be interpreted to include maritime cyber-attack, which is as a form of a hostile act at sea.¹¹⁵ This is because cyber hostilities against coastal States which involve gaining unauthorised access to vital security information of a State can, under certain circumstances, be seen as a threat to the sovereignty, territorial integrity or political independence of that State. If the circumstance is such that it makes the State's security network vulnerably to cyber-attacks that can lead to grave consequences, it can be deemed as an abuse of the right of innocent passage. The right of innocent passage is lost when a cyber intrusion in the communication or defence systems of a coastal State is detected and perceived as a security threat.¹¹⁶ This is because the exercise of this right can be

¹¹¹ Abbas "The Principle of the Right of Innocent Passage" in *Assessing the 'Law of the Sea': A Case for the US' Right of Passage in the Strait of Hormuz* (2020) 4.

¹¹² Article 19 of UNCLOS.

¹¹³ Article 19(2)(b) of UNCLOS.

¹¹⁴ *Ibid.*

¹¹⁵ *Ibid.*

¹¹⁶ Article 19(2)(k) of UNCLOS.

seen as conditional upon compliance with the lawful standard of behaviour.¹¹⁷ The cyber intrusion changes the 'innocent' status accorded to a State whose flag a passing ship flies when passage becomes prejudicial to the security of the coastal State.¹¹⁸ For instance, the use of 'cyber weaponry' as a medium to conduct unauthorised cyber intrusion under the guise of intelligence gathering can be perceived as a threat to the maritime cyber security of the host coastal State.¹¹⁹

Article 25(1) provides for the right of the coastal State not to allow the passage of a vessel that has violated the right of innocent passage. This is an explicit option provided by UNCLOS to victim States. Can this option sufficiently address the breach of security resulting from MCAs? In the context of MCAs, the victim State may need to seize an opportunity to be proactive in defending its national security. If the victim State relies solely on article 25(1), it becomes challenging to avert an adverse consequence resulting from the violation of the right of passage. This is because the victim's reaction occurs after the attack has been launched. This means that the victim is given the option of carrying out a countermeasure to address an established breach of maritime security. The introductory chapter states that maritime cyberspace is a crucial aspect of maritime security due to increasing ICT reliance in the shipping industry. The absence of specific provisions in the UNCLOS on maritime cyber security creates room for the deductive application of its provisions for regulating maritime security. This leaves States without specific guidance on the steps to tackle incidental issues arising from self-defence, such as attribution of State responsibility as well as anticipatory acts of self-defence.

Article 31 provides that flag States must bear international responsibility for any loss or damage caused by their warships or other non-commercial government ships. This can be implied to include damages resulting from unlawful activities carried out onboard their ships with external consequences. For example, such unlawful activities can be cyber-attacks that threaten the cyber defence network of a State or other critical infrastructure of a State which are ICT-reliant. This interpretation can create a legal foundation for attribution and justification to defend against an MCA.

¹¹⁷ Vecchio (ed) *International Law of the Sea: Current Trends and Controversial Issues* (2014) 206.

¹¹⁸ Tanaka *The International Law of the Sea* 2ed (2015) 87; Article 19(1)(2) UNCLOS; Ahmed "International Law of the Sea: An Overlook and Case Study" 2017 8 *Beijing Law Review* 21 28-29.

¹¹⁹ *Ibid.*

It is submitted that when an MCA by a State results in loss of lives or damage to critical infrastructures of another State, the attacking State must accept liability for their unlawful act. The victim-State, on its part, can protect its maritime security from the attacking State in the way and manner it chooses, but within the confines of the law. Every State has a right of navigation on the high seas.¹²⁰ This right can be infringed upon through a cyber-attack under the guise of intelligence gathering or outright unauthorised cyber intrusion. Can this breach of the right of navigation be interpreted as a violation of the jurisdiction of the State, which has its flag flying aboard the targeted ship? Article 94 provides for the international duties of the flag of a State, which includes its jurisdiction over a ship flying its flag and its duty to ensure safety at sea. It states that:

1. Every State shall effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag...3. Every State shall take such measures for ships flying its flag as are necessary to ensure safety at sea with regards, inter alia, to: (a) the construction, equipment and seaworthiness of ships; (b) the manning of ships, labour conditions and the training of crews, taking into account the applicable international instruments; (c) the use of signals, the maintenance of communications and the prevention of collisions...

In carrying out these duties, ensuring the safety of their ship encompasses protection from kinetic and other forms of attacks such as cyber-attacks.¹²¹ Based on the provision of article 94 of UNCLOS, States are required to take the necessary steps to ensure that their flagship's operating and IT systems are protected from all forms of attacks.¹²² The steps taken by States to achieve this can be by way of self-defence or by taking other non-forceful measures. With ships' increasing reliance on information technology, the safety measures required of flag States need to include protection of maritime cyberspace.

The above provisions of UNCLOS are relevant in guiding States to understand that they have jurisdiction over various safety issues concerning their flagship, including cyber security issues. These provisions can serve as the legal foundation for States who wish to take anticipatory steps to ensure the safety of their critical maritime

¹²⁰ Article 90 of UNCLOS.

¹²¹ Hosanee "A Critical Analysis of Flag State Duties as Laid Down under Article 94 of the 1982 United Nations Convention on the Law of the Sea" *The United Nations-Nippon Foundation Fellowship Programme* (2009–2010) https://www.un.org/Depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/hosanee_0910_mauritius.pdf (accessed 2020-07-18) 23 .

¹²² Article 94(3) of UNCLOS.

infrastructure and personnel at sea. They confirm the significance of protecting the ship's communication and navigation systems because they are crucial aspects of preventing accidents.¹²³

2.2.2. Regional Laws on Cyber Security

A maritime cyber-attack is an unlawful act that requires a legal framework to ensure that its perpetrators are held accountable within the confines of the law. In determining the issue of lawful response to a criminal cyber-attack, that is, where MCA is viewed from the perspective of a crime, there are applicable regional laws. The Council of Europe's Convention on Cybercrime often referred to as the Budapest Convention, is a relevant instrument on cyber security to be appraised. This convention has been described as the only multilateral, legally binding instrument that deals with cybercrime.¹²⁴ This assertion can appear inapplicable to the current reality even though the African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014, has not entered into force.¹²⁵ This means that it is not legally binding until it enters into force.¹²⁶ It is submitted that the Budapest Convention correctly qualifies as the only multilateral legally binding instrument on cybercrime, out of which many countries have enacted domestic laws to combat cybercrime.

The Budapest Convention's preamble states that its main objective is to criminalise unlawful cyber acts and facilitate detection, investigation, and prosecution.¹²⁷ The significance of criminalising unlawful cyber acts is that it creates a *locus standi* to prosecute an offence that is known to law. This allows prosecutors to establish the criminal liability of the perpetrators of the crime. It can be applied to maritime cyber

¹²³ Hosanee *The United Nations-Nippon Foundation Fellowship Programme* (2009–2010), https://www.un.org/Depts/los/nippon/unfff_programme_home/fellows_pages/fellows_papers/hosanee_0910_mauritius.pdf (accessed 2020-07-18) 32.

¹²⁴ Jurich "Cyberwar and Customary International Law: The Potential of a 'Bottom-Up' Approach to an International Law of Information Operations" 2008 9 *Chicago Journal of International Law* 275 283.

¹²⁵ African Union "Convention on Cyber Security and Personal Data Protection" (2014) https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 2020-07-18) .

¹²⁶ CCDCOE "African Union" (undated) <http://ccdcoe.org/organisations/au/> (accessed 2020-06-10).

¹²⁷ Stevens "Internet War Crimes Tribunals and Security in an Interconnected World" 2009 18 *Transnational Law and Contemporary Problems* 657 685.

security because individuals can commit cybercrimes against a ship, submarine, or persons on board. This is an essential aspect of maritime cyber security.

Articles 2-11 of the 2001 Budapest Convention on Cybercrime list several offences classified as forms of cyber interference or attacks. They are classified into a) offences against the confidentiality, integrity and availability of computer data and systems; b) computer-related offences; c) content-related offences; and d) offences related to infringements of copyright and related rights. The vulnerability of navigation and operation systems in the territorial seas to 'offences against the confidentiality, integrity and availability of computer data and systems such as illegal access, interception, data and system interference'¹²⁸ can lead to grave consequences. These grave consequences caused by MCAs can include collision due to altering navigational operation data, explosions due to operations systems interference at an oil rig and illegal access to critical security codes for launching weapons from a ship or submarine. States should have laws that can be used to determine the criminal liability of the perpetrators of those crimes and defend against imminent cyber-attacks.

The significance of the Budapest Convention is that it provides States with the option of addressing unlawful cyber incidents that fall below the threshold of armed attack when the aggressor is an individual with no proven State-sponsorship. Such aggressors are viewed from the criminal law perspective. Unlawful MCAs committed by individuals is a breach of maritime cyber security, and when attributed to States, the applicable laws should be those that regulate the relations between States. It has been argued that the Budapest Convention does not provide a specific global standard for adequately responding to the threat posed by cybercrime.¹²⁹ It allows member States to adopt their own regulations and take measures that they deem fit. This flexibility seems to be the case with most conventions, thereby providing opportunities for improvement and incorporation into their domestic laws. The Budapest Convention on cybercrime is not recognised as reflecting or having

¹²⁸ Articles 2-5 2001 of the Budapest Convention on Cybercrime.

¹²⁹ Stahl 2011 *Georgia Journal of International and Comparative Law* 264; Dobbins, Solomon, Chase, Henry, Larrabee, Lempert, Liepman, Martini, Ochmanek and Shatz *Choices for America in a Turbulent World: Strategic Rethink* (2015) 67, states that China and Russia have rejected the Budapest Convention as a development international norm on cybersecurity.

generated customary international law.¹³⁰ It lacks specific implementation guidelines because it only offers wide-ranging guiding principles and proposals like other guidelines and recommendations.¹³¹

Another critical regional law is the 2014 AU Convention on Cyber Security and Personal Data Protection (AU Convention on Cyber Security). This Convention defines critical cyber infrastructure as:

cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace.¹³²

Ships, ports, and marine installations fit into this definition due to their increasing reliance on information technology for their operation and importance to economic stability, national security, and international stability of coastal and flag States. For example, the navigation and communication systems of a ship can be referred to as critical cyber infrastructure of the marine sector of the State.¹³³ Ships and submarines can carry weapons that are essential to national security. An MCA occurring against them such that it disrupts their navigation system can lead to collision and explosion. States should be able to prevent such incidents.

The convention provides alternative rules and regulations for when an MCA does not meet the threshold for the use of force in self-defence. It provides that States should collaborate with stakeholders to develop cyber security policy by identifying the risks and outlining the objectives for implementing relevant principles.¹³⁴ This implies that States need to adopt the strategies they deem appropriate and adequate to implement this national security policy. The flexibility of this provision permits a subjective approach to addressing the threats against maritime cyber security. States will tend to lean towards addressing the issues that may arise, especially anticipatory self-defence against MCA, from the perspective that supports their foreign policies and national interests.

¹³⁰ Jurich 2008 *Chicago Journal of International Law* 289.

¹³¹ Stahl 2011 *Georgia Journal of International and Comparative Law* 265.

¹³² Article 1 of the African Union Convention on Cyber Security and Personal Data Protection of 2014.

¹³³ Critical Infrastructure Sectors “Transportation Systems Sector” <https://www.cisa.gov/transportation-systems-sector> (accessed 2020-10-23) .

¹³⁴ Article 24 of the African Union Convention on Cyber Security of 2014.

States' compliance with developing a national cyber security framework depends on establishing relevant legislations and institutions¹³⁵ to protect critical infrastructure, including maritime infrastructure, against damage. In determining and anticipating self-defence against MCA, the AU has mandated the adoption of cyber security monitoring structures.¹³⁶ Therefore, the onus is on States to develop a national framework to respond to anticipated maritime cyber security threats.¹³⁷ However, this AU mandate to legislate and establish relevant institutions must be within the confines of the relevant principles of international law, including international customary law.¹³⁸ This safeguard provision appears to regulate States' potential liberalism or conservatism in their approach to defend their maritime interests against cyber-attacks anticipatorily. A member State has no legal basis for using force in defending against a State-sponsored breach of its cyber security since the AU Convention on Cyber Security provides for the use of peaceful dispute resolution mechanisms to address disputes that may arise between States. It is submitted that this provision precludes the use of force to defend against imminent MCA despite the probability that the dispute to be settled can arise from an aggressor's use of force.¹³⁹

Also, the African Union has developed a 2050 Africa's Integrated Maritime Strategy, which acknowledges, as stated above, a similar description of threats to maritime security by including threats that affect the crude oil supply chain.¹⁴⁰ Likewise, the European Union has stated that maritime security:

is understood as a state of affairs of the global maritime domain, in which international law and national law are enforced, freedom of navigation is guaranteed and citizens, infrastructure, transport, the environment and marine resources are protected.¹⁴¹

These descriptions of maritime security reflect the similarity in the objective to secure the maritime domain but portray an absence of a unified approach to ensuring maritime security. The lack of specific actions that can be lawfully taken to secure

¹³⁵ Article 25(4) of the African Union Convention on Cyber Security of 2014.

¹³⁶ Article 27 of the African Union Convention on Cyber Security of 2014.

¹³⁷ *Ibid.*

¹³⁸ Article 33 of the African Union Convention on Cyber Security of 2014.

¹³⁹ Article 34 of the African Union Convention on Cyber Security of 2014

¹⁴⁰ African Union "2050 Africa's Integrated Maritime Strategy" www.cggrps.org/wp-content/uploads/2050-AIM-Strategy_EN.pdf (accessed 2020-02-10).

¹⁴¹ Council of the European Union European Union Maritime Security Strategy (11205/14) (24 June 2014) 2.

the maritime domain creates room for flexibility in interpretation to accommodate evolving threats such as cyber-attacks. It also allows States to choose their actual line of action, which can always be justified as exercising the right to safeguard maritime security.

2.2.3. Suppression of Unlawful Acts Against the Safety of Maritime Navigation Convention and its Additional Protocol

As with many international legal instruments, not all relevant issues, such as maritime security, were exhaustively addressed in the UNCLOS. As a result of this limitation, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) was adopted in 1988.¹⁴² The main objective of this treaty is to create an avenue for determining the criminal liability of the person who commits an illegal act against a vessel.¹⁴³ These illegal acts which are likely to endanger safe navigation and peoples' lives include the intimidation or seizure of ships by force, violent acts against the ship or persons onboard ships, the placing of devices on board a ship through any means to cause damage or interfere with navigational facilities of a ship and altering communication data.¹⁴⁴ This SUA provision can be interpreted to include MCA as a dangerous illegal act when it threatens lives aboard a ship and jeopardises the safe navigation of ships.

Also, article 13 provides that States should work together to prevent these unlawful acts from originating in their territories. This provision creates a legal obligation on States to prevent and defend against unlawful acts which threaten maritime security. It emphasises the requirement for interrelations between States to ensure that perpetrators do not have an enabling environment to launch MCAs. States have the responsibility to effectively control their cyberspace by ensuring that it is not exploited or used as a medium to launch an attack against another State. As aptly stated in the Tallinn Manual,

¹⁴² <https://www.imo.org/en/About/Conventions/Pages/ListOfConventions.aspx> (accessed 2020-06-05); 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) (1678 UNTS 222, (1988) 27 ILM 672, (1988) 11 LOSB 14; adopted: 10.03.1988; EIF: 01.03.1992).

¹⁴³ *Ibid.*

¹⁴⁴ Article 3 of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) (1678 UNTS 222, (1988) 27 ILM 672, (1988) 11 LOSB 14; adopted: 10.03.1988; EIF: 01.03.1992).

A State must exercise due diligence in not allowing its 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.¹⁴⁵

The cyber infrastructures under a State's governmental control include maritime cyber infrastructures such as flag ships over which flag States have jurisdiction¹⁴⁶

In 2005, the SUA Convention was amended through an additional protocol.¹⁴⁷ The 2005 SUA protocol expanded the list of unlawful acts against navigation and the right to repel such threats. According to article 3*bis* of the protocol, an offence is committed:

(a) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act: (i) uses against or on a ship or discharges from a ship any explosive, radioactive material or BCN weapon in a manner that causes or is likely to cause death or serious injury or damage; or (ii) discharges, from a ship, oil, liquefied natural gas, or other hazardous or noxious substance,... in such quantity or concentration that causes or is likely to cause death or serious injury or damage; or (iii) uses a ship in a manner that causes death or serious injury or damage; or (iv) threatens, with or without a condition, as is provided for under national law, to commit an offence...¹⁴⁸

All these provisions are relevant to the subject of maritime cyber security because MCAs, such as malicious software attacks,¹⁴⁹ can be a means through which all the above-listed offences are committed. Given the increased reliance on ICT in the shipping industry, it is submitted that unlawful cyber activities in the territorial seas and high seas can be committed by persons against a ship and marine installations. Such acts can have fatal consequences such as deaths, explosions, collisions, and the discharge of weapons of mass destruction at sea. When they are State-sponsored, the victim State should hold the aggressor State responsible under international law.

¹⁴⁵ Schmitt *Tallinn Manual* 2.0 30.

¹⁴⁶ Schmitt *Tallinn Manual* 2.0 62.

¹⁴⁷ This provided for three new categories of offences: using the ship as a weapon, proliferation of weapons of mass destruction on the high seas and transporting an alleged offender who violated the UN Anti-terrorism Convention.

¹⁴⁸ Article 4(5) of the, 2005 Protocol to the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005 Protocol to SUA) (adopted: 14.10.2005; EIF: 28.07.2010;

¹⁴⁹ Norton "Malware Attacks: What you need to know" (undated) <https://us.norton.com/Internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html> (accessed 2021-11-30) - a malware attack is when cybercriminals create malicious software that's installed on someone else's device without their knowledge to gain access to personal information or to damage the device. Different types of malware include viruses, spyware, ransomware, and Trojan horses.

Also, the 2005 Protocol to SUA acknowledges the right of flag States to defend against all forms of maritime attacks with the conditions of necessity and proportionality.¹⁵⁰ It provides that:

the use of force shall be avoided except when necessary to ensure the safety of its officials and persons on board, or where the officials are obstructed in the execution of the authorised actions. Any use of force pursuant to this article shall not exceed the minimum degree of force which is necessary and reasonable in the circumstances.

This provision asserts the requirement to comply with the customary international law on self-defence. It can be interpreted in the context of the use of force by a State or against an individual in self-defence. It is submitted that unlawful interference with the safety of maritime navigation can be a justification for the use of force. In line with the objectives of this treaty, States can use force to ensure the safe navigation of the ship and safety on board in certain circumstances. The threat to safety at sea can occur because of an MCA, necessitating a proportional use of force. The necessity to use force can arise when the offences listed in article 4(5) of the protocol are committed through unlawful cyber operations.

2.2.4. The International Maritime Organisation's Guidelines on Maritime Cyber Security

The International Maritime Organization (IMO), formerly known as the inter-Governmental Maritime Consultative Organisation, is a specialised agency of the United Nations that ensures best practices on maritime security matters.¹⁵¹ IMO Guidelines on maritime cyber risk management aims to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Maritime Safety Committee (MSC) is the foremost technical body of the organisation.¹⁵² Its functions include:

to consider any matter within the scope of the Organisation concerned with aids to navigation, construction and equipment of vessels, manning from a safety

¹⁵⁰ Article 8(2) of the 2005 Protocol to SUA.

¹⁵¹ Article 1(a) of the 1948 Convention on the International Maritime Organization (entered into force in 1958).

¹⁵² International Maritime Organization "Structure of IMO" <http://www.imo.org/en/About/Pages/Structure.aspx#6> (accessed 2020-06-05) ; the Organization consists of an Assembly, a Council and five main Committees: the Maritime Safety Committee; the Marine Environment Protection Committee; the Legal Committee; the Technical Cooperation Committee and the Facilitation Committee and a number of Sub-Committees support the work of the main technical committees.

standpoint, rules for the prevention of collisions, handling of dangerous cargoes, maritime safety procedures and requirements...¹⁵³

IMO Guidelines on maritime cyber risk management aims to safeguard shipping from current and emerging cyber threats and vulnerabilities. MCA is a matter that falls into the above-listed issues that the Maritime Safety Committee is concerned with. One of the issues in its current agenda is cyber security.¹⁵⁴ This makes it relevant as a source of regulating maritime cyber security. In June 2017, the MSC adopted a resolution on Maritime Cyber Risk Management in Safety Management Systems. It encouraged States and other stakeholders to ensure that cyber risks are appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

The standards and IMO guidelines regulating the right to respond to maritime threats are reflected in the 1974 International Convention for the Safety of Life at Sea (SOLAS) as amended. This convention is referred to as the most important treaty on the security of merchant ships.¹⁵⁵ It was amended in 2004 to include the International Ship and Port Facility Code (ISPS Code).¹⁵⁶ As aptly reported, this safety measure “requires [S]tates to have a methodology for security assessments to ensure that there are plans and procedures in place to respond to a security threat”.¹⁵⁷ This code is intended to enhance the security of ships and ports, given the contemporary challenges of terrorism and cyber-attacks. It comprises comprehensive security-related requirements for States, port authorities and shipping companies. The IMO regulations and guidelines are designed to help member States design and improve their maritime security strategy.¹⁵⁸

It is submitted that since these IMO guidelines provide States and other stakeholders with strategies and standards for security risk assessment and management to ensure safety at sea, it can serve as a source of maritime security law. It stands as

¹⁵³ *Ibid.*

¹⁵⁴ *Ibid.*

¹⁵⁵ <https://www.imo.org/en/OurWork/Security/Pages/GuideMaritimeSecurityDefault.aspx> (accessed 2020-06-05).

¹⁵⁶ Safety4sea “Security Measures: A brief Review of ISPS Code Implementation” <https://safety4sea.com/cm-security-measures-a-brief-review-of-isps-code-implementation/> (accessed 2020-01-31).

¹⁵⁷ Fink *Meeting the Challenge: A Guide to United Nations Counterterrorism Activities*. Report of International Peace Institute (2012) 80-82.

¹⁵⁸ *Ibid.*

an authority that States can rely upon in deciding to apply reasonable force to repel an imminent threat. States can rely on its guidelines for direction in assessing an imminent threat and the necessary step to repel it.

2.2.5. The UN Charter and the Judicial Interpretation on the Use of Force and Armed Attack

One of the main objectives of the UN is to maintain global peace and security. Its provisions are interpreted by the ICJ, which is its principal judicial organ.¹⁵⁹ The relevance of its provisions to maritime security law is based on peaceful relations between States and the protection of their territorial rights. The UN Charter, among other issues, legitimises the right of a State to repel unlawful acts that threaten its territorial rights. The UN Charter is one of the relevant legal instruments regarding its provision for self-defence. However, its interpretation has created scholarly contributions from different perspectives, especially on anticipatory self-defence in the cyber context.¹⁶⁰ It has been asserted that:

While the use of force in the cyber context poses the challenge of ‘how’ and ‘when’ the existing legal framework regulating the use of force can be applied, it is capable, in principle, of being applied to any type of force that can be qualified as such.¹⁶¹

This triggers the debate on the modality of invoking anticipatory self-defence, which falls within the legal framework for regulating the use of force. The significance of the UN Charter and its judicial interpretation of maritime security is that it guides States in taking the legitimate steps to defend their maritime rights and interests without violating the principles of international law on the use of force and self-defence. These principles are evidenced by customary international law, which is one of the primary sources of international law.¹⁶² Customary international law arises from general State practices which create legal obligations for States to abide by. For example, the *Caroline* case of 1837 forms the foundation for the legal requirement of imminence, necessity and proportion when acting in self-defence. A summary of this

¹⁵⁹ Article 92 of the 1945 UN Charter.

¹⁶⁰ Gill and Ducheine 2013 *International Law Studies* 438; Tsagourias 2012 *Journal of Conflict and Security Law* 229-244; Schmitt (ed) *Tallinn Manual 2.0 on the International Law Application to Cyber Warfare* 2ed (2017) 375.

¹⁶¹ Gill and Ducheine 2013 *International Law Studies* 439.

¹⁶² Article 38 of the Statute of the International Court of Justice.

case is that British troops invaded the U.S. territory and destroyed the steamboat Caroline in 1837.¹⁶³ This incident led to the formulation of conditions to be fulfilled to justify the British violation of U.S. territorial sovereignty and which still form the basis for the customary principles governing the issue of self-defence in international law.

Article 51 of the UN Charter requires that a State must be a victim of an armed attack for the use of force in self-defence to be lawful.¹⁶⁴ While interpreting the UN Charter on self-defence in several cases, the ICJ has acknowledged the relevance of the rules of customary international law and general principles of *jus ad bellum*, such as there must be a significant armed attack and a response proportionate to the injury suffered; the attack must be attributable, and use of force must be a last resort.¹⁶⁵

In the *Oil Platform's case*, the ICJ stated the need to prove that one had been a victim of an armed attack as required by international customary law and article 51.¹⁶⁶ The case between the U.S and Iran was about the lawful use of force in self-defence as provided for in article 51 of the UN Charter. In 1987 and 1988, the U.S navy launched armed attacks against Iranian oil platforms as self-defence in response to a missile strike by Iran on a tanker that was rebadged as a U.S flag-carrier and a U.S warship struck by a mine while sailing in international waters near Bahrain.¹⁶⁷ The ruling of the ICJ in the Oil Platforms case affirms the right to self-defence and the degree of scale and effect in determining what amounts to an armed attack. Also, it affirmed the right to self-defence in the marine environment by

¹⁶³ *Caroline Case of 1837; facts taken from D.J. Harris, Cases and Materials on International Law, 5th Edition, 1998.*

¹⁶⁴ 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 anyway affect the authority and responsibility of the security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*

¹⁶⁵ Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States, Merits, Judgment, (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ]; Nuclear Weapons case (1996) par 141, Case Concerning Oil Platforms (Islamic Republic of Iran v. United States) 2003 ICJ reports, 161 par 43; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, ICJ Judgment (2005) 168 par 147; *Dinstein Computer Network Attacks and Self-Defence* 109.

¹⁶⁶ The Oil Platforms Case (2003) par [61-64].

¹⁶⁷ *Ibid.*

ruling that Iran had the right to defend against threats to their offshore installations and infrastructure.¹⁶⁸

In the *Nicaragua case*, the ICJ was asked to find that the military and paramilitary activities by the US against Nicaragua between 1981 to 1984, which included the laying of the mines in the internal waters and in the territorial sea of Nicaragua, was a violation of customary international law and the principles of international law on the use of force. In this case, the ICJ held that the two factors determining international customary law are State practice and *opinio juris*.¹⁶⁹ It also provided principles guiding the scope and limitations to self-defence.¹⁷⁰ The ICJ emphasised the need to distinguish between armed attacks which as the gravest form of the use of force and other attacks that do not meet this threshold.¹⁷¹ It ruled that the most severe form of use of force is armed attack and that the violence qualifying an incident as use of force can be determined by the consequence of that act and not strictly through the type of weaponry.

In the *Nuclear Weapons case*, the ICJ, in its advisory opinion, affirmed that article 51 applies to any use of force despite the weapons used.¹⁷² In this case, the ICJ was asked to provide a legal opinion on the threat or use of nuclear weapons is allowed or prohibited under international law. It ruled that armed attack is not limited to specific weapons because the UN Charter, the “most directly relevant applicable law”, is silent on the kind of weapons that can be used to cause an armed attack.¹⁷³ It is submitted that this rationale can be applied to the maritime cyber security context by asserting that cyber weaponry can also be used to cause an armed attack. Therefore, anticipatory self-defence is an essential option in terminating an imminent cyber threat at sea, which could lead to a severe breach of the cyber security of commercial or military ships.

2.3. Domestic Laws

Cyber security does not exist in a legal vacuum. Many of the international legal instruments discussed above require incorporation into domestic laws for

¹⁶⁸ *Ibid.*

¹⁶⁹ *Nicaragua case* (1986) 14 *supra* par 195

¹⁷⁰ *Ibid.*

¹⁷¹ *Ibid.*

¹⁷² *Legality of the Threat or Use of Nuclear Weapons* [1996] ICJ Reports 226.

¹⁷³ *Nuclear weapons case supra* par 37-50

implementation to improve maritime cyber security. The relevance of looking into these domestic laws is that their codification of unlawful cyber acts affirms the opinion of States over the wrongfulness of these acts. Where these unlawful acts occur on an international level, victim-States can justifiably defend themselves against the internationally wrongful act. These States are enjoined by the relevant international legal instruments discussed above to enact laws to address maritime security threats, including MCAs. African States tend to rely on domestic laws to address all forms of cyber security issues. For instance, a high-level Global Maritime Security Conference was hosted by Nigeria in 2019, which focused on discussing maritime security threats and planning different tactics to prevent cyber security attacks.¹⁷⁴

Domestic laws of States are evolving in their commitment to tackling MCAs,¹⁷⁵ among other maritime security threats, which can be perpetrated by lone individuals who act in their private capacity and group of hackers who may act as unofficial agents of a State.¹⁷⁶ When individuals and commercial shipping companies are victims of MCAs, the State's domestic laws on cybercrime within whose jurisdiction the incident occurred can be applied to prosecute perpetrators who are not State-sponsored. States must cooperate with each other in carrying out investigations necessary to bring the perpetrators to justice. When State-sponsorship is attributed to States, it becomes an international law issue that is negotiated and mediated by State parties in many cases.¹⁷⁷ While some countries have statutes that apply specifically to cybercrime, others use a combination of legislative frameworks relevant to cybersecurity, as is the case in South Africa. These cybercrime laws are used to prosecute perpetrators of cyber-attacks whose unlawful acts are not attributable to a State.

The relevant legislative instruments to cybersecurity in the South African context include the Cybercrimes Act 19 of 2020, which is partially in effect, the Electronic

¹⁷⁴ World Oceans Council “Global Maritime Security Conference” <https://www.oceancouncil.org/event/global-maritime-security-conference/> (accessed 2020-07-18).

¹⁷⁵ *Ibid.*

¹⁷⁶ Clark “Shipping Laws and Regulations 2021” <https://iclg.com/practice-areas/shipping-laws-and-regulations/2-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels> (accessed 2020-06-04).

¹⁷⁷ Article 34 of the African Union Convention on Cyber Security, 2014.

Communications and Transactions (ECT) Act of 2002, and the Protection of Personal Information Act (POPIA) of 2013. The primary South African source of law regulating cyber security is the ECT Act, which can be used to prosecute offenders, especially cyber-related crimes not attributable to a State, on board a ship within the extraterritorial jurisdiction of South African courts. In order to bring the perpetrators of these crimes to justice, it is crucial to determine the jurisdiction of the court. Section 90 of the ECT Act provides that:

A court in the Republic trying an offence in terms of this Act has jurisdiction where—

- (a) the offence was committed in the Republic;
- (b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
- (c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or
- (d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

In the absence of specific domestic laws on MCAs, States enact relevant laws to prosecute it as a crime. This provides an avenue for determining the liability of perpetrators but not for repelling such attacks. Section 85-89 of the ECT Act provide for the definition and categorisation of cybercrime. Section 86 identifies cyber offences by providing that a person who unlawfully intentionally or unintentionally acts in a manner that renders data ineffective or causes a security breach or denial of its efficient and effective usage is guilty of an offence.¹⁷⁸

¹⁷⁸ Section 86 of the Electronic Communications and Transactions (ECT) Act 25 of 2002: “(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993), a person who intentionally accesses or intercepts any data without authority or permission to do so is guilty of an offence. (2) A person who unintentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed, or otherwise rendered ineffective, is guilty of an offence. (3) A person who unlawfully produces, sells, offers to sell, procures for use, designs adapts for use distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section. is guilty of an offence. (4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence. (5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.”

Accessing, altering, and misrepresenting critical data, which is crucial to an operating system¹⁷⁹ such as a shipboard system. Attempting to commit these listed offences is also an offence.¹⁸⁰ The above provisions reflect how the domestic law has incorporated international instruments on maritime security to address the question of jurisdiction¹⁸¹ and classification of cyber offences.¹⁸² This is because it reflects South Africa's treaty obligations concerning maritime security, which includes cyber security as required by the IMO guidelines, SOLAS, as discussed earlier in this chapter. Domestic laws on maritime security serve as a platform for addressing liabilities and claims for compensation in the event of unlawful incidents.¹⁸³ Not all States have maritime cyber security laws, but a State like Turkey introduced cyber laws to address criminal activities in its jurisdiction.¹⁸⁴

The relevance of cybersecurity to the smooth operation of Nigeria's maritime domain is rooted in the Nigerian domestic law on cybercrime¹⁸⁵ and maritime security.¹⁸⁶ Like other countries such as South Africa and Turkey, Nigeria enacted the Cybercrimes (Prohibition, Prevention, etc) Act of 2015 which provides for offences and penalties for computer-related offences such as system interference, unlawful access to a computer, unlawful interception, unauthorised modification of computer systems, network data and system interference.¹⁸⁷ In Nigeria, the Nigerian Maritime Administration and Safety Agency (NIMASA) Act of 2007 established NIMASA which is saddled with the responsibility of providing maritime security as part of its functions and duties in Nigeria. A combined reading of these domestic laws provides the legal framework for regulating maritime cybersecurity offences by non-State actors. Their provisions address issues relating to mutual assistance, jurisdiction and extradition. Nigeria's domestic laws also reflect its treaty obligations on maritime security stipulated by the IMO guidelines and SOLAS.

¹⁷⁹ Section 87 of Act 25 of 2002.

¹⁸⁰ Section 88 of Act 25 of 2002.

¹⁸¹ Section 90 of Act 25 of 2002.

¹⁸² Sections 85-89 of Act 25 of 2002.

¹⁸³ Kindt "Vessel-Source Pollution and the Law of the Sea" 1984 17 *Vanderbilt Journal of Transnational Law* 287 319-320.

¹⁸⁴ Bıçakcı, Ergun and Celikpala "The Cyber Security Scene in Turkey" in *A Primer on Cyber Security in Turkey: and the Case of Nuclear Power* (2015) 22, 24.

¹⁸⁵ Cybercrimes (Prohibition, Prevention, etc) Act of 2015.

¹⁸⁶ Section 22(1)p Nigerian Maritime Administration and Safety Agency Act of 2007.

¹⁸⁷ Sections 5, 8, 10, 12 and 16 Cybercrimes (Prohibition, Prevention, etc) Act of 2015.

It is submitted that domestic laws on maritime security have limited relevance to the subject of MCAs. Their provisions are not focused on the issue of self-defence but on identifying unlawful cyber incidents and determining liability after a suspected breach of maritime security. Their relevance to the issue of self-defence can arise when these unlawful incidents are attributable to a State if effective control of the attacker by the State can be established.

2.4. Scholarly Writings on Maritime Cyber Security

One of the sources of international law which regulates the relationship between States is “the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.”¹⁸⁸ Maritime cyber security is an aspect of international law that focuses on regulating maritime and cyber interests of States in their interrelations among themselves. The above provision is a directive to the ICJ, and it is assumed that it shows evidence of customary international law.¹⁸⁹ Justifying which writers are most qualified on this subject can be based on “highlighting the quality of work, the expertise of a writer, the official authority of a writer and agreement among multiple writers.”¹⁹⁰ In addition to the multiple justifications for referring to various scholarly works, it is submitted that the teachings of renowned scholars provide valuable legal ideas and arguments which can be applied in determining the legal issues arising from maritime cyber security.

The concept of maritime security has been defined from negative and positive perspectives.¹⁹¹ From the negative perspective, it has been described concerning the threats and challenges facing the maritime domain. This description focuses on the absence of adequate security at sea. It emphasises different types of security breaches, including piracy¹⁹², collision, explosions, terrorism, and data breach. The occurrence of any of these security breaches can be referred to as a threat to maritime security.

¹⁸⁸ Article 38(1) of the Statute of the ICJ.

¹⁸⁹ Danilenko *Law-Making in the International Community* (1993) 33–36.

¹⁹⁰ Helmersen “Finding ‘the Most Highly Qualified Publicists’: Lessons from the International Court of Justice” 2019 30(2) *European Journal of International Law* 509–535 513.

¹⁹¹ Bueger “What is Maritime Security?” 2015 53 *Marine Policy* 159 159.

¹⁹² Article 101 of UNCLOS.

Maritime security comprises of the regulation of peaceful activities at sea.¹⁹³ This means that the safety of life and ship at sea is evidence of maritime security. This is reflected in the IMO's guidelines that direct stakeholders to comply with specific standards for maritime security. It can also be implied that non-interference with critical infrastructures of vessels and marine installations, including the reliant Internet facilities, is a feature of maritime security. The absence of any form of attack at sea is maritime security.

Bueger argues that maritime security can be viewed from three perspectives:

The frameworks that are particularly useful are (1) 'semiotics' which intends to map different meanings by exploring the relations between maritime security and other concepts, (2) the 'securitisation' framework which provides the means to understand how different threats are included in maritime security, and (3) 'security practice theory' which aims at understanding what actions are undertaken in the name of maritime security.¹⁹⁴

These second and third contexts are critical to this study. This is because the 'securitisation' framework of maritime security, as described above, includes maritime cyber security threats. The normative understanding about forms of threats to maritime security needs to be expanded to recognise cyber-attack as a serious threat.¹⁹⁵ In the context of this thesis, breach of maritime security includes imminent cyber-attacks and actual cyber-attacks, which will be generally referred to as "cyber-attacks". Cyber-attacks are becoming more conspicuous among other forms of breaches of maritime security. Understanding the uniqueness of this form of threat to maritime security cannot be overemphasised. In order to address this security threat, States will require guidance in undertaking legitimate security practices that are compliant with international law requirements on this subject.

Applying Bueger's 'securitisation framework' enables the identification of actions that will amount to a breach of maritime security. States are guided by looking at legal instruments that identify these unlawful acts. This gives them the legal authority to formulate laws and policies to ensure that their maritime security is effective. For

¹⁹³ Kraska and Pedrozo *International Maritime Security Law* (2013) 1.

¹⁹⁴ Bueger 2015 *Marine Policy* 160.

¹⁹⁵ Klein *Maritime Security and the Law of the Sea* (2011) 319-320.

example, the South African 2002 ECT Act used to prosecute cyber-related crimes includes those that occur within its maritime jurisdiction.¹⁹⁶

Also, Bueger's 'security practice theory' aims at identifying legitimate options available to States in defending themselves against maritime cyber security threats, including cyber-attacks. The security practice theory creates a framework for assessing the security risks against ships, ports, or marine installations of a State and the applicable maritime security guidelines. Maritime security can be viewed from different and sometimes overlapping perspectives. Rahman argues that States' policies and operations intended to address maritime security requires focusing on:

Security of the sea itself, Ocean governance, Maritime border protection, Military activities at sea, Security regulation of the maritime transportation system.¹⁹⁷

In this modern area, all the above listed focal areas rely on information technology partially or totally for smooth operation. This Internet reliance is increasing, and more innovative ways are evolving to cater to the above-listed aspects in the maritime domain. For instance, ocean governance, which incorporates guidelines and actions in regulating marine affairs through legal and institutional frameworks, is adapted to the marine environment's technological advancement to ensure security at sea successfully. The State-controlled agency with the mandate to ensure maritime border protection will secure its marine domain by taking all forms of threats at sea into cognisance. This includes those that threaten the critical operating systems of an Internet-reliant ship, port or marine installations. States carry out military activities at sea, including planting sea mines, taking off fighter jets and launching missiles from ships. Securing these military operations, including those relying on information technology, falls within the ambit of maintaining maritime security.¹⁹⁸

Maritime security became an issue for debate when the U.S published the foremost national strategy for maritime security in 2005 (2005 NSMS), where it defined the Maritime domain as:

¹⁹⁶ Section 90(d) ECT Act 25 of 2002.

¹⁹⁷ Rahman *Concepts of Maritime Security: A Strategic Perspective on Alternative Visions for Good Order and Security at Sea, with Policy Implications for New Zealand* (2009) 31.

¹⁹⁸ Nielsen "The Role of the U.S. Military in Cyberspace" 2016 15(2) *Journal of Information Warfare* 27 35.

all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.¹⁹⁹

This includes maritime-related activities on ships, oil rigs and at the ports. The infrastructure, cargo and vessels need to be protected and defended from any form of attack. The security of the maritime domain is essential for the smooth running of maritime transportation, trade, and sustainable use of the marine environment. According to the United States' 2005 NSMS, terrorism is the main threat to maritime security because it is characterised by asymmetric forms of threats which includes the proliferation of weapons of mass destruction and the use of cyber weaponry to achieve a destructive consequence at ports, aboard a ship or on an oil rig.²⁰⁰ The main objective of maritime security is to protect lives, property, the marine environment and the economy from being threatened by a security breach at sea.²⁰¹ Therefore, it is agreeable that maritime security refers to measures taken to protect, prevent and respond to all types of attacks on ships, terminals, ports, oil rigs and all equipment supporting maritime operations.²⁰²

Hawkes' definition of maritime security as:

those measures employed by owners, operators, and administrators of vessels, port facilities, offshore installations, and other marine organisations or establishments to protect against seizure, sabotage, piracy, pilferage, annoyance, or surprise²⁰³

portrays the allowance States have to establish respective measures or legal framework for attaining maritime security. Also, this definition reflects some of the seven threats to maritime security as identified by the UN Secretary-General in 2008.²⁰⁴ The security threats listed in the report are piracy and armed robbery against ships; maritime terrorist acts; illicit trafficking in arms and weapons of mass

¹⁹⁹ Department of Homeland Security "National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security" (October 2005) https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf ; also available at <https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html> (accessed on 2019-06-26).

²⁰⁰ *Ibid.*

²⁰¹ Randrianantenaina *Maritime Piracy and Armed Robbery against Ships: Exploring the Legal and the Operational Solutions. The Case Of Madagascar* (2013) https://www.un.org/depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/Randrianantenaina_1213_Madagascar.pdf (accessed 2019-06-26) 18-19.

²⁰² International Maritime Organisation.

²⁰³ Hawkes *Maritime Security* (1989) 3

²⁰⁴ UNGA "Oceans and the Law of the Sea: Report of the Secretary General" (10 March 2008) UN Doc A/63/63, par [39].

destruction; illicit traffic in narcotic drugs and psychotropic substances; smuggling and trafficking of persons by sea; illegal, unreported and unregulated fishing; intentional and unlawful damage to the marine environment. The threats to or actual attacks on maritime security may be executed through various means. Likewise, different types of weapons may be employed to defend against these attacks. As aptly stated,

The diverse maritime security threats also result in the adoption of different measures in response to these threats. The capacity of each regional actor also dictates what is considered needed to enhance maritime security.²⁰⁵

These security threats can be tangible, as in physical, or intangible, as in virtual attacks when broadly viewed. For instance, the physical attacks can be piracy or military attacks, while the perceptual attacks may be cyber in nature. Irrespective of the form of attack, the scale and effect may be manifested in different dimensions. While the destructive effect of a bomb blast is readily visible, an attack in cyberspace can lead to consequences that may sometimes be similar to that of a physical attack or manifested in an intangible form. It has been debated whether the physical form of the consequence of an attack should determine its gravity. This will be discussed in the following chapters.

Furthermore, maritime security has been viewed from a legal perspective. Kraska and Pedrozo argued that it “includes legal authorities to counter traditional and conventional threats, as well as irregular or asymmetric dangers, against the territorial integrity or political independence of flag, port, coastal and landlocked States.”²⁰⁶ This description focuses on the institutional framework for securing the maritime domain. This implied that a security agency charged with securing lives and property at sea is maritime security. The ‘traditional and conventional threats’ which security agencies counter at sea do not include maritime cyber threats. This is because the critical infrastructure of ships now uses less ‘traditional and conventional’ Internet-reliant operating systems. The unique feature of maritime cyber threats and attacks makes it unparalleled to the orthodox types of threats and attacks that the existing laws recognise.

²⁰⁵ Galani and Evans (eds.) ‘The Interplay between Maritime Security and the 1982 United Nations Convention on the Law of the Sea: Help or Hindrance?’ in *Maritime Security and the Law of the Sea* (2020) 8.

²⁰⁶ Kraska and Pedrozo *International Maritime Security Law* (2013) 5.

Also, it has been asserted that the scope of maritime security measures for many countries, including the U.S, covers:

International and national peace and security; sovereignty, territorial integrity and political independence; security of sea lines of communications; security protection from crimes at sea; resource security, access to resources at sea and to the seabed; environmental protection; security of all seafarers and fishermen.²⁰⁷

It can be inferred that maritime security issues affect economic development, the marine environment, national and human security. The significance of these issues is manifested in UNCLOS and IMO's guidelines which have a common objective of promoting maritime security. This objective to ensure maritime security includes achieving cyber security in the marine environment. The potential attacks that threaten the maritime domain can be carried out in different ways ranging from the use of tangible force (such as mines, guns, or other explosives) to intangible cyber weaponry, which equally poses a threat to maritime operations and safety. Although maritime stakeholders have published and are still developing maritime security strategies, there is no clear path concerning the legal paradigm on defending against maritime cyber armed attacks.²⁰⁸ Among all types of illegal maritime attacks, those that occur through cyberspace pose a unique threat.

Notably, nineteen international experts²⁰⁹ drafted a manual on the international law applicable to cyber warfare; it was later updated and is now referred to as the '2017 edition of the Tallinn Manual 2.0'. This manual has been referred to as the most comprehensive analysis of the current application of international law to cyber

²⁰⁷ Feldt, Roell and Thiele "Maritime Security – Perspectives for a Comprehensive Approach" 2013 222 *ISPSW Strategy Series: Focus on Defence and International Security* 1 2-3.

²⁰⁸ The United States of America has published a National Maritime Security Strategy which is available at <http://www.navy.mil/maritime/Maritimestrategy.pdf> (accessed 2019-06-26) ; NATO and the member states of the Alliance also have maritime security strategies which are viewed at http://www.nato.int/docu/review/2010/maritime_security/end_of_naval_era/en/index.htm (accessed 2019-06-26) ; The EU Maritime Security Strategy available at http://ec.europa.eu/maritimeaffairs/policy/index_en.htm (accessed 2019-06-26); The African Union's 2050 Maritime Strategy available at <http://www.au.int/pages/maritime/news/1st-conference-african-ministers-responsible-maritime-related-affairs-back-back-4th-af> (accessed 2019-06-26).

²⁰⁹ Prof. Michael Schmitt, Air Commodore (Retired) William H. Boothby, Bruno Demeyere, Prof. Wolff Heintschel von Heinegg, Prof. James Bret Michael, Prof. Thomas Wingfield, Prof. Eric Talbot Jensen, Prof Sean Watts, Dr. Louise Arimatsu, Capt. (Navy) Genevieve Bernatchez, Col. Penny Cumming, Prof. Robin Geib, Prof. Terry D. Gill, Prof. Derek Jinks, Prof. JannKleffner, Dr. Nils Melzer, Brigadier Gen. (retired, Canadian Forces) Kenneth Watkin, Dr. Kenneth Geers, Dr. Rain Ottis.

operations.²¹⁰ It defines the use of force²¹¹ which is relevant in determining the status of MCA as a form of force. Its definition of 'threat of force' is relevant to assessing the legality of anticipatory self-defence against MCA. It states that:

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.²¹²

This assertion suggests that for States to defend themselves anticipatorily against MCA, the imminent attack should be such that it could meet the threshold of armed attack if it is not repelled.²¹³ Therefore, in accordance with customary international law, the principles of 'necessity and proportionality' as well as 'imminence and immediacy' must be considered when States act to protect their maritime cyberspace²¹⁴

The Bush Doctrine is fundamental to understanding the position of U.S on the subject of self-defence. According to this doctrine, the United States could invoke preemptive self-defence before a threat matures even though there is no certainty as to whether the threat would occur.²¹⁵ This appears to be a liberal approach for interpreting the concept of self-defence against a breach of cyber security. This approach has evolved into establishing a cyber-command with its objectives, including denying cyber freedom of action in cyberspace to US adversaries.²¹⁶ The US has affirmed that in line with its inherent right to self-defence, all forms of hostile acts including cyber-attacks will be responded to.²¹⁷

From this statement, it could be inferred that the US considers cyber-attack as a use of force that violates article 2(4) of the UN Charter, necessitating an action in self-defence. It can be interpreted as a specific mandate which permits anticipatory self-defence against cyber-attack without clearly stating the means of enforcement. The

²¹⁰ *Ibid.*

²¹¹ Schmitt (ed) *Tallinn Manual 2.0* 330.

²¹² Schmitt (ed) *Tallinn Manual 2.0* 338.

²¹³ Schmitt (ed) *Tallinn Manual 2.0* 339.

²¹⁴ Schmitt (ed) *Tallinn Manual 2.0* 348-350.

²¹⁵ Shah "The Bush Doctrine of Pre-emptive Strikes; A Global Pax Americana" *Global Issues* (24 April 2004 (available at <http://www.globalissues.org/article/450/the-bush-doctrine-of-pre-emptive-strikes-a-global-pax-americana> (accessed 2018-09-12))).

²¹⁶ US Department of Defence, Cyber Command Fact Sheet (25 May 2010) (available at www.defence.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf).

²¹⁷ *Ibid.*

U.S is setting the pace for an interpretation of the relevant principles of international law that suits the cyber security policy of individual States. Since establishing a rule of customary international law requires an extensive, uniform, and representative State practice,²¹⁸ it is pertinent to assess whether more countries share the same perspective with the United States on this subject. This will be discussed in the following chapters.

It has been argued that self-defence is a natural law. Since an international instrument expressly provides for it,²¹⁹ it should not be viewed as a limitation but an emphasis of its legitimacy, especially if the threat is looming or genuine.²²⁰ Therefore, in determining the legality of anticipatory defence against MCA, it is debatable that the focus should be on the probable consequences or potential damage instead of the wrongful violation of the victim's cyberspace. Should the right to self-defence arise at the instance of an imminent electronically delivered threat or upon assessment of potential or actual loss of lives and damage to property?

Anticipatory self-defence can be understood by using the 'imminence' principle of *jus ad bellum*,²²¹ which provides for the norms and processes involved in determining the justification for a State's use of force against a perceived threat.²²² Although customary international law permits the use of force in self-defence in situations described as 'overwhelming circumstances with no time to deliberate', applying this to the maritime context raises legal issues due to the unique nature of the technology involved in executing a maritime cyber-attack.²²³

It has been argued that international cyber-attack should be seen as a criminal threat that can justify self-defence due to the absence of explicit international law

²¹⁸ ICRC "Customary International Law" available at <https://perma.cc/P8V5-VVYD> accessed 2018-05-21).

²¹⁹ Article 51 of the UN Charter.

²²⁰ Kelsen *The Law of the United Nations* (1950) 792.

²²¹ The main principles of *jus ad bellum* are right authority, right intention, reasonable hope, proportionality, and last resort

²²² Graham "Cyber Threats and the Law of War" 2010 4 *Journal of National Security Law and Policy* 87 88; Walzer *Just and Unjust Wars: A Moral Argument with Historical Illustrations* 2ed (1997 44, 4ed (2006) 85.

²²³ Brunstetter and Braun "From Jus ad Bellum to Jus ad Vim: Recalibrating Our Understanding of the Moral Use of Force" 2013 27(1) *Ethics and International Affairs* 87 88: "we articulate the limitations of jus ad bellum principles in evaluating recent trends in international affairs—such as the rise of non-state actors and the advancements in precision weapons technology (for example, drones)—that have weakened the sovereignty norm and facilitated small-scale uses of force to combat perceived threats."

provisions, especially on using force by terrorists and non-State actors.²²⁴ In practice, this would require an aftermath assessment of the cyber-attack that will not allow the opportunity to repel an imminent attack that potentially meets the threshold of armed attack. When the unique nature of MCA is taken into consideration, an objective interpretation of the relevant international law provisions can provide an argument for legalising anticipatory self-defence against MCA so that maritime cyber security is improved.

There are three instances of cyber-attacks that are relevant for assessing State practices on the subject.²²⁵ First is the Estonia and NATO incident of 2007, where Estonian officials saw Denial of Service attacks directed at government websites as cyberwar. They likened it to a possible conventional shutdown of Estonia's ports. Secondly, the Georgia and Russia situation of 2008 was the first confirmed use of cyber-attack during a conventional armed conflict. The third is the *Stuxnet* incident where computers at Iran's nuclear program were infected.²²⁶ An additional incident is the Israel Defence Force's (IDF) physical use of deadly force against Hamas' cyber headquarters by bombing their cyber facility in reaction to a cyber-attack launched by Hamas. The IDF's action has been a subject of debate pertaining to whether it was legitimate, proportional, or necessary.

Interestingly, all these incidents have a common feature of States' inability to strictly comply with the prerequisite for invoking self-defence as set out by the rule of customary international law.²²⁷ While the victim states often claim their act of self-defence was necessary and justified, the aggressor states tend to complain that the response was not proportionate and excessively unnecessary. Attribution has been noted as a critical element in invoking self-defence. Its requirement for clear and convincing evidence is a challenging standard of evidence to prove due to the unique and dynamic features of cyber security. Currently, there are instances of States denying responsibility for an obvious cyber-attack carried out by their organs or citizens.²²⁸ Also, due to the lack of cyber intelligence precision in developing

²²⁴ *Ibid*; Ozubide "How the Use of Force Against Non-state Actors Transformed The Law of Self-defence After 9/11" 2016 41 *SA Yearbook of International Law* 1-29.

²²⁵ O'Connell 2012 *Cyber Security and International Law: Meeting Summary* 4.

²²⁶ *Ibid*.

²²⁷ O'Connell 2012 *Cyber Security and International Law: Meeting Summary* 6.

²²⁸ Siman-Tov and Even *A New Level in the Cyber War between Israel and Iran*. Report. Institute for National Security Studies, 2020, www.jstor.org/stable/resrep25542 (accessed 2020-10-23) .

countries, there can be instances of States taking some preemptive steps based on wrong assumptions or security intelligence reports.

Despite the possibility of triggering a military response to the *Stuxnet* attack, Iran would have failed to meet most of the above-listed prerequisites for determining whether MCA fall under *jus ad bellum* or necessitate the right to self-defence.²²⁹ By failing to meet these conditions, the objective to ensure cyber security by allowing States to exercise their right to self-defence is hindered. This implies that States cannot protect themselves until the consequent damage from a cyber-attack is assessed. Interpreting article 51 with these strict preconditions endangers the cyber security of a State. It contradicts the objective of the UN Charter to prevent war and maintain international peace and security.²³⁰ The position of the ICJ on the legality of cyber weapons is not clear and State practice on addressing cyber-attack is not consistent.²³¹ Therefore, formulating international customary law on this issue might seem impossible.

The rules of international customary law need to be updated to reflect prevalent State practices influenced by the politics of international law. Some of these State practices are inappropriate and should not be supported by the law even if the world powers perpetrate them. The existing provisions in international law seem to have been designed to address the global security challenges in the 20th century but not the modern security threats,²³² including those posed by MCA. Therefore, a new set of customary international law rules and general principles need to be formed to address the unique nature of MCA in a technologically advanced era.

The main aim of anticipatory self-defence in State practice is to repel an imminent attack.²³³ This goal should be met irrespective of the type of attack to prevent an imminent threat from resulting in avoidable deaths, injury, and destruction of property. As earlier stated, this assertion is predicated upon the provision of article 51 of the UN Charter. In interpreting this provision, some scholars have provided various views. One view supported the need for preemption based on the nature of

²²⁹ *Ibid.*

²³⁰ Preamble and article 1 of the UN Charter .

²³¹ Shackelford "The Law of Cyber Peace" 2017 18(1) *Chicago Journal of International Law* 1 28.

²³² Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue and Spielgel "*The Law of Cyber-Attack*" 2012 100 *California Law Review* 817 877.

²³³ Gray *International Law and the Use of Force* (2018) 174 .

the threat,²³⁴ while others have dismissed the idea.²³⁵ Another writer suggested that applying the above provision as automated self-defence could be very reckless or seem challenging to implement lawfully.²³⁶ Also, it has been argued that preemptive self-defence is different from anticipatory self-defence because the latter is the right to use force against budding threats instead of the former, which uses force to repel a fully blown imminent threat.²³⁷ This extends article 51 to allow unilateral preventive action based on individual States' varied perceptions of potential threats.²³⁸ This volatile approach could jeopardise the objective of ensuring international peace and security.²³⁹

However, there are particular challenges associated with addressing the issue of anticipatory self-defence. Firstly, there is the lack of ubiquitous application or interpretation of existing laws and procedures on the use of force, self-defence and domestic criminal law.²⁴⁰ Scholars have written extensively on these subjects.²⁴¹ The ICJ has provided interpretations that have been subject to further analysis with no universal agreement of the specific rules guiding the use of force and self-defence. Attempting to apply existing laws such as UNCLOS III and the UN Charter on the use of force, and specifically, on anticipatory self-defence, has generated conflicting scholarly arguments.²⁴²

One of the main issues concerns the process of determining whether a threat is imminent or genuine. It has been argued that it is practically difficult to distinguish between merely preparatory actions and those within the initial phase of an armed attack in the maritime cyber context.²⁴³ For instance, malicious software could be introduced into a ship's operating system, which could be triggered at any time by

²³⁴ Reisman and Armstrong "The Past and Future of the Claim of Preemptive Self-defence" 2006 100(3) *American Journal of International Law* 525 526.

²³⁵ O'Connell 2012 *Cyber Security and International Law: Meeting Summary* 5.

²³⁶ Dinstein *Computer Network Attacks and Self-Defence* 106.

²³⁷ Reisman and Armstrong 2006 *American Journal of International Law* 526.

²³⁸ United Nations Secretary General "2004 High Level Panel Report on Threats, Challenges and Change, A more Secure World: Our Shared Responsibility" (available at www.un.org/ruleoflaw/blog/document/ (accessed 2018-03-25)).

²³⁹ *Ibid.*

²⁴⁰ Sklerov 2009 *Military Law Review* 1 6.

²⁴¹ Gray *International Law and the Use of Force* (2018) 170-174; Reisman and Armstrong 2006 *American Journal of International Law* 526; Dinstein *Computer Network Attacks and Self-Defence* 106; Sklerov *supra*; Stahl 2011 *Georgia Journal of International and Comparative Law* 251; O'Connell 2012 *Cyber Security and International Law: Meeting Summary* 6.

²⁴² *Ibid.*

²⁴³ *Ibid.*

the hacker to enable him or her to control the ship's navigation. Also, anticipatory self-defence has been seen as 'interceptive self-defence' because it can only be legally invoked before a launched attack reaches its target.²⁴⁴ In addition to these divergent views, State practices on this subject tend to be influenced by their relative interpretations, mostly tailored to suit their immediate circumstances.²⁴⁵

Secondly, the non-existence of a treaty that creates the legal obligation for States to assist each other in investigating MCA originating from their jurisdiction is problematic.²⁴⁶ It has been suggested that existing international legal instruments and principles such as the UNCLOS III, the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) and its 2005 Protocol, and the Convention establishing the International Maritime Organization could guide the development of a comprehensive legal framework.²⁴⁷ Attempting to apply these instruments may be challenging because MCA is not limited to State actors and is not clearly defined. It could be a type of piracy at sea as defined by UNCLOS III.²⁴⁸ An attack could be carried out by the citizen of a country who resides in another country against a third country with or without government sponsorship.²⁴⁹ This raises several issues, including investigation, attribution, and targeting attackers in the State from where the attack originated.²⁵⁰ Notwithstanding its contribution to threatening maritime security, the swiftness and complexity of MCA require unique sets of laws, regulations and established procedures.

Thirdly, the parochial nature of existing international cyber security laws or agreements²⁵¹ has led to a failure to provide for anticipatory self-defence against MCA inadequately. The various States create subjective interpretations of these laws by drafting them to suit their national interest, leading to unclear and non-universal laws for responding to an imminent threat to maritime cyber security.²⁵² States are guided by the principles of territorial jurisdiction and the inherent right of self-defence

²⁴⁴ Dinstein *War, Aggression and Self-Defence* (2011) 203-205.

²⁴⁵ Reisman and Armstrong 2006 *American Journal of International Law* 549.

²⁴⁶ Sklerov 2009 *Military Law Review* 1 9.

²⁴⁷ Stahl 2011 *Georgia Journal of International and Comparative Law* 251.

²⁴⁸ Article 101 of UNCLOS III which defines piracy as a variety of transnational crime conducted by non-state actors in international waters.

²⁴⁹ Dinstein *Computer Network Attacks and Self-Defence* 103.

²⁵⁰ Dinstein *Computer Network Attacks and Self-Defence* 108.

²⁵¹ Sklerov 2009 *Military Law Review* 1 5.

²⁵² Kanuck "Sovereign Discourse on Cyber Conflict Under International Law" 2010 *88 Texas Law Review* 1571 1581.

in determining their response to an attack.²⁵³ However, it has been suggested that the focus should be on the gravity of the result of the MCA and not only the physical damage as portrayed by the scale and effect principle decided by the ICJ in the *Nicaragua's* case.²⁵⁴ This could accommodate some severe damages that are not physical but risk falling below the threshold of armed attack due to their form.²⁵⁵ The application of this 'scale and effects' principle,²⁵⁶ especially in the context of MCA, has not been universally accepted.²⁵⁷

This has contributed to the challenges affecting the lawful application of anticipatory self-defence against MCA. The ICJ distinguished the uses of force that can be classified as armed attack and that which do not meet that threshold by applying the scale and effect criteria.²⁵⁸ Applying these criteria to the maritime context means that where a use of force, in the form of an MCA, leads to the death of human beings or destruction or damages to property, it would constitute an armed attack in scale and effect.²⁵⁹ When a cyber-attack occurs, the type of property destroyed or damaged could be intellectual property or data breach, which grossly affects the operating systems for controlling a ship. This can only be determined after the imminent attack has occurred. Therefore, the scale and effect criteria may only apply to anticipatory self-defence against MCA to perceive the necessity or imminence of the threat.

Developing an international legal framework for specifically addressing maritime cyber security can be derived from the duties and responsibilities UNCLOS imposes to combat piracy.²⁶⁰ This might be difficult because the relevant provisions of articles 17, 21, 25, 94 and 113 of UNCLOS and its definition of piracy appear to be narrow due to non-consideration of the evolving contemporary threat posed by MCA. It is safe to assume that the rationale behind the UNCLOS and its objectives were not designed to address the issue of anticipatory self-defence against MCA. Also, expressly determining the attacker's intent as a condition for categorising a MCA might be difficult but could be implied. Cyber activities such as introducing malware,

²⁵³ *Ibid.*

²⁵⁴ Schmitt (ed) *Tallinn Manual 2.0* 292.

²⁵⁵ *Ibid.*

²⁵⁶ *Nicaragua case* (1986) 14 *supra* par 195.

²⁵⁷ Kretzmer 2013 *European Journal of International Law* 243.

²⁵⁸ *Nicaragua case* (1986) 14 *supra*

²⁵⁹ Schmitt (ed) *Tallinn Manual 2.0* 341.

²⁶⁰ Stahl 2011 *Georgia Journal of International and Comparative Law* 251.

denial of service, and other dangerous cyber activities within the victim's operating system are hostile acts.

All these scholarly arguments on the incidental issues concerning maritime cyber security can provide analytical guidance to States exercising their right to self-defence. These discussions by scholars and groups of experts are significant in paving the way towards forming consensus among States on the formulation of a treaty. This is evident in the reports of the UN Group of Governmental Experts (GGE)²⁶¹ that deal with cyber issues in the context of international security. This 2015 GGE report affirmed that article 51 of the UN Charter applies to cyberspace and recognises the applicability of the customary international law principles of necessity and proportionality.²⁶² This shows that a consensus is gradually evolving on the issue of the legitimate use of force to uphold maritime cyber security.

2.5. Conclusion

From the preceding, maritime security can be understood from different perspectives. Threat to maritime cyber security is not universally acknowledged as a forceful form of threat to maritime security. However, it is a modern type of threat that can gravely affect maritime activities. Understanding these perspectives of maritime security will inform a more precise assessment of legal implications or policy formulation towards enhancing security at sea in the face of emerging threats.

Aggressors who threaten maritime cyber security can be States or non-State actors. They can cause harm or damage to maritime personnel and infrastructures, respectively.²⁶³ The non-State actors may be sponsored by States or act independently. Likewise, victims of a breach of maritime cyber security can be a State or private commercial vessels or individuals. Although maritime threats are generally categorised as crimes, terrorism and piracy, cyber threat is the contemporary threat affecting global industries, including the shipping industry.

In subsequent chapters, it will be argued that to have effective maritime cyber security policies, State practices need to be synchronised on issues of technical

²⁶¹ The GGE was established by the UN Secretary General with a mandate from the UN General Assembly to study, in addition to its other objectives, how international law applies to States' cyber activities, with a view to forming a consensus on the issue.

²⁶² Egan 2017 35 *Berkeley Journal of International Law* 169 171.

²⁶³ *Ibid.*

standards and legal norms concerning jurisdiction, State responsibility, self-defence and use of force.²⁶⁴ This desirable agreement on MCA issues can pave the way for a universally acceptable multilateral treaty. Existing legal instruments and scholarly opinions have suggested that portraying cyber-attack as armed attack requires aftermath analyses of the type of cyber weapons and debilitating consequences as the determining factors.²⁶⁵ This creates a challenging situation for justifying anticipatory self-defence measures. Against this backdrop, the issue of maritime cyber-attack as use of force and armed attack will be discussed in the following chapters consecutively.

The above discussion of the relevant provisions of the United Nations Charter and other international conventions on cybercrime such as the Convention on Law of the Sea, Budapest Convention on Cyber Crime, European Union General Data Protection Regulation, and the African Union Convention on Cyber Security and Personal Data Protection need to be collectively considered in applying principles of international law to cyberspace. The interpretation of these legal instruments should be guided by the existence of the established right of States to self-defence and the uniqueness of cyberspace.

These legal instruments can be amended to include specific guidance to States in exercising the right to self-defence against MCAs. For instance, in accordance with article 37 of the AU Convention on Cyber Security and Personal Data Protection, States can propose an amendment that will provide for specific implementation guidelines for member States instead of the broad guiding principles and mandates. Also, it is necessary to understand the relationship between a cyber-attack and an armed attack, the foreseeability of a cyber-attack, and the attribution of a cyber-attack to a State. This will enhance the approach adopted by States with regard to anticipatory self-defence against MCA. Regional agreements on these issues can create a solid foundation for future treaties that are more specific on the use of force in the maritime cyberspace. To advance the frontier of the existing legal framework which regulate maritime cyber security, it is essential to understand MCA within the context of relevant international laws.

²⁶⁴ Gable 2010 *Vanderbilt Journal of Transnational Law* 89.

²⁶⁵ Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 54 *Harvard International Law Journal* 18 18-24.

CHAPTER 3: MARITIME CYBER-ATTACK AS USE OF FORCE

3.1. Introduction

The concept of maritime cyber-attack (MCA) within international law has been introduced in the preceding chapters as a critical aspect of maritime security. Its scope, as well as the relevant legal instruments to understanding it, have been identified. The challenges associated with applying these laws to maritime cyber security were acknowledged. It was also established in the preceding chapter that international law could be applied to maritime cyber security, especially when the perpetrator of the MCA is a State and the victim is another State. The focus of this thesis is on anticipatory self-defence against an MCA. However, it is essential to discuss article 2(4) of the UN Charter, which generally prohibits the use of force, before discussing the exception to this prohibition as stated in article 51 of the UN Charter. In addition to being a treaty-based rule, the meaning of the use of force has been a subject of debate as reflected in State practices over its interpretation and the preconditions for using force in self-defence as provided by article 51 of the UN Charter.²⁶⁶ The main goal of this chapter is to argue that MCAs can constitute uses of force for the purpose of article 2(4) of the UN Charter. The relevance of this argument lies in the fact that the gravity threshold, which is used to qualify an armed attack, as provided for by article 51 of the UN Charter, may also be used to determine whether an act amounts to a use of force. Before diving into the crux of the discussion, it is necessary to highlight the existence of violent acts at sea, provide a brief historical background of the concept of the use of force and clarify some of the terminologies used to enable the use of 'MCAs' appropriately for analysing it as a form of use of force.

One of the main legal issues that arise from this interdisciplinary subject which covers the fields of cyberlaw, maritime law and international law, is the perception of State-attributed MCA as a use of force.²⁶⁷ The attacking State can carry out this use of force against another State and the victim-State can also use force as one of its

²⁶⁶ Corten *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (2010) 5.

²⁶⁷ The use of the word 'State-attributed' is intentional. It captures the reality of State practice of circumventing the prohibition of the use of force, as provided by article 2(4) of the UN Charter, by employing the services of other groups or mercenaries to carry out their agenda against another State. This raises the question of attribution which can be direct or indirect. If the mercenaries can be linked to the State, attribution can be established.

options in self-defence against the attacker. Some of the terminologies used to describe force in cyberspace related to national security, such as computer network attacks (CNA), have become more available for public knowledge. They have become subject matters that can be discussed extensively without fear of breaching any code of secrecy on classified information because they are now popularly known.²⁶⁸

Maritime cyber operation (MCO), maritime cyber intrusion/interference (MCI) and maritime cyber-attack (MCA) are commonly used to describe or define maritime cyber security incidents. Their interpretations have legal consequences mainly when analysed within the context of international law.²⁶⁹ Although they are frequently used interchangeably, they can have different meanings with different legal implications.²⁷⁰ Their legal implications are relevant in determining when the breach of maritime cyber security amounts to the use of force, rises to the level of a cyber ‘armed attack’ or triggers actions in self-defence.²⁷¹ Determining these core issues can create the basis for understanding the legality of anticipatory self-defence against an attack targeting maritime cyber security. It provides clarity as to the legal options available to a State whose cyberspace is attacked, by a non-State actor or another State, with the possibility of causing loss of lives and destruction to property. Likewise, the victim State may be guided to correctly interpret whether a security threat amounts to unlawful use of force or/an armed attack depending on how it is interpreted.²⁷²

Also, understanding the potential ambiguities, similarities and contradictions in the definitions are relevant in drafting applicable policies and implementing strategic decisions to address maritime cyber security issues. Some definitions and descriptions may be given based on a State’s interest or reflect some experts’ opinions. For instance, the NATO cooperative cyber defence centre of excellence (CCDCOE) has provided a list of definitions of cyber terminologies drawn from the Tallinn Manual and policy documents.²⁷³ Likewise, the International Court of Justice

²⁶⁸ Armistead *Information Operations: Warfare and the Hard Reality of Soft Power* (2004) 74.

²⁶⁹ Roberts “A New Frontier: Defining Cyber-Attack and the Ramifications for Jus ad Bellum and Jus in Bello Law” 2017 12 SSRN (available at <https://ssrn.com/abstract=3009377> (accessed 2018-12-10)).

²⁷⁰ www.ccdcoe.org (accessed 2018-11-29).

²⁷¹ Roberts 2017 12 *supra*

²⁷² *Ibid.*

²⁷³ www.ccdcoe.org (accessed 2018-11-29).

(ICJ) has proffered legal reasoning on the issues of use of force, armed attack and self-defence, which may serve as guidelines for understanding the legal paradigm of maritime cyber-attack.

MCA is a unique form of cyber interference due to the maritime location of its occurrence, especially with regards to the origin of the attack and the result of the act. It may originate from the sea, and the effect is felt on the land. It may originate from the land, and the effect is felt at sea. Also, there is no universally accepted international legal instrument specifically designed to regulate self-defence measures available to states against maritime cyber interference. States rely on applying analogies from the legal reasoning of existing legal instruments as guidance to act lawfully in the uncharted territory of maritime cyber security. Notably, the legal reasoning and rules of engagement for acting in self-defence can be deduced from the existing international laws and the rulings of the International Court of Justice on the use of force, armed attack, and self-defence. This introductory section seeks to introduce the forceful tendency of maritime attacks and the historical background on the concept of the use of force. This is intended to lay a foundation for further analysis in the latter part of this chapter to determine whether or in what circumstances MCAs can qualify as use of force.

3.1.1. Violent Acts in the Maritime Sector

The main classifications of maritime attacks include piracy²⁷⁴, maritime terrorism,²⁷⁵ armed robbery²⁷⁶, trafficking and other forms of attack. Piracy involves the hijacking

²⁷⁴ Article 101 of UNCLOS defines piracy as any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft; any act of inciting or of intentionally facilitating an act described before.

²⁷⁵ Council for Security Cooperation in the Asia Pacific (CSCAP) defines maritime terrorism as “the undertaking of terrorist acts and activities within the maritime environment , using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements including tourist resorts, port areas and port towns or cities” www.maritimeterrorism.com/definitions/ accessed on 20 June, 2019.

²⁷⁶ Resolution A.1025 ‘The International Maritime Organization (IMO) “Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships” 2010 26th Assembly session defined armed robbery against ships as: “...any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against a person or property on board such a ship, within a State’s internal waters, archipelagic waters and territorial sea; any act of inciting or of intentionally facilitating an act described above”.

of vessels, hostage-taking of sea travellers, and criminal incidents of robbery. According to Feldt, Roell and Thiele,

the threat caused by Somali piracy off the coast of Somalia and in the Indian Ocean is and will remain of significance for international shipping in the foreseeable future, and will continue to cause high economic costs.²⁷⁷

The main perpetrators of maritime terrorism are Al-Qaeda, the Abdullah Azzam Brigades and sometimes Al-Shabaab.²⁷⁸ These terrorists carry out attacks with political, religious, or ideological motives. Their maritime attacks can be very disastrous.²⁷⁹ As aptly stated by Roell,

A terrorist attack on a fully loaded gas tanker in one of the mega harbours would have a devastating effect on world trade and provide terrorists with an event comparable to 9/11.²⁸⁰

Over the years, some successful maritime attacks have resulted in injuries, loss of lives, and properties. In October 2000, 17 U.S Sailors were killed and 39 wounded in the attack against the US destroyer USS Cole in Yemen.²⁸¹ In October 2002, an Al-Qaeda linked group attacked a French oil tanker, resulting in the death of one crew member and spilling 90,000 tons of oil into the Gulf of Aden. This had a disastrous impact on Yemen's economy as the monthly container traffic fell from 43,000 to 3,000, and many labourers at the port lost their jobs.²⁸² In February 2004, a ferry was attacked in the Philippines and 116 people died.²⁸³ In July 2010, a Japanese oil tanker was attacked in the Strait of Hormuz. This attack caused serious destruction to the hull and led to the death of a crew member.²⁸⁴ More recently, the foreign minister of the United Arab Emirate labelled an attack on four commercial oil tankers off Fujairah as 'a dangerous escalation'.²⁸⁵ Also, the explosions in the Gulf of Oman,

²⁷⁷ Feldt *et al* *ISPSW Strategy Series: Focus on Defence and International Security* 5.

²⁷⁸ Herbert-Burns "Countering Piracy, Trafficking, and Terrorism: Ensuring Maritime Security in the Indian Ocean" in Michel & Sticklor (eds.) *Indian Ocean Rising: Maritime Security and Policy Challenges* 2012 Washington: STIMSON 23-39.

²⁷⁹ Roell "Maritime Terrorism. A threat to world trade" 2009 *Institut für Strategie-Politik-Sicherheits- und Wirtschaftsberatung Berlin* 1 4.

²⁸⁰ *Ibid.*

²⁸¹ Attack on the USS Cole, <https://al-bab.com/attack-uss-cole> (accessed 2019-06-20).

²⁸² BBC News "Yemen says tanker blast was terrorism" (2002-10-16) 1. http://news.bbc.co.uk/2/hi/middle_east/2334865.stm (accessed on 2019-06-20)

²⁸³ The Associated Press "World Briefing\ Asia: The Philippines: Bomb Caused Ferry Fire" (2004-10-12) *The New York Times* 1.

²⁸⁴ UAE confirms oil tanker attack, Al Jazeera, <https://www.aljazeera.com/news/2010/8/6/uae-confirms-oil-tanker-attack> (accessed 2019-06-20).

²⁸⁵ Nada Altaher and Ben Westcott, CNN news report of May 13, 2019 <https://edition.cnn.com/2019/05/12/middleeast/uae-cargo-ship-sabotage-intl/index.html> (accessed 2019-06-20).

which were alleged to have been caused by limpet mines on two tankers bearing Iranian hallmarks, is an addition to the list of maritime attacks. The above-listed attacks are non-exhaustive but intended to highlight the violent nature of the growing threats to maritime security.

In addition to this list of maritime attacks is the modern threat of MCAs. It occurs through ICT platforms by permitting illicit activities which have the potential of causing loss of lives, damage to property, and pollution to the marine environment of a State. Although the general overview of cyber-attack and other incidents at sea have been previously discussed, it is imperative to critically assess these maritime attacks in the context of international law. Assessing the forceful nature of these violent acts against maritime security provides the elements for determining their qualification as use of force.

3.1.2. Historical Background on the Use of Force

The usual understanding of the use of force has evolved from the ancient natural law school of thought era to the present age where it is prohibited by the United Nations (UN) Charter.²⁸⁶ In the ancient era, the natural law scholars depicted the use of force as the divine will to fight for a just cause for good to triumph over evil.²⁸⁷ The emergence of positivism in the nineteenth century marked the next era. This period has been referred to as the positivist period as it marked the emergence of sovereign States with the sovereign rights to war through unilateral declarations.²⁸⁸ In this era, the use of force was either a full-blown war or limited actions in self-defence to address a particular incident.²⁸⁹ After the first world war, States agreed to establish limitations to the right to war.²⁹⁰ In 1919, the Covenant of the League of Nations was signed and came into force in January 1920, together with the rest of the Treaty of Versailles.²⁹¹ This Covenant could not achieve its objective to prevent war because a consensus could not be formed in taking decisions.²⁹² States such as Japan, Italy

²⁸⁶ Article 2(4) of the United Nations Charter.

²⁸⁷ Arend and Beck *International Law and the Use of Force: Beyond the UN Charter Paradigm* (1993) 12-15.

²⁸⁸ Arend and Beck *International Law* 17.

²⁸⁹ *Ibid.*

²⁹⁰ Arend and Beck *International Law* 19-20.

²⁹¹ Covenant of the League of Nations of 1919 13(2) AJIL Suppl 128; adopted: 28.04.1919; EIF: 10.01.1920)

²⁹² Paquin "Why Did the League of Nations Fail?" 1943 34(3) *The Social Studies* 121 122.

and Germany left the organisation, while the US never joined.²⁹³ They returned to the old style of collective self-defence by States based on coalitions.²⁹⁴ As aptly stated by Fenwick,

the failure of the League is the failure of the plan of collective security embodied in Articles 10, 11 and 16 of the Covenant.²⁹⁵

In 1928, the Kellogg-Briand Pact was signed to prohibit the use of force as a way for dispute settlement and to seek peaceful means for settling disputes.²⁹⁶ The concept of self-defence was not defined in the text of the Pact, but it was implied by States so much so that States waged war without declaring it under the guise of self-defence.²⁹⁷

After the second world war, 50 countries came together in 1945 to complete a draft of the UN Charter which later came into force in 1945 after being ratified by 29 countries.²⁹⁸ The UN Charter prohibits the use of force against other States except in certain circumstances. As aptly stated by Merriam,

Two key sources of law on the state's right to self-defence arose in the 19th and 20th centuries, ... Each of these instances provides an example of the continuing influence of the natural law on international law.²⁹⁹

Based on this historical account, it is submitted that the prohibition of the use of force is a fundamental part of the evolving principle of *jus ad bellum*. This principle governs when States may lawfully recourse to the use of force against another State.³⁰⁰ It entails issues regarding States' having the right authority, right intention, acting proportionally, and going to war as a last resort.

It is against this historical background that the use of force is being interpreted within maritime cyber security. The legal doctrines applied by scholars to interpret the provision of the UN charter on the use of force has been generally grouped into

²⁹³ Waxman "5 Things to Know About the League of Nations" (25 January 2019) <https://time.com/5507628/league-of-nations-history-legacy/> accessed 2021-03-24).

²⁹⁴ UN Geneva "League of Nations" (undated) <https://www.ungeneva.org/en/history/league-of-nations> (accessed 2021-08-02).

²⁹⁵ Fenwick "The 'Failure' of the League of Nations" 1936 30(3) *The American Journal of International Law* 506 507.

²⁹⁶ DeBenedetti "Borah and the Kellogg-Briand Pact" 1972 63(1) *The Pacific Northwest Quarterly* 22 23.

²⁹⁷ Quigley *Tragedy and Hope* (1966) 294.

²⁹⁸ USA Office of the Historian "The Formation of the United Nations, 1945" (undated) <https://history.state.gov/milestones/1937-1945/un> (accessed 2021-03-24).

²⁹⁹ Merriam "Natural Law and Self-Defence" 2010 206 *Military Law Review* 43 59

³⁰⁰ Carr *Inside Cyber Warfare* 2ed (2012) 48.

restrictive and expansionist (also known as extensive) perspectives.³⁰¹ While the restrictive scholars, mainly in Europe, adopt a positivist approach, the expansionists, who are predominantly United States scholars, are receptive towards interpretations in line with their national policies.³⁰² The restrictive and expansionist approaches can be mutually dependent because they clarify what the law provides concerning the prohibition on the use of force and the reality of its practical application, respectively. Adopting a hybrid application of both approaches can create a balanced interpretation of article 2(4) of the UN Charter. This will allow the law to evolve while adapting to contemporary security challenges such as MCAs.

3.2. Maritime Cyber Operation, Interference or Attack

As previously discussed, the terms “maritime cyber-attack, operation and interference” have been used interchangeably by various scholars in describing cyber incidents. Understanding which of them can amount to forceful and / or illegal acts in the maritime domain is fundamental. Defining or describing these terminologies provides clarification for determining the legal obligations of States when acting in self-defence for the purpose of article 51 of the UN Charter. It showcases their differences, similarities, contradictions, and possible overlaps. In understanding MCA as use of force, it is important to analyse the definitions proffered by scholars in explaining MCI as cyber operations or cyber-attacks that cause damage to property or grievous harm or possible impediment to the optimum functioning of an operating system. These attacks can be carried out by either an aggressor or in defence. They are of various types and can be broadly classified as active or passive.

3.2.1. Maritime Cyber Operation

Cyberspace is an equipped realm that uses electronics to carry information through interrelated systems and structures. It is a platform through which cyber operations take place and requires proper regulation.³⁰³ It has been described as:

³⁰¹ Ruys “Divergent Views on the Charter Norms on the Use of Force — A Transatlantic Divide?” 2015 109 *Proceedings of the Annual Meeting* 67 67-68; Corten *The Law Against War* (2010) 5.

³⁰² Koskenniemi “Iraq and the ‘Bush Doctrine’ of Pre-emptive Self-Defence. Expert analysis”, Crimes of War Project” (20 August 2002) www.crimesofwar.org/expert/bushkoskenniemi.html (accessed 2021-04-06).

³⁰³ Kuehl “From Cyberspace to Cyberpower: Defining the Problem” in *Cyberpower and National Security* (2009) 26-28.

A domain that refers to a theoretical environment comprised of the Internet together with other computer and telecommunications networks, connected to the Internet or not.³⁰⁴

This implies that cyber operations refer to all activities in cyberspace that rely on legal or illegal information technology. It is submitted that this is a broad classification for all activities in cyberspace, irrespective of the perpetrators, the legality of their acts, or attributability. For this research, when these activities occur in the marine environment, such as involving the operating systems of ships, ports, oil rigs or other maritime installations, they can be described as maritime cyber operations (MCOs). When cyber operations become unlawful and are perpetrated by individuals who are not sponsored by a State, they are classified as cybercrimes. These cybercriminals have been described as cyberterrorists, hacktivists, state-sponsored actor depending on their intent, the complexity of their attack and the sponsorship.³⁰⁵ They have been categorised based on their level of sophistication into:

1. Established actors – those with the most advanced, accurate, and agile tools.
2. Emerging actors – which include nation-states, criminal organizations and those with defined processes.
3. Opportunistic actors – generally those associated with cybercriminal activity. An important differentiator in the three categories of this framework of sophistication is motivation.³⁰⁶

Based on these descriptions of unlawful cyber operations by non-State actors, it is submitted that MCOs can be determined by assessing the nature of the cyber operation, the motive and/ or the actor's target, and the possibility of State-sponsorship or other accomplices. Identifying the actors involved in an MCO is relevant in determining either State response or State responsibility.

3.2.2. Maritime Cyber Interference

The Tallinn Manual has described cyber interference as a non-consensual cyber operation that disturbs the state of affairs of a State, thereby violating its

³⁰⁴ Delerue *Cyber Operations and International Law* (2020) 29.

³⁰⁵ Testimony of Lillian Ablon "Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data" Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, on 15 March 2018, 2. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf (accessed 2022-05-19).

³⁰⁶ Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar. 2019 Public-Private Analytic Exchange Program https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf (accessed 2022-05-19).

sovereignty.³⁰⁷ This means that for a cyber operation to become cyber interference, it must intrude or tamper with the functionality of the infrastructures of a State. Non-state actors may also suffer from cyber interference. For this research, when the target's location, the origin of the intrusion or consequences of the cyber interference is situated in the marine environment, it can be referred to as maritime cyber interference (MCI). MCI can evolve into a more complex form of a cyber incident with more severe consequences.

3.2.3. Maritime Cyber-Attack

Understanding the concept of maritime cyber-attack is relevant to the core of this research. Certain maritime cyber operations, incidents or interference can be seen as forms of attack. The concept of attack has been defined as “acts of violence against the adversary, whether in offence or defence”.³⁰⁸ This hostility can occur at sea.³⁰⁹ A cyber-attack has been defined as:

a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.³¹⁰

This means that the grievous consequence or impact of the maritime cyber operation determines its qualification as an MCA. The ICJ expressed this legal reasoning in the *Nicaragua case* when it ruled that the act qualifying an incident as use of force can be determined by the consequence of that act and not strictly through the type of weaponry.³¹¹ The *Nuclear Weapons case* also affirms that the type of weaponry capable of being used to cause an attack is not limited to kinetic military weapons.³¹² It can be submitted that; an attack can be launched using cyber weaponry and it can qualify as a forcible act when its consequence is severe. Therefore, an MCA refers to the use of cyber weaponry, which can be described as cyber force, with the intent to destroy, alter, or disrupt information or data of maritime infrastructures. This

³⁰⁷ Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2017) 22-13, 313.

³⁰⁸ Article 49(1) Additional Protocol I to the Geneva Conventions.

³⁰⁹ Article 49(3) Additional Protocol I to the Geneva Conventions.

³¹⁰ Schmitt (ed.) *Tallinn Manual* 415, Rule 92.

³¹¹ *Military and Paramilitary Activities (Nicaragua v. U.S.)*, 1986 I.C.J. 4, para [228].

³¹² *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, July 8, 1996, ICJ Rep. 1996, 244 par [39].

involves cyber-attacks against computer resources on ports, ships, and all programmed maritime operations.³¹³

These definitions of cyber-attack can be categorised by the perspective from which they are drawn. They include the permissive, functionality, restrictive and motive perspectives.³¹⁴ The permissive perspective does not emphasise prohibition but the inference from the negative consequence of an act.³¹⁵ The functionality perspective focuses on the consequences of threat to the ability and fitness of the target. It refers to hostile acts that create a situation whereby the target cannot play its role or be utilised.³¹⁶ The restrictive perspective focuses on the restriction on optimum performance, which leads to unfavourable consequences.³¹⁷ The motive perspective, as the name implies, assesses or infers the intention to cause a particular defect. It depicts the purpose or reason behind specific actions.

Cyber-attacks have been described as:

having direct secondary effects resulting in physical casualties, substantial physical damage, or such substantial and long-term damage to critical infrastructure that the carrying out of a State's essential functions or its social and political stability are seriously impaired should...³¹⁸

This definition has been labelled as a highly permissive view.³¹⁹ This is because it suggests accommodating the negative consequence of these damaging cyber operations to label them as cyber-attacks.

Another view that was expressed by most of the experts in the Tallinn Manual is the functionality view. This view sees cyber operation in the form of a cyber-attack, either from an aggressor or a defending State, as that which is reasonably expected to cause grievous damage to persons or property or impede effective operation necessitating the substitution of a physical component.³²⁰ This view appears to be 'non-permissive of the damages caused by cyber operation but creates room for anticipating it and preventing its occurrence. Its emphasis on possible damage to

³¹³ Hayes *Maritime Cybersecurity: The Future of National Security* (doctoral thesis, Naval Postgraduate School Monterey, California) 2016 6.

³¹⁴ Roberts 2017 SSRN 16.

³¹⁵ Merriam Webster Dictionary "Permissive" <https://www.merriam-webster.com/dictionary/permissive> (accessed 2019-03-13).

³¹⁶ Roberts 2017 supra.

³¹⁷ *Ibid.*

³¹⁸ Gill and Ducheine 2013 *International Law Studies* 438, 460.

³¹⁹ *Ibid.*

³²⁰ Gill and Ducheine 2013 *International Law Studies* 417.

critical components to the extent of needing replacement³²¹ can be seen as a limitation. This limitation creates a dichotomy between cyber operations that can be labelled as cyber-attack and other forms of cyber operations. Other forms of potentially damaging cyber operations that do not impede the functionality of components which will require replacements are not accommodated by this definition. Therefore, permissiveness still features in this definition despite the focus on functionality in assessing the potential damage that the cyber-attack can cause.

Another description worth considering is from the perspective that all cyber operations expected to cause death, injury, or physical damage and disability to a computer or computer network include severely disruptive denial of service can amount to a cyber-attack.³²² This view has been criticised as being restrictive. The restriction to specific consequences of the cyber-attack is not all-encompassing. There are other grave forms of problems caused by cyber-attacks that may not fit into the above-listed categories. In addition, a restrictive definition asserts that cyber warfare is “an attack by one hostile nation against the computers or networks of another to cause disruption or damage.”³²³ This definition has been criticised for its non-inclusion of cyber activities by terrorists and other individuals. This can lead to a state’s inability to lawfully invoke article 51 of the UN Charter against these non-state actors.³²⁴ Notwithstanding, States do not lose their inherent right of self-defence in the circumstance. They may use necessary force within the confines of international law and domestic laws of the adversary’s host country.

Furthermore, cyber-attack has been described that as:

[consisting] of any action taken to undermine the functions of a computer network for a political or national security purpose.³²⁵

This description can be criticised as narrow because it makes no room for other motives except politics and national security. Sometimes, cyber-attacks are carried out for economic disruption and cause civil turmoil.³²⁶

³²¹ *Ibid.*

³²² Roberts 2017 SSRN 16-17

³²³ Shackelford and Andres “State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem” 2011 42 *Georgetown Journal of International Law* 971 978.

³²⁴ Roberts “Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors” 2014 41 *Northern Kentucky Law Review* 535 539.

³²⁵ Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue and Spiegel “The Law of Cyber-Attack” 2012 100 *California Law Review* 817 826.

Cyber-attack has also been defined as:

[T]he unauthorised penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls.³²⁷

This definition mainly focuses on the motive and effect of unauthorised cyber operations on data stored on state-owned computers. If interpreted literally, cyber-attacks against individuals are excluded.

In addition, the cyber operation has been defined from a 'target' perspective. It refers to a cyber-attack that involves an incursion on the computer systems of any vital state-owned infrastructure regardless of the consequences of any material damage or fatalities.³²⁸ From this definition, it can be inferred that a specific target can determine whether a cyber-attack can be said to have occurred. This definition has been criticised as misleading because it focuses only on the object of the attack in determining the occurrence of a cyber-attack without specific reference to the instruments of the attack.³²⁹ It is submitted that both opinions reflect a combination of factors that should be considered simultaneously to ascertain the occurrence of a cyber-attack correctly.

Another definition of a cyber-attack is an attack that leads to the compilation of propaganda intended to undermine society and the State and compel the state to formulate resolutions in support of an opposition party.³³⁰ This definition portrays an unlawful cyber operation from a psychological perspective. For instance, the alleged Russian interference in the 2016 US election through flooding the Internet with false news to sway voters in a specific direction can be seen as a case in point.³³¹

³²⁶ Roberts *Northern Kentucky Law Review* 539; Kilovaty "Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare" 2015 4(3) *Journal of Law and Cyber Warfare* 210 210.

³²⁷ Clarke and Knake *Cyber War* (2010) 246.

³²⁸ Banks and Criddle, "Customary Constraints on the Use of Force: Article 51 with an American Accent" 2016 29(1) *Leiden Journal International Law* 67 89.

³²⁹ Nguyen "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare" 2013 101(4) *California Law Review* 1079 1086-1087.

³³⁰ See fn 59 above at 1 825 (quoting *Shanghai Cooperation Agreement*, Shanghai Cooperation Organization, Annex 1, 209).

³³¹ Van De Velde "The Law of Cyber Interference in Elections" (2017) 10 <https://ssrn.com/abstract=3043828> (accessed 2019-04-01).

The Budapest Convention on cybercrime classifies cyber incidents into a list of crimes, including illegal access, illegal interception, and system and data interference.³³² It refers to illegal access as the total or partial access to a computer system without rights that could be committed by breaching safety measures with dishonest purposes such as acquiring computer data wrongfully.³³³ Illegal interception is criminalised as the intentional and unjustified technical interference of private computer data transmissions.³³⁴ This treaty defines data interference as the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right, which may or may not cause serious harm.³³⁵ Likewise, it describes system interference as the illegal obstruction of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.³³⁶ These actions violate the integrity, confidentiality of computer and data systems. The convention portrays them as crimes under criminal law. It is submitted that describing these offences as crimes appears to create a presumption that they are below the threshold of armed attack but should be addressed by domestic laws of affected States.

From the above definitions, a few things can be observed. Most of the scholars use the terminologies such as cyber-attack, operations, intrusion, and warfare interchangeably. Some interpretations have broadened the scope of cyber security, while others have narrowed it in their analysis by limiting the cyber acts to States. Also, some have focused on the intangible use of the Internet without considering the possibility of using kinetic force against servers or other computer installations as a form of cyber-attack. It can be observed that some definitions do not reflect the reality of the modern threat of cyber-attack. It is better in assessing maritime cyber security to view malicious hacking of computer systems at sea as a form or threat of cyber-attack³³⁷ once detected even without known proof of specific damage. This is due to the increased frequency and sophistication of threats of modern cyber interference, which sometimes prevent an immediate knowledge of the extent of the damage.

³³² Articles 2-11 of the Budapest Convention on Cybercrime, 2011.

³³³ Article 2 of the Budapest Convention on Cybercrime, 2011.

³³⁴ Article 3 of the Budapest Convention on Cybercrime, 2011.

³³⁵ Article 4 of the Budapest Convention on Cybercrime, 2011.

³³⁶ Article 5 of the Budapest Convention on Cybercrime, 2011.

³³⁷ DeLuca "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors" 2013 3(9) *Pace International Law Review Online Companion* 278 281.

Furthermore, it seems the definitions of cyber-attack may be relative and tailored to synchronise with the foreign policies of different States.³³⁸ The United States of America, on the one hand, advocates for its inherent right to self-defence against all forms of cyber operations from an aggressor because they should be seen as an attack on or threat to the United States. From its perspective, it focuses on the purpose of the cyber-attack by restricting it to aggressive acts against critical cyber systems.³³⁹ Likewise, the Shanghai Cooperation Organization³⁴⁰ has a similar perception on the issue of threats of cyber-attacks. Its scope in defining cyber-attack is broadly inclusive of using cyber operations to cause political instability.³⁴¹

Notwithstanding the plurality of definitions from various perspectives, applying them to the context of maritime cyber incidents may lead to a uniquely recommendable definition. Hence, an MCI or MCA can be defined as an act performed through electronic means that has a direct or indirect effect at sea, is unauthorised and therefore prima facie illegal. It is important to note that defending against this illegal activity may require cyber operations or kinetic force to thwart the cyber-attack.³⁴² This means that MCI may be carried out by different means to disrupt the optimum functioning of an Internet-dependent operating system of a ship.³⁴³ States may interpret this disruption as a threat to their maritime security depending on the existing international relationship between the affected States and their foreign policies. It may either be called MCA or MCI if it falls below the threshold of armed attack.³⁴⁴ A State's perception of the severity of an MCI can be a primary deciding factor for whether it qualifies as an MCA.

A cyber-attack may be in the form of hacking of computers, bombing of Internet facilities, cutting off communication cables, or infecting an operating system with viruses.³⁴⁵ The classification as MCA is based on the occurrence of cyber-attacks in

³³⁸ Waxman "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" 2011 36 *Yale Journal of International Law* 421 458-59.

³³⁹ Hathaway *et al.* "The Law of Cyber-Attack" 2012 100 *California Law Review* 817 824.

³⁴⁰ The Shanghai Cooperation Organization is a security cooperation group whose membership is made up of Russia, China and most of the former Soviet Central Asian republics. It also includes Iran, India, and Pakistan who are observers.

³⁴¹ Hathaway *et al* 2012 *California Law Review* 825.

³⁴² Hathaway *et al* 2012 *California Law Review* 826.

³⁴³ This assertion agrees with the United States' objective-based perspective rather than the means-based view of the Shanghai Cooperation Organization.

³⁴⁴ Hathaway *et al* 2012 *California Law Review* 833.

³⁴⁵ Hathaway *et al* 2012 *California Law Review* 826.

the maritime domain. A mild MCA may sometimes be classified as a mere interference. They may be classified based on their legality and description in international law as crime, terrorism, and warfare. Also, they may be identified as active or passive attacks.³⁴⁶ A recent report by GAO on cyber weaponry outlines examples of cyber interference³⁴⁷ which may qualify as a cyber-attack. An attack that is characterised by flooding the network, systems, or applications with enormous data traffic, thereby frustrating their use, is referred to as a “denial of service” (DOS).³⁴⁸ This attack could be more complex when several hosts are used to perform it, making it look like multiple attacks from various sources. This complex form of DOS is referred to as distributed denial of service (DDOS).³⁴⁹ Another dangerous type of cyber interference is malicious software. It is popularly referred to as “malware”. This secretly inserted program is usually intended to compromise the privacy, veracity and accessibility of the victim’s operating systems, records, or applications.³⁵⁰ This malware can be in various forms such as worms, Trojan horses, logic bombs, viruses and ransomware.

Also, an MCA can be in the form of eavesdropping, whereby the attacker seizes and modifies data communication and then re-inserts the altered information. This is popularly known as “man-in-the-middle”.³⁵¹ An attacker can use an encrypted version of a victim’s login details to access a system without knowing the login details. Also, an attacker can use different phishing methods,³⁵² which entail obtaining confidential information by deception to compromise systems or networks. They can also alter folder questions, especially in online applications intended to compromise information on record.³⁵³ This is usually referred to as structured query

³⁴⁶ Stahl “The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cyber Security” 2011 40 *Georgia Journal of International and Comparative Law* 247 261.

³⁴⁷ Government Accountability Office, Weapons Systems Cybersecurity GAO-19-128 (October 18, 2018) Report to the Committee on Armed Services, U.S. Senate 41.

³⁴⁸ *Ibid.*

³⁴⁹ *Ibid.*

³⁵⁰ *Ibid.*

³⁵¹ *Ibid.*

³⁵² Phishing- when the attacker masquerades as a legitimate business or reputable person via an email or website to obtain certain information; Spear phishing- when phishing attacks are closely tailored to the audience; and Whaling - phishing that targets high ranking members of organisations.

³⁵³ Government Accountability Office, Weapons Systems Cybersecurity GAO-19-128 (October 18, 2018) Report to the Committee on Armed Services, U.S. Senate 41.

language injection. An attacker can insert susceptibilities in hardware or software to allow the developer to influence the victims' systems anytime in the future remotely.

The above possibilities of MCAs are non-exhaustive. It has been argued that their classifications as active and destructive or passive and non-destructive may assist in determining whether an MCA is a mere cyber-attack or an armed attack.³⁵⁴ Despite the various nomenclatures, including cyber aggression, cyber-attack, cyber interference, cyber warfare, cyber terrorism, and cybercrime, there is a similar feature of a cyber form of hostility. This hostile act can be carried out by an adversary or in defence of a victim. They have been broadly categorised as destructive, that is, when a cyber-attack is deliberate and intended to cause damage to the target's operating systems, and non-destructive, that is when the cyber activity is to exploit confidential information.³⁵⁵ Despite the classifications, destructive and non-destructive cyber operations may be generally offensive. Especially in the case of non-destructive cyber operations, also known as cyber exploitation, obtaining confidential information through non-destructive means does not erase the likelihood of destruction. The technical nature of the cyber activities in both cases may be different due to the disparity in motives. However, cyber-attack and cyber exploitation take advantage of the vulnerability of the victim.³⁵⁶

Legal analysis of both classifications of attack and exploitation can lead to different policy pathways. Questions about when cyber activities are legal or illegal may arise and when they amount to an armed attack or use of force. On the one hand, illegal maritime cyber operations can be referred to as those that jeopardise a coastal State's security or economic sovereignty. The use of malware³⁵⁷ and other cyber activities to cause grievous bodily harm, to inflict financial losses, destruction, and damage to property at sea, are examples of wrongful MCAs.³⁵⁸ They can be carried out by individuals and generally referred to as cybercrime or by the State and referred to as cyber-attack.

³⁵⁴ Lin "Offensive Cyber Operations and the Use of Force" 2010 4 *Journal of National Security Law and Policy* 63 63.

³⁵⁵ *Ibid.*

³⁵⁶ Lin 2010 *Journal of National Security Law and Policy* 64.

³⁵⁷ Malicious Software delivered through the Internet.

³⁵⁸ Schimdt *Tallinn Manual 2.0* 106.

The Tallinn manual³⁵⁹ provides an insight into cyber activities that may be illegal. Although its list is non-exhaustive, it is worth investigating. Unlawful threat or use of force by cyber means is a form of illegal cyber operation by a State against another State which jeopardises the national security of the victim-State by inhibiting the optimum functioning of information technology-reliant maritime infrastructure.³⁶⁰ Activities involving cyber-enabled weapons with potential adverse effects aboard or beyond the ship are illegal cyber-attacks.³⁶¹ It refers to the use of cyber weaponry as described earlier, including malware and DDOS , which can hamper efficiency of the communication, navigation, and other operating systems on or linked to the ship.³⁶² Cyber exploitation of confidential security information is illegal as well. The misuse of confidential security information may lead to grave consequences and may be seen as a threat to national security. Also, unauthorised research conducted through cyber means is illegal.³⁶³ This form of cyber espionage is unlawful but may not affect the functioning of the operating systems linked directly or indirectly to the ship. It is less likely to rise to the level of a cyber-attack immediately. However, the long-term consequence of what the aggressor might do with information gotten through the illegal surveillance may not be accurately determined. Cyber interference of States' infrastructures such as communication systems, power grids, transportation systems or security equipment operated by cyber connections amounts to illegal cyber operations.³⁶⁴

Hostile intent is required in determining an illegal cyber operation.³⁶⁵ If the aggressor does not expressly state it, it could be inferred from the type of intrusion. According to Jensen,³⁶⁶

Regardless of the perpetrator's identity, he has either demonstrated hostile intent or committed a hostile act by attempting to penetrate a computer system linked to critical national infrastructure. Such an intrusion must be considered an unlawful use of force under international law.³⁶⁷

³⁵⁹ Schimdt *Tallinn Manual 2.0* 242.

³⁶⁰ *Ibid.*

³⁶¹ *Ibid.*

³⁶² *Ibid.*

³⁶³ *Ibid.*

³⁶⁴ *Ibid.*

³⁶⁵ Sharp (Sr.) *Cyberspace and the Use of Force* (1999) 132.

³⁶⁶ Professor, International and Operational Law Department, The Judge Advocate General's School, U.S. Army.

³⁶⁷ Jensen "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defence" 2002 38 *Stanford Journal of International Law* 207 235.

It is submitted that the demonstration of hostile intent confirms the forceful nature of an illegal act when it is non-consensual, and its target is a critical national infrastructure. As Jensen rightly stated, such a cyber-attack qualifies as the use of force. There are instances where cyber operations are routed through other computers without the users' knowledge before hitting the target. The oblivious users who do not know about their computers' involvement are eschewed from being responsible for the illegality due to the absence of hostile intent. This will be discussed in detail in the next section below.

Contrarily, legal forms of cyber-attacks refer to statutorily permitted instances when computer-generated operations can be used in defence against an adversary. For example, if a cyber-attack is detected onboard a ship that threatens its navigational system. It can apply maritime cyber security measures to repel the cyber-attack to prevent the vessel from being damaged or lost at sea. However, there are other measures apart from Internet-related responses. Kinetic force can be used by destroying the server which is powering the cyber-attack. This destruction could be done by dropping bombs or missiles or any other necessary and proportional means to thwart the cyber-attack. Also, the victim State can suspend the right of innocent passage³⁶⁸ to vessels that are reasonably believed to pose a grave threat to the maritime cyber security of the victim State. In addition, submarine communication cables of an aggressor can be cut to foil their threatening maritime cyber activities.

3.3. Use of Force in the Context of Maritime Cyber Security

After understanding that threats to maritime security include cyber-attacks, it is critical to determine whether a cyber threat or hostility falls within the scope of use of force. This will enable proper legal framework analysis about MCA and anticipatory self-defence against it. It is relevant for clarifying the yardstick needed to determine when to establish whether a maritime cyber-attack is an armed attack or not and the legitimate response, which will be discussed in the next chapter.

3.3.1. Meaning of Force

It is essential to know the meaning of force for proper contextualisation and interpretation of its legal implications. Some of the incidental issues in international

³⁶⁸ Schimdt *Tallinn Manual 2.0* 242.

law, such as the peremptory norm of the prohibition against the use of force,³⁶⁹ legal uses of force, and acts that fall below the threshold of force, require a preliminary understanding of the meaning of the legal term “force”.³⁷⁰ What is the meaning of force? The connotative meaning of force suggests a degree of compulsion or violence targeted towards someone, something, or the achievement of an objective. Historically, States used force to acquire new territories through conquest.

In the legal context, force is often used to depict duress or coercion, which has legal implications depending on the context.³⁷¹ It may be used lawfully or unlawfully. It is a descriptive constituent of legal terminologies such as aggression, armed attack, cyber-attack, cyber-crime. These terminologies may differ or overlap depending on the perspective from which they are assessed. Notably, there is no universal definition for the use of force, but its principle is predicated upon the provisions of articles 2(4) and 51 of the UN Charter. The former generally prohibits the use of force, while the latter lawfully permits it in the context of self-defence. Article 2(4) has been described as the origin of present-day conversation about what amounts to the use of force.³⁷² It is the legal foundation for all analyses on the contemporary conflicts between States which emanate from perceived threat or violation of their territorial integrity and political sovereignty. It creates the basis for determining the options available to States when acting in self-defence.

Lin has described the use of force as:

Actions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not these actions cause immediate physical damage.³⁷³

These actions can be in the form of political or economic pressure with varying degrees of consequences. They can involve the use of the military or State-sponsored non-State actors. These different forms of force may be combined to achieve the desired agenda, such as a maritime cyber-attack. Relying on Lin’s

³⁶⁹ Orakhelashvili *Peremptory Norms in International Law* (2009) 51.

³⁷⁰ Ruys “The Meaning of Force and the Boundaries of the *Jus Ad Bellum*: Are Minimal uses of Force Excluded from UN Charter Article 2(4)?” 2014 108(2) *The American Journal of International Law* 159 160-162.

³⁷¹ For instance, article 51 of the UN Charter makes provision for when force can be used legally in self-defence.

³⁷² Scott, Billingsley and Michaelsen *International Law and the Use of Force: A Documentary and Reference Guide* (2009) 57.

³⁷³ Lin 2010 *Journal of National Security Law and Policy* 74.

description of the use of force, when a maritime cyber-attack creates an effect that prevents a critical maritime infrastructure from being used for its designed purpose, it is a forceful act. The damaging consequences may vary in form and severity. It is submitted that a major MCA which impedes the operation of a State's crucial marine infrastructure can be reasonably treated as a use of force. What reasonable standard may be applied to ascertain this?

Generally, the use of force is unlawful and prohibited, especially in the context of inter-state relationships. More specifically, article 2(4) of the UN Charter prohibits the use of force in its provision, 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.

It can be inferred that prohibition against the use of force encompasses the threat of force. This means that the prohibition of the use of force also makes the threat of force illegal. The provision prohibits all forms of force that oppose territorial integrity and political sovereignty.³⁷⁴ Territorial integrity refers to the inviolability of a State's territory, which is manifested through political independence.³⁷⁵ Therefore, a direct violation of territorial integrity will always constitute a use of force.

The interpretation of what use of force entails has led scholars to argue that it should not include economic, political, or psychological coercion.³⁷⁶ This interpretation has been challenged by innovation and technology, which now can employ an intangible form of coercion to cause death. For instance, the artificial cardiac pacemaker of a patient who underwent a heart procedure can be remotely hacked through a cyber-attack that can cause death.³⁷⁷ Likewise, a cargo ship with chemical tankers can be

³⁷⁴ Corten *The Law Against War* (2010) 201 states that: "The rule prohibiting the use of force has generally been characterised as jus cogens both by States (a) and by doctrine and case law (b)."; The International Law Commission has also stated that: "the most reliable known example of a peremptory norm [is] the prohibition of the use of armed force in violation of principles of international law embodied in the Charter" A/37/10, 3 May–23 July 1982 (1982) YILC, II Part Two, 56, par [2].

³⁷⁵ Oppenheim „International Law“ in *Disputes, War and Neutrality* 7ed (1952) 154.

³⁷⁶ Li "When Does Internet Denial Trigger the Right of Armed Self-Defence?" 2013 38 *Yale Journal of International Law* 179, 184; Doc. 215, I/1/10, 6 U.N.I.C.O Docs. 559 (1945). See Doc. 784, I/1/27, 6 UNICO Docs. 334- 35 (1945). Brazil proposed an amendment to article 2(4) of the UN Charter should include the words: "and from the threat or use of economic measures" but it was rejected by a vote of 26 – 2.

³⁷⁷ Kuehn B.M. "Pacemaker Recall Highlights Security Concerns for Implantable Devices" www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.118.037331 (accessed 2020-02-17) .

heated until it explodes³⁷⁸ due to electronic malfunction. In 1945, the drafters of the UN Charter did not envisage this possibility since the technology was not available at the time. With the evolving forms of weaponry that may be employed to cause grievous harm, the understanding of the use of force is beginning to change.

Schmitt defines the use of force³⁷⁹ which is relevant in determining the status of MCA as a form of force. His definition of 'threat of force' is relevant to assessing the legality of anticipatory self-defence against MCA. Conversely, force may be lawfully used in certain statutorily permitted circumstances. For instance, force may be permitted in self-defence, but it must be reasonable. Reasonable force is determined by certain factors, which include necessity and proportionality. This will be discussed in the following chapters. The use of force has been described as an act of aggression against another State.³⁸⁰ It is an act that violates the sovereignty and territorial integrity of another State.

Based on the above scholarly descriptions and interpretation of the international law prohibition on the use of force, it is submitted that understanding the use of force requires a flexible approach. This can be observed in the ICJ ruling on the Nicaragua case that an act of intervention does not always determine the use of force. The outcome of the type of force used is a significant determinant for labelling the incident a use of force.³⁸¹ Also, article 41 of the UN Charter provides a list of non-armed uses of force, including complete or partial interruption of the sea and other means of communication. Can this be interpreted to cover cyber-attack as a form of use of force? This will be discussed in the next section.

3.3.2. Maritime Cyber-Attack as a Type of Force

The legal paradigm of use of force as initially conceived has evolved over the years to accommodate other ways of exerting force without guns and bombs. States have recently witnessed the use of force as an act of self-defence against a new form of 'armed force' of cyber-attack. This reflects the argument that:

³⁷⁸ The Maritime Executive "MAIB: Overheated Cargo Caused Stolt Groenland Explosion" (20 July 2021) <https://www.maritime-executive.com/article/maib-overheated-cargo-caused-stolt-groenland-explosion> (accessed 2021-07-23)..

³⁷⁹ Schmidt (*Tallinn Manual 2.0* 330.

³⁸⁰ Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. GAOR 6th Comn., 29th Sess., 2319th plen. mtg., Annex, U.N. Doc. A/RES/3314 (XXIX) (1975).

³⁸¹ Military and Paramilitary Activities (*Nicaragua v. U.S.*), 1986 I.C.J. 4, para [228] (27 June 1986).

since 1945 a new legal paradigm has emerged - the 'post-Charter self-help' paradigm. This paradigm, we submit, reflects contemporary international law relating to the recourse to armed force.³⁸²

The potential threat of cyber-attack on a ship can be seen in the fact that a ship can be hijacked and becomes a dangerous weapon while under the attacker's control. It can be used to execute a catastrophic act. This can amount to the use of force and potentially trigger the right to anticipatory self-defence as provided for in the UN Charter.³⁸³ How can force be exercised through cyber means? The answer to this question requires understanding that:

Article 2(4) is a legal rule located in the text of a multilateral treaty which requires adaptation to changing circumstances. The challenge becomes one of remaining faithful to its core meaning without thereby sacrificing the flexibility ordinarily required in interpreting constitutional norms.³⁸⁴

Since article 2(4) of the UN Charter does not specify the methods through which threat or use of force can be exercised, the use of the Internet as a medium for delivery can be on the same theoretical footing as the traditional methods of delivery.³⁸⁵ Despite the argument that the provision on the use of force referred to armed force,³⁸⁶ it may be applied to the cyber context. This would show that cyber force is carried out by unique weapons designed to cause destruction and possible loss of lives.³⁸⁷

Despite the unique nature of cyber-attacks, the legal principles on the use of force may be applied.³⁸⁸ This can be seen in Lin's argument, where he described an instance of the use of force through cyber means:

cyber-attacks on the controlling information technology for a nation's infrastructure that has a significant impact on the functioning of that infrastructure (whether or not it caused immediate large-scale death or destruction of property) would be an armed attack for Article 51 purposes, just

³⁸² Arend and Beck *International Law and the Use of Force: Beyond the UN Charter Paradigm* (2014) 5.

³⁸³ Article 2(4) and 51 of the UN Charter of 1945.

³⁸⁴ Gordon "Article 2 (4) in Historical Context" 1985 10(2) *Yale Journal of International Law* 271 273.

³⁸⁵ Aldrich "How do you Know you are at War in the Information Age?" 1999-2000 22 *Houston Journal of International Law* 223 237.

³⁸⁶ Benatar "The Use of Cyber Force: Need for Legal Justification?" 2009 1 *Gottingen Journal of International Law* 375 384; Randelzhofer "Article 2(4)" in *The Charter of the United Nations: A Commentary* (2002) 118; Schmitt "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" 1998-1999 37 *Columbia Journal of Transnational Law* 885 906-908.

³⁸⁷ Brownlie *International Law and the Use of Force by States* (1963) 362.

³⁸⁸ Gill and Ducheine 2013 *International Law Studies* 439.

as would a kinetic attack that managed to shut down the system without such immediate secondary effects³⁸⁹

This description focuses on undermining the proper functioning of an operating system. It does not emphasise preliminary cyber intrusions which pose threats. For instance, there are cases of cyber exploitation whereby important security information may be stolen without undermining the functioning of that system at that time. Although the stolen data may be used to cause other forms of damages to the victim states' security, it may not be seen as a use of force at the outset because the proper functioning of a system was not impaired.³⁹⁰ The legal implication is that a cyber-attack that threatens peace and security but does not meet the armed attack threshold will not trigger the right of self-defence as provided for in article 51 of the UN Charter.³⁹¹

The ICJ has interpreted the concept of the use of force by clarifying its scope and legal implications. The *Nicaragua* case emphasised that not all use of force may be viewed as armed attack necessitating self-defence as provided for in article 51 UN Charter. This creates two categories of force. The first category is the gravest form of force which may be referred to as armed attack and trigger a response in line with article 51. The second category refers to those below the threshold of an armed attack which is the less grave form of force. The court has applied the 'scale and effect test' in distinguishing between these categories.³⁹² Hence, all armed attacks may use force, but not all use of force can be classified as armed attacks.³⁹³ It is submitted that the degree of the graveness of force indeed determines the categorisation as an armed attack.

In the *Corfu Channel* case, the court suggested that the factor of 'graveness' applies in determining the existence of use of force.³⁹⁴ It ruled that:

³⁸⁹ Lin 2010 *Journal of National Security Law and Policy* 74.

³⁹⁰ Hathaway *et al* 2012 *California Law Review* 830.

³⁹¹ *Nicaragua v US* para [195, 211]; Strydom and Juma "Maintaining International Peace and Security: The Enforcement of International Law" in *International Law* (2016) 204.

³⁹² Military and Paramilitary Activities in and Against Nicaragua par [195].

³⁹³ *Military and Paramilitary Activities in and Against Nicaragua*, par [191]; *Oil Platforms* (Iran v. U.S.), 2003 ICJ Report 161, para [51 and 64].

³⁹⁴ *Corfu Channel Case (United Kingdom v. Albania)*, 1949 ICJ Report p. 4, 23 (Apr.9): Here Albania alleged that the unauthorized mine sweeping operation by the British Navy in Albanian waters was a use of force, but the United Kingdom rejected this accusation by claiming that its actions were limited. The court held that the operation was not a use of force but an infringement on Albania's sovereignty.

nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania. The Court therefore reaches the conclusion that Albania is responsible under international law for the explosions which occurred on October 22nd, 1946, in Albanian waters, and for the damage and loss of human life which resulted from them...³⁹⁵

Despite the court's conclusion, in this case, there are specific actions in international relations though may fall below the threshold of use of force.³⁹⁶ At the end of its judgment, the court stated that the British Navy did not violate article 2(4) with the intent to exercise political pressure on Albania.³⁹⁷ This statement is ambiguous as it neither clearly confirms the thresholds in determining the use of force nor the requirement of the intent to exercise political pressure to qualify an act as a use of force.³⁹⁸

The ICJ distinguished the uses of force that can be classified as armed attack and that which do not meet that threshold by applying the scale and effect criteria.³⁹⁹ In the *Nuclear weapon's case*, the ICJ pointed out, among other things, that both threat and use of force are illegal is prohibited by article 2(4) of the UN Charter. It stated that weapons used as a threat of force do not exclude nuclear weapons.⁴⁰⁰ It ruled that article 2(4) and 51 of the UN Charter:

These provisions do not refer to specific weapons. 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, including nuclear weapons...⁴⁰¹

This judicial reasoning can be extended to recognise cyber force as a form of use of force. This is because force may be applied with various forms of weaponry due to modern technology.

Applying this judicial rationale to MCAs will help to shape the law governing maritime cyber security. Applying the court's criteria in determining the use of force to the maritime context can mean that where a use of force, in the form of an MCA, leads to the death of human beings or destruction or damages to property, it would, in

³⁹⁵ *Corfu Channel* (1949) 23.

³⁹⁶ Corten *The Law Against War* (2010) 69-70.

³⁹⁷ *Corfu Channel* (1949) 23.

³⁹⁸ Ruys 2014 *The American Journal of International Law* 166.

³⁹⁹ *Nicaragua* (1986) 14.

⁴⁰⁰ *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* 1996 ICJ Reports 244 par [39].

⁴⁰¹ *Nuclear Weapons* (1986) 244 par [39].

scale and effect, constitute an armed attack.⁴⁰² It can be reasonably inferred that any invasion with hostile intent that would justify the option to use force constitutes a use of force as provided for in the UN Charter, irrespective of the labelling of such acts by the affected states.⁴⁰³ As rightly stated by Ruys,

the wholesale exclusion of small-scale or targeted forcible acts from the scope of UN Charter Article 2(4) is fraught with conceptual difficulties, does not correspond to actual customary practice, and has unfortunate consequences as a matter of policy.⁴⁰⁴

Applying the principles of *jus ad bellum* to cyber operations would qualify them as a cyber force if they resulted in death or grievous harm to individuals or large scale damage or destruction to tangible or intangible property.

3.3.3. Maritime Cyber-attack as Unlawful Use of Force

After establishing above that MCA can qualify as a type of force in certain instances, addressing when this form of force is unlawful is relevant to discussing what States can do to defend against it. Unlawful use of force, which is the focus of this subsection, is prohibited by article 2(4) of the UN Charter. The lawful use of force, which will be discussed in the following chapter, arises when acting in self-defence, as provided in article 51 of the UN Charter. How does MCA qualify as unlawful use of force?

Acts that violate the rules and regulations stipulated by the IMO to ensure maritime security⁴⁰⁵ can be classified as illegal. These maritime attacks adopt varying degrees of violence and sometimes maybe justified when done in self-defence. What makes them illegal can be the accompanying threat to life, property, marine environment and/ or the sovereignty of States. It violates the territorial integrity of a State and can adversely affect its citizens. It challenges the jurisdiction of a State over its maritime zone, ship or port through coercion and threat of tangible or intangible force.

⁴⁰² Schmitt (ed) *Tallinn Manual 2.0* 341.

⁴⁰³ Ruys 2014 *The American Journal of International Law* 171.

⁴⁰⁴ Ruys 2014 *The American Journal of International Law* 210.

⁴⁰⁵ The IMO highlights the relevant instruments that States should comply with to achieve maritime security. These instruments are the 1974 SOLAS as amended, the ISPS Code, the 1988 SUA Convention and its 2005 protocol.

Although the high sea belongs to no State, it is a collective space that should be regulated for safe use by all.⁴⁰⁶

The illegality of maritime attacks is not only determined by the kinetic form of the attack. For instance, IMO states that:

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.⁴⁰⁷

When a technology asset of a ship, port or an oil rig is threatened, maritime security is at risk. This implies that a cyber incident that threatens or results in ‘shipping-related operational, safety or security failure’ is an illegal maritime attack. Notably, this ‘illegal act’ can become justified when proportionately carried out in self-defence. When a technology asset is threatened or employed to cause damage to the marine environment, a maritime cyber incident occurs. Scholars have described this incident as maritime cyber operations, interference, or attack. Understanding these terminologies is relevant in determining the form of force or violence that is created in cyberspace.

The targets of MCAs are maritime vessels, ports, and installations at sea, namely: ships, ports, and oil rigs. Ships at sea carry goods, passengers and can be used by States for military defence activities. They are mainly classified into a bulk carrier, tanker, container, naval, offshore, special purpose and passenger ships.⁴⁰⁸ They are structured according to their intended uses, with modern ones relying on information technology for some or all their operations. Cyber interference aboard a ship can cause operational, safety and security failure.⁴⁰⁹ As aptly stated,

Vulnerable systems onboard include the navigation bridge, cargo handling equipment, the engine room, the power management system, and administrative as well as communicational systems.⁴¹⁰

⁴⁰⁶ UNODC “UNODC Global Maritime Crime Programme” (undated), <https://www.unodc.org/unodc/en/piracy/index.html?ref=menuside> (accessed 2020-02-12).

⁴⁰⁷ <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> (accessed 2020-02-11).

⁴⁰⁸ Marine Insight “A Guide to Types of Ships” <https://www.marineinsight.com/guidelines/a-guide-to-types-of-ships/> (accessed 2020-04-03).

⁴⁰⁹ International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, 2017).

⁴¹⁰ Mraković and Vojinović “Maritime Cyber Security Analysis – How to Reduce Threats?” 2019 13 *Transactions on Maritime Science* 132 133.

The areas of a ship, port or oil rig which are primarily vulnerable include the navigation systems, safety system, engine control and monitoring systems, cargo control systems and drilling systems.⁴¹¹ Interference with the information technology system of these vulnerable areas can adversely jeopardise the safety of personnel and the efficiency of the ship. According to the IHS Markit maritime security survey, navigation systems are the most vulnerable to MCI.⁴¹² For instance, tanker ships that carry flammable liquid cargo can collide and explode because of a cyber-attack on the ship's navigation system. Likewise, a cyber-attack on a passenger ship's vulnerable systems can put passengers' lives in danger.

These vulnerable targets can face unintentional threats from employees' negligence. Attackers can intentionally orchestrate the threats. The attacker's intent can include exploiting the ship's vulnerability to impede the supply chain of an oil rig, diverting a valuable cargo to a pirate territory, causing a cargo ship with chemical tankers to overheat, and disrupting the engine and monitoring control. Identifying a threat to maritime cyber security is the first step to repelling it. How can this threat be recognised? A threat to maritime cyber security can be perceived from an aggressor's intended or actual action. It has been argued that,

...the central element of the threat is action or the potential for action. It may be a threat of death, physical harm, political harm or legal or an unspecified/unarticulated harmful action.⁴¹³

This means that an aggressor's capability to cause harm or damage to infrastructure, which ensure maritime cyber security is a significant factor for determining threat. Also, the overt action of the aggressor can be implied as a demonstration of intent to cause harm or damage.

A survey of the threat analysis on maritime cyber security shows that the nature of cyber-attacks includes malware, phishing, spear phishing, application attack, brute force, denial of service, a network of protocol attack, a man in the middle, theft of credentials and exploitation of a known vulnerability.⁴¹⁴ The forms of cyber-attacks

⁴¹¹ IHS Markit *Maritime Cyber Security Results* (2018) 3.

⁴¹² *Ibid.*

⁴¹³ Benard *Port security - Threat and Vulnerability, Case: Takoradi Port* (doctoral thesis Laurea University of Applied Sciences, Leppävaara, 2015) 20

⁴¹⁴ IHS Markit *Maritime Cyber Security Results*: This third annual maritime cyber security survey was conducted by IHS Fairplay in association with BIMCO (Baltic and International Maritime Council) to analyse cyber threats facing the shipping industry.

that can affect the maritime industry include manipulating submarines into collision, maritime terrorism, ballistic missiles launched from ships, all of which can be executed through cyber means maliciously or ignorantly.⁴¹⁵ These maritime attacks can cause various degrees of damage to property, injuries or loss of life. It is submitted that MCAs can qualify as unlawful use of force when it has violent consequences.

Based on tactical cyber intelligence reporting, the maritime supply chain is regularly targeted through emails to unsuspecting employees by using seemingly legitimate business subjects. When such emails are opened, malware can be delivered into a vessel, port, or oil rig's network or operational technology. As aptly stated by the report:

Fraudulent emails designed to make recipients hand over sensitive information, extort money or trigger malware installation on shore-based or vessel IT networks remains one of the biggest day-to-day cyber threats facing the maritime industry. These threats often carry a financial liability to one or all those involved in the maritime transportation supply chain.⁴¹⁶

This form of attack can lead to enormous economic loss. Economic losses can directly or indirectly threaten the smooth governance of the State.

3.3.4. Evolving Legal Norms on the Use of Force

Assessing the legality of a maritime cyber-attack and its qualification as use of force in international law requires careful consideration of articles 2(4) and 51 of the UN Charter and contextual analysis. Hostile acts that violate the territorial integrity or contravene the purposes of the UN Charter amounts to illegal use of force.⁴¹⁷ The purposes of the UN are:

to keep peace throughout the world; to develop friendly relations among nations; to help nations work together to improve the lives of poor people, to conquer hunger, disease and illiteracy, and to encourage respect for each other's rights and freedoms; to be a centre for harmonising the actions of nations to achieve these goals.⁴¹⁸

⁴¹⁵ Bateman "Regional Maritime Security: Threats and Risk Assessments" 2010 1 *University of Wollongong Research Online*, 10 14.

⁴¹⁶ Drayad Global July 20,2020 <https://channel16.dryadglobal.com/maritime-cyber-security-threats-jul-2020-week-two> accessed 2020-12-16).

⁴¹⁷ Article 51 UN Charter; Wood "International Law and the Use of Force: What Happens in Practice?" 2013 53 *Indian Journal of International Law* 345 352.

⁴¹⁸ UN "History of the UN" (undated) <https://www.un.org/un70/en/content/history/index.html> (accessed 2020-02-21).

The use of force may be illegal if carried out with no justification or legal if carried out in self-defence. Can MCAs be categorised as one of such illegal hostile acts? Comparative analysis of scenarios of when kinetic and cyber forces amount to the use of force can create a more pragmatic understanding of the issues at stake. For instance, If the stock market is disrupted temporarily by a cyber-attack in the form of data manipulation or a detonated explosive device that brought down part of the country's stock exchange building, the use of force in both contexts will be assessed be different. The former will less likely be referred to as a use of force even though it caused the same effect of a temporary shutdown as the latter, which would easily be referred to as a use of force due to its physical damage. This shows the double standard in the legal assessment of cyber interference and the use of kinetic force to label them as the use of force or armed attack. Despite achieving the same disruptive consequences in the stock market, the absence of physical destruction by cyber interference readily disqualifies it from being classified as a use of force or armed attack.

Also, suppose the communication channel of a naval vessel is jammed due to a cyber-attack. In that case, it may not be labelled as the use of force but probably referred to as a threat of force because it may be interpreted as a preamble to an imminent attack. On the other hand, if the same breach in communication occurs because of destruction to their submarine communication cables by another state in control of the exclusive economic zone,⁴¹⁹ it may be more quickly labelled as a use of force. Although UNCLOS provides for the requirement to respect the rights and duties of coastal states,⁴²⁰ this provision has been criticised for its ambiguity. It has been argued that this provision does not limit warships with cyber capabilities, which may operate under the right of innocent passage in the exclusive economic zone of a coastal State.⁴²¹ Contrarily, some states argue that despite the provision for innocent passage, notification or consent must be obtained from the coastal state⁴²² because this right is impliedly accompanied by obligations that ensure that the coastal State's security interest is always protected.

⁴¹⁹ Article 57 of UNCLOS : This refers to an area beyond the territorial sea within 200 nautical miles seaward of the respective State's baselines.

⁴²⁰ Article 58(3) of UNCLOS.

⁴²¹ Schmidt *Tallinn Manual 2.0240*.

⁴²² Article 6-7 of the Law of the Territorial Sea and the Contiguous Zone of the Republic of China 1992; article 9(2) Act on the Marine Areas of the Islamic Republic of Iran in Persian Gulf and the Oman Sea of 1993.

Scholars have proposed several approaches in determining when a maritime cyber-attack constitutes the use of force. First is the instrument-based approach, which focuses on the mode or type of cyber weaponry used to carry out the attack.⁴²³ The features of cyber weaponry need to be analysed compared to the kinetic force of military weapons with a specific focus on the effect and extent of the damage. As discussed previously, this comparison can be adjudged as imbalanced due to the unique nature of cyber weaponry. The sophistication of certain malware or computer viruses may not be adequately appreciated by non-cyber experts carrying out comparative analysis only with guidance from their knowledge of sophisticated kinetic weapons. It is submitted that a cybersecurity analyst can, more accurately, perceive the hostile and coercive nature of an MCA.

Secondly, the target-based approach can help to determine whether an MCA is a use of force.⁴²⁴ This approach focuses on the importance of the infrastructure hit by a cyber-attack in addition to the potentially catastrophic consequence based on its significance to a State. This means that when a cyber-attack targets a critical infrastructure of a State or a flag ship, it can be referred to as the use of force. The critical infrastructure of a ship includes navigation and communication systems which are very important to the safety of a ship and those on board. It is submitted that when an MCA threatens these critical infrastructures, it amounts to a threat or use of force.

Thirdly, the consequence approach focuses on whether the gravity of the MCA meets the threshold of armed attack or use of force with specific attention to the imminence of 'cyber' violence. This implies that when an MCA leads to the threat of or actual loss of lives or enormous damage to property, it amounts to an illegal use of force. These approaches are a slight modification of the requirements under *jus ad bellum*⁴²⁵ due to the uniqueness of the issue of cyber security when analysed under the framework of international law.

⁴²³ Hollis "Why States Need an International Law for Information Operations" 2007 11 *Lewis and Clarke Law Review* 1023 1041.

⁴²⁴ Sharp *Cyberspace and the Use of Force* (1999) 129-130; Graham 2010 *National Security Law and Policy* 87 91.

⁴²⁵ Nguyen "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare" 2013 101(4) *California Law Review* 1079 1084.

Although the term 'use of force' seems to be broad in scope,⁴²⁶ some scholars have a contrary opinion.⁴²⁷ The broad scope suggests that the use of force encompasses incidents that qualify as armed attack or fall below its threshold, acts of aggression or below its threshold, incidents that qualify as use of force or others that merely infringe on States' sovereignty. Gordon, while referring to the *Corfu Channel* case, states that:

The idea that force is permissible so long as it is not directed against the integrity of the invaded state's territorial boundaries or its independence was first advanced during oral argument...⁴²⁸

Based on this assertion, it is submitted that MCA amounts to a violation of the integrity of a State's territorial seas when critical maritime infrastructures are threatened or destroyed.

The use of force is not as broad as it seems, but it requires the assessment of different incidents to determine when they amount to the use of force.⁴²⁹ Brownlie argues that there can be potentially lawful bases of use of force on the grounds of applying forcible responses to unlawful territorial invasions or instances of mere aggressive encounters.⁴³⁰ When this argument is assessed through the lens of customary practices of States over the years, evidence of the narrow scope of article 2(4) can be found based on two main issues. Firstly, incidents of small-scale forcible acts have been treated as illegal acts of violation of states' sovereignty, but not use of force.⁴³¹ The second issue concerns small-scale forcible acts, such as proportional countermeasures, though legal. However, they do not draw legitimacy from article 51 of the UN Charter as responses to armed attacks.

⁴²⁶ Special Committee on the Question of Defining Aggression, UN GAOR, 4th Session, 82nd meeting at 20 (Mexico), UN Doc. A/AC.134/SR.82 (June 7, 1991); 'by way of illustration, several statements made during the negotiations on the General Assembly's Definition of Aggression indicate that the notion of force is broader in scope than armed attack or aggression and that various minor incidents that do not qualify as aggression may nevertheless constitute a use of force'.

⁴²⁷ O'Connell "The Prohibition on the Use of Force" in *Research Handbook on International Conflict and Security Law* (2015) 89 102.

⁴²⁸ Gordon "Article 2(4) in Historical Context" 1985 10(2) *Yale Journal of International Law* 271 275; Statement of Sir Eric Beckett (*U.K. v. Alb.*), 1948 I.C.J. Pleadings (3 *Corfu Channel*) 295-96 (Public Sitting of Nov. 11-12, 1948).

⁴²⁹ *Ibid.*

⁴³⁰ Brownlie *International Law and the Use of Force by States* (1963) 373.

⁴³¹ For example, the *Corfu Channel's* case; SC Res. 138 (June 23, 1960); Letter Dated 15 June 1960 from the Representative of Argentina Addressed to the President of the Security Council, UN Doc. S/4336 (1960) complaining about the violation of Argentine's sovereignty through a covert operation by Israeli agents to kidnap a Nazi fugitive from Argentina without first seeking the approval from the host country.

According to Ruys,

small-scale incidents are not necessarily beyond the scope of Article 2(4) (again, no absolute *de minimis* threshold exists). The reaction of the victim state (for example, the flag state of a sunken ship) arguably provides a useful indicator of the political context. Hence, when such a state frames the incident by reference to Article 2(4), the indication is that the incident is part of a broader dispute between sovereign states.⁴³²

It is submitted that international law politics may cloud the legality or illegality of force or threat of force. States may react differently to labelling the act in question based on factors that align with their national interests or foreign policy. They include shared responsibility, consent, and intention to preserve international relations.⁴³³ States may exercise restraint due to shared responsibility of being partially at fault for provoking the ensuing situation. When there is a mutual liability for the use of force by both states, they are less likely to claim the illegal of use of force. For example, the 1982 explosion of a trans-Siberian pipeline was caused by computer malware intentionally fixed in Canadian software by the Central Intelligence Agency because they knew it would end up in the hands of the Soviet agents. The Russian State Security thought they had secretly obtained America's latest software technology. Consequently, the details about the explosion were not released publicly, and it was never formally attributed to the US.⁴³⁴

There are instances where a state which exercises sovereignty over its cyber infrastructures confidentially consents to cyber intrusion by another state in furtherance of a common interest.⁴³⁵ In addition, there could be an intention to prevent escalation of the issues arising from cyber interference to avoid endangering international relations between the affected States. This implies that determining the threat or use of force may depend on the existing friendly or unfriendly relations between states. States are more likely to refrain from labelling an act as a use of force to protect the existing cordial relationship. In contrast, unfriendly states are more likely to identify the threat or use of force without sentiments.⁴³⁶ This creates an ambiguity in determining state practice and *opinio juris* on the interpretation and

⁴³² Ruys 2014 *The American Journal of International Law* 207.

⁴³³ *Ibid* at 169.

⁴³⁴ Safire "The Farewell Dossier" (2004-02-02) *The New York Times* 1.

⁴³⁵ *Ibid*.

⁴³⁶ Corten *The Law Against War* (2010) 91.

application of the UN provision on the threat and use of force.⁴³⁷ Whereas some states would utterly declare an act as use of force, some others would say it is no use of force. Another group of states may refrain from commenting on the legality of the threat or use of force. Most of these choices depend on the existing friendly or unfriendly relations between the aggressor and victim states.

In the *Oil Platforms* case, Judge Simma argued that the use of force that falls below the armed attack threshold might be responded to with a similar form of necessary and proportional force.⁴³⁸ This view has been criticised as creating a high possibility of a full-scale conflict. It has been argued that forcible countermeasures to acts below the threshold of armed attack should be interpreted as different rights to apply force to defend and assert the rights that have been illicitly infringed upon.⁴³⁹

Some writers opine that the use of force in response to an invasion is outside the scope of the use of force but within the purview of the powers of law enforcement agencies.⁴⁴⁰ However, proposing that unlawful acts against a third State are not within reach of the prohibition on the use of force is incompatible with international customary law and objectionable when viewed from a policy perspective.⁴⁴¹ It will be more reasonable to assert that intentional threat or use of force on another State's territory, irrespective of the actual target, should be classified within the scope of article 2(4) of the UN Charter.⁴⁴² Consequently, it is submitted that cyber-attacks that fits into this pattern can amount to illegal use of force. If the cyber-attack threatens or undermines a State's security through its maritime zone or on the high sea, it could amount to a use of force. Also, if it is intended to threaten or trigger coercive

⁴³⁷ Ruys 2014 *The American Journal of International Law* 170.

⁴³⁸ *Oil Platforms (Iran v. U.S.)* 2003 ICJ Rep., at 324, par [12] (separate opinion Simma J.); Judge Simma points to a potential loophole in *Nicaragua*, where the court ruled out the possibility of forcible countermeasures by third states, though without expressly ruling out the permissibility of forcible countermeasures by the immediate victim of the use of force concerned.

⁴³⁹ Gill "The Forcible Protection, Affirmation and Exercise of Rights by States Under Contemporary International Law" 1992 23 *Netherlands Yearbook of International Law* 105 116; Gill cites "compelling policy considerations" for not relying on self-defence, since abroad interpretation of "armed attack" would, in his view, lead to the escalation of interstate conflicts.

⁴⁴⁰ Fleck "Rules of Engagement of Maritime Forces and the Limitation of the Use of Force Under the UN Charter", 1989 31 *German Yearbook of International Law* 165179-180; 2007 Institute of International Law resolution on self-defence which states that, 'In case of an attack of lesser intensity [than an "armed attack"] the target State may also take strictly necessary police measures to repel the attack.'

⁴⁴¹ Ruys 2014 *The American Journal of International Law* 159 197.

⁴⁴² *Ibid.*

measures against a State through its maritime zone and on the high sea, it could be labelled as use of force.

The Tallinn manual states that:

A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.⁴⁴³

This statement is based on the ICJ's ruling in the *Nicaragua* case.⁴⁴⁴ It suggests that despite the absence of the definition of threat or use of force, there are forms of force that do not qualify as use of force as provided for in article 2(4) of the UN Charter. These may include economic or political force, which may take the form of cyber operations to create a negative impact on a state's political climate. Following the rationale of the ICJ in the *Nicaragua* case, a government-funded cyber operation in the form of non-destructive economic or political force will not amount to the use of force.⁴⁴⁵ Hon. Harold Koh, in his remarks, summarises the factors that should be considered in determining whether cyber force amounts to use of force:

In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognising challenging issues of attribution in cyberspace), the target and location, effects, and intent, among other possible issues.⁴⁴⁶

His remarks are in line with Schmitt's list of factors that can be used to assess the qualification of cyber-attacks as use of force: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.⁴⁴⁷ This is not an exhaustive list of factors or possible issues that can be considered in determining whether cyber force amounted to the use of force. This incomprehensive list allows for reasonable flexibility through a case-by-case analysis of cyber incidents. The Tallinn Manual provides a more detailed list of factors that capture Koh's and Schmitt's views. This manual can guide States in their assessment of cases of use of force.

Rule 69(9)(a) of the Tallinn Manual proposes that when a cyber-attack results in physical harm to people and damages to property, it is severely sufficient to qualify

⁴⁴³ Rule 69 in Schmidt's *Tallinn Manual* (2017) 330.

⁴⁴⁴ *Nicaragua judgment*, par [195].

⁴⁴⁵ Schmidt *Tallinn Manual* 331.

⁴⁴⁶ Hon. Harold Koh "Remarks at the U.S. Cyber Command Inter-Agency Legal Conference" (18 September 2012), <https://2009-2017.state.gov/s//releases/remarks/197924.htm> accessed 2019-05-18).

⁴⁴⁷ Schmitt "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework" 1999 37(3) *Columbia Journal of International Law* 898-899.

as the use of force. When the consequence of the cyber-attack appears as a mere inconvenience, it will not amount to the use of force.⁴⁴⁸ For a State to determine a case of use of force, it needs to assess the extent, length of time and strength of an attack.⁴⁴⁹ This rule also acknowledges the relativity in the interpretation of severity when the target of the attack is critical to national interests such as naval security. This relativity exists because of varying national interests among States. The absence of a globally accepted definition of critical national interests allows for a flexible interpretation of the concept of the use of force when the severity of the attack is being assessed. It is submitted that the frequency of a cyber-attack can be considered as a contributing factor when assessing severity as a chief factor in determining the use of force.

Another factor that the Tallinn Manual proposes is that of immediacy. The drafters argue that a cyber-attack that produces an instant consequence is more likely to qualify as the use of force.⁴⁵⁰ This means that the likelihood of a cyber-attack being tagged as use of force diminishes as the duration for the manifestation of the consequence of the attack increases. This can be interpreted simultaneously with the factor of 'directness', which states that:

Cyber operations in which cause and effect are clearly linked are more likely to be characterised as uses of force than those in which they are highly attenuated.⁴⁵¹

Both factors of 'immediacy' and 'directness' can be criticised as lacking in precision and need to be cautiously applied. This is because the inability to detect the consequence of a cyber-attack quickly should not alter the reality that a use of force has occurred. States with sophisticated information technology are better positioned to detect a manifestation of the consequence of a cyber-attack quickly. Some types of complex cyber-attacks can be cloaked to avoid detection until maximum damage is caused. It is submitted that if the consequence of the attack manifests immediately, a clear case of use of force can be made. Nevertheless, suppose the State's security assessment concludes that the extent of the foreseeable consequence of the cyber-attack on its critical infrastructure can only be determined in the near future. In that case, a case of threat of force can be made.

⁴⁴⁸ Schmitt *Tallinn Manual 2.0* (2017) 334.

⁴⁴⁹ *Ibid.*

⁴⁵⁰ *Ibid.*

⁴⁵¹ *Ibid.*

Also, invasiveness, a factor that considers the extent of unauthorised intrusion into a State's computer network system, determines the use of force. As aptly stated by the Tallinn Manual,

the more secure a targeted cyber system, the greater the concern as to its penetration. For example, intrusion into a military system that has been accredited at Evaluation Assurance Level 7...is more invasive than merely exploiting vulnerabilities of an openly accessible...system...⁴⁵²

This implies that the highly secured cyber systems of a State can be categorised as critical cyber infrastructures. The sophistication of an aggressor's cyber capability can render a highly secured cyber system porous. The rationale behind this argument is that cyber espionage will not amount to the use of force since espionage is not prohibited in international law.⁴⁵³ When this is applied to MCAs, it can be argued that all forms of cyber espionage can quickly escalate to a full-blown attack since the extent of the destructive intent of the attacker cannot be readily ascertained. The invasiveness of a cyber-attack on critical maritime infrastructures can provide guidance in determining the use of force.⁴⁵⁴ The possibility of quickly identifying the consequence of the breach in cyber security allows for a more straightforward contextual assessment of the use of force. Subjective consequences of MCAs lead to a contentious assessment of the occurrence of the use of force.

The sophistication of cyber weaponry has evolved over the years to a level where they could potentially be treated as weapons of mass destruction. In order to qualify as a WMD, the cyber operation must act as a weapon, be capable of causing mass casualties within a single strike and should be conventionally recognised as a special type of weapon.⁴⁵⁵ Although this is unprecedented in the context of maritime cyber security, the unceasing increase in the sophistication of cyber-attacks can increase the likelihood of the occurrence of a destructive cyber-attack of that severe magnitude.⁴⁵⁶ Policymakers have been advised to establish proper legal regulations to deter highly destructive cyber-attacks by updating the list of WMD to include a

⁴⁵² *Ibid.* While referring to the Common Criteria for Information Technology Security Evaluation, International Standard ISO/IEC 15408, ver. 3.1 (July 2009), the *Tallinn Manual* stated this in Rule 69(9)(d).

⁴⁵³ Rule 32 of Schmidt's *Tallinn Manual 2.0*.

⁴⁵⁴ Rule 69(9)(e).

⁴⁵⁵ Mauroni *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy* (2016) 36.

⁴⁵⁶ Hatch "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits" 2018 11(1) *Journal of Strategic Security* 43 49.

particular class of cyber weapons.⁴⁵⁷ From the above analysis, it can be deduced that certain forms of cyber-attack do not amount to the use of force in the traditional sense, but under some circumstances, cyber-attack can amount to the use of force. Maritime cyber exploitation should, at the minimum, be seen as a threat of force if not use of force, since the threat of force does not require evidence of destruction.⁴⁵⁸ It is submitted that the threat of force emanating from maritime cyber exploitation can be perceived as preliminary stages of an armed attack which will justify anticipatory self-defence.

The UN Charter is the principal international instrument that prohibits the use of force in its article 2(4). The primary purpose of the provision of article 2(4) of the UN Charter is to prohibit an aggressor State from using force against another State. The provision has been interpreted from various perspectives by numerous scholars and the ICJ. However, the conspicuous issue arising from the debate is that the gravity threshold, which is used to qualify an armed attack necessitating the use of force in self-defence, may also be used to determine whether an act amounts to a use of force. On the one hand, scholars such as Corten and O'Connell have argued in support of the view on *de minimis* threshold by citing some evidence. They assert that there were many instances when aggressive actions by states were lawfully executed without the prerequisite for a legal justification to defend against an armed attack as provided for in article 51 of the UN Charter or the need to be labelled as use of force. Ruys proposes a contrary view that adducing that less grave aggressive acts should not be labelled as unlawful use of force in line with article 2(4) of the UN Charter is conceptual confusion.

Ruys' argument portrays the customary international law practice on the subject because any threat or actual invasions which exhibit aggressive purposes are viewed mainly by States as falling within the scope of the use of force. The exception is seen when attacking States attempt to circumvent international law prohibition on the use of force by attempting to underrate their aggressive actions.⁴⁵⁹ This rationale

⁴⁵⁷ *Ibid.*

⁴⁵⁸ Wortham "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" 2012 64(3) *Federal Communications Law Journal* 643 643.

⁴⁵⁹ Corten *The Law Against War* (2010) 247-248: "As a *jus cogens* rule, the prohibition of the use of force cannot be circumvented,...It may well be, besides, that some coercive acts may be performed by one State outside of its territory, without it being a question of invoking article

is in line with the ICJ's advisory opinion in the *Nuclear Weapons*' Case where it ruled that:

Whether this is a "threat" contrary to Article 2, paragraph 4, depends upon whether the particular use of force envisaged would be directed against the territorial integrity or political independence of a State, or against the Purposes of the United Nations or whether, in the event that it were intended as a means of defence, it would necessarily violate the principles of necessity and proportionality. In any of these circumstances the use of force, and the threat to use it, would be unlawful under the law of the Charter.⁴⁶⁰

The threat of MCA or an actual MCA can qualify as use of force in this regard, especially if the incident arises from a dispute between States.⁴⁶¹

Determining the use of force in the context of a confrontation between an aircraft and a ship can be based on the perception of a mere harassment or actual use of force. Heinegg asserts that:

A use of force against foreign warships or military aircraft in the sea areas and the above airspace beyond the outer limit of the territorial sea will most likely qualify as a use of force and bring an international armed conflict into existence.⁴⁶²

Applying this criterion for determining non-traditional use of force at sea can appear to be complicated. For instance, MCAs may entail the use of non-traditional, but aggressive cyber weaponry which can qualify as use of force.⁴⁶³ China and the U.S. have opposing views on the right to conduct military activities in the EEZ. While China holds the view that coastal States have the right to regulate not only economic activities, but also foreign military activities,⁴⁶⁴ the U.S. disagrees. These military activities include conducting surveillance and marine data collection in the EEZ of foreign states.

On February 21, 2022, it was reported that a Royal Australian Air Force P-8 Poseidon was illuminated by a laser from a Chinese People's Liberation Army Navy ship while flying over Australia's northern Economic Exclusion Zone. China denied

2(4),...In each individual case then, one should question the threshold above which one moves from a simple coercive operation to a real use of force in international relations...".

⁴⁶⁰ *Nuclear Weapons* par [48].

⁴⁶¹ Ruys 2014 *The American Journal of International Law* 159 209.

⁴⁶² Heinegg "The difficulties of conflict classification at sea: Distinguishing incidents at sea from hostilities" 2016 98 (2) *International Review of the Red Cross*, 449–464, 459.

⁴⁶³ *Ibid.*

⁴⁶⁴ Yang "The Freedom of Navigation in the South China Sea: An Ideal or a Reality?" 2012 3 *Beijing Law Review* 137, 140–41.

this allegation.⁴⁶⁵ This is a maritime incident that threatens the safety of ship and aircraft with the potential of escalation. Australia has launched an investigation into this incident. Though this incident has not been described by Australia as a threat to national security, it is being taken seriously with a demand from the Chinese government to provide an explanation for their action.⁴⁶⁶

3.4. Conclusion

Based on the discussion in this chapter, the terminologies used interchangeably by scholars to describe incidents in maritime cyber security have their own meanings, although they are interrelated. Using the appropriate terminology to describe a cyber incident clarifies the principles of international law that should apply to that circumstance, especially on the option of self-defence available to the victim. It has been shown that a maritime cyber-attack is the most appropriate terminology to describe a breach of maritime cyber security, which amounts to the use of force. This was deduced from the chronological analysis that: all maritime cyber activities can be referred to as maritime cyber operations; a cyber operation that invades or intrudes another maritime cyberspace without consent is maritime cyber interference; maritime cyber interference that causes damage with its unique form of cyberspace-violence or hostility is a form of force, and this use of cyber force can be described as a maritime cyber-attack. The unlawfulness of MCAs, which amounts to force, is based on the international law prohibition on the use of force except when it is a justifiable act in self-defence.

The normative orientation for the interpretation of the use of force has evolved. As opposed to a restrictive approach, several factors play their roles in concluding that the violation of article 2(4) prohibition on the use of force has occurred in the context of maritime cyber security. The frequency of a cyber-attack must be considered when assessing severity as a chief factor in determining whether an MCA amounts to the use of force. It enables proper assessment of the scope and duration of the attack. It contributes to the determination of the gravity of the attack. Applying the factor of 'immediacy' or directness of the attack⁴⁶⁷ in determining whether MCA

⁴⁶⁵ [Dzirhan Mahadzir https://news.usni.org/2022/02/21/australian-leaders-call-for-investigation-into-chinese-laser-harassment-of-surveillance-aircraft-pla-denies-wrongdoing](https://news.usni.org/2022/02/21/australian-leaders-call-for-investigation-into-chinese-laser-harassment-of-surveillance-aircraft-pla-denies-wrongdoing) (accessed 24-05-2022).

⁴⁶⁶ *Ibid.*

⁴⁶⁷ Schmitt *Tallinn Manual 2.0* (2017) 334.

amounts to the use of force cannot provide an accurate assessment in all instances except where the effect of the MCA can be known instantly. The inability to quickly detect the consequence of a cyber-attack should not alter or deny the reality that a use of force has occurred. Suppose the State's security assessment concludes that the extent of the foreseeable consequence of the cyber-attack on its critical infrastructure can only be determined soon. In that case, a case of threat of force can be made.

A key issue is that the invasiveness of a cyber-attack on critical maritime infrastructures can guide States in determining whether the use of force has occurred. This invasiveness can be likened to espionage. Since scholars have established that cyber espionage can quickly escalate to a full-blown attack, it is correct to assert that the extent of the destructive intent of the attacker cannot be readily ascertained. When a cyber-attack is attributed to a State, the victim State is more inclined to declare that the use of force has occurred. Following the application of these factors, the impact of cyber force can be recognised in the context of maritime security as a real type of force. This is because an MCA can cause grave danger or enormous damage with virtual strength, sophistication, and speed. The potential devastation that is threatened by the launch of an MCA is too significant to be ignored. The scale and gravity of force involved in an MCA must be measured with cognisance of cyber weaponry's unique and intangible nature.

Some types of MCA may be seen as a deliberate projection of lethal force into a State's territory and will fall within the scope of article 2(4). Comparing the scale and effect of an MCA to that resulting from the use of tangible force is relevant in determining whether it meets the threshold of armed attack necessitating the use of force in self-defence. It has been established that MCAs can be described as the use of force where critical infrastructures in the marine environment are threatened using sophisticated cyber weaponry. Where MCA falls below the threshold of armed attack and is categorised as use of force, the victim State does not lose its right to self-defence, but it is restricted from using armed force as an option while acting in self-defence.

CHAPTER 4: MARITIME CYBER-ATTACK AS AN ARMED ATTACK

4.1. Introduction

The significance of discussing armed attacks in this chapter stems from the international law exception to the prohibition on the use of force. The concept of MCAs as the use of force has been dealt with in the preceding chapter focusing on article 2(4) of the UN Charter, which prohibits the use of force. Article 51 of the UN Charter will be the main legal provision to be considered in this discussion because it provides that the occurrence of an armed attack permits the lawful use of force in self-defence. This provision justifies a State to use force in repelling an incoming forceful attack and/or reacting to a completed attack in self-defence.⁴⁶⁸ This permissive use of force is a legal right that arises when a State perceives being threatened with force.⁴⁶⁹ The provision of article 51 of the UN Charter guides States concerning which acts are acceptable under certain conditions, especially when faced with MCA that amounts to an armed attack.

Since there is no treaty law definition of an armed attack⁴⁷⁰, describing an MCA as an armed attack requires understanding the requirements for qualifying an incident as an armed attack. The ICJ described these requirements to involve the use of force capable of causing grave destructive consequences like traditional military weapons would do.⁴⁷¹ Some of the legal issues that arise from the description of armed attack

⁴⁶⁸ *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, I.C.J. Reports 2005, 222, par[146] "...while Uganda claimed to have acted in self-defence, it did not ever claim that it had been subjected to an armed attack by the armed forces of the DRC...The Court has found...that there is no satisfactory proof of the involvement in these attacks, direct or indirect, of the Government of the DRC"; Hurd "Permissive Law on the International Use of Force" 2015 109 *Proceedings of the Annual Meeting: Adapting to a Rapidly Changing World* 63 65: "The legal right to use force begins with the internal perception by a state of being under threat and of the need to respond to that threat with force."

⁴⁶⁹ *Ibid.*

⁴⁷⁰ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits, Judgment. I.C.J. Reports 1986, 94, par [176] "...a definition of the "armed attack" which, if found to exist, authorizes the exercise of the "inherent right" of self-defence, is not provided in the Charter, and is not part of treaty law".

⁴⁷¹ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* I.C.J. Reports 1986, 103, par [195] [There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, 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". This description, contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law]; Juma

include: What conditions should be satisfied for an incident to amount to an armed attack? Does all use of force qualify as an armed attack? Is it only kinetic attacks that can qualify as the use of force? What are the principles regulating a State's reaction to an imminent armed attack? All these issues will be discussed in this chapter except the last one. So, for this discussion, a "maritime cyber armed attack" will be viewed as a grave attack on the critical cyber infrastructure within the maritime jurisdiction of a State. This chapter seeks to determine the conditions required to qualify an incident as an armed attack while focusing on when MCAs can amount to an armed attack.

Identifying the attacker responsible for an MCA and the victim of an armed attack is relevant in invoking the provision of article 51 of the UN Charter. This requires considering whether a State can be a victim of a "maritime cyber armed attack" or react with cyber force and/or other forceful means in self-defence to an imminent armed attack. An analysis of the ICJ's reasoning and scholarly debates on the provision of article 51 of the United Nations Charter on armed attack will pave the way for a corresponding description of the concept of "maritime cyber armed attack". It will be argued that when illegal use of cyber force against critical marine infrastructures of a State causes grave destruction of tangible or intangible property and/or loss of life, a "maritime cyber armed attack" can be deemed to have occurred. How to make the assessment will be discussed with a focus on critical factors such as the vulnerability of the victim's maritime cyber security, a probable consequence of the MCA, and the cyber capability of the attacker.

4.2. The Right of Self-defence

The sovereignty of a State implies a right to act in self-defence and a duty to avoid violating another States' sovereignty.⁴⁷² The right to self-defence refers to the legitimate right of states to use force in the face of an armed attack.⁴⁷³ It is an exception to the prohibition on the use of force as provided for in article 2(4) of the UN Charter. It is one of the ways a State can react when faced with an imminent

and Strydom "Maintaining International Peace and Security: The Enforcement of International Law" in *International Law* (2016) 226.

⁴⁷² Shaw *International Law* 9ed 993.

⁴⁷³ Article 51 of the UN Charter; Koh's Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (18 September 2012), <https://2009-2017.state.gov/s//releases/remarks/197924.htm> (accessed 2019-07-02).

threat or an attack.⁴⁷⁴ It is the inherent right of States to repel an imminent threat of attack or an actual attack. Webster aptly explains that⁴⁷⁵ “a just right of self-defence always attaches to nations as well as to individuals and is equally necessary for the preservation of both.”⁴⁷⁶

This assertion emphasises the significance of article 51 of the 1945 UN Charter on self-defence as an inherent right of States and the right of individuals.⁴⁷⁷ It is a right that comes with the birth of the State, and it is crucial to the continued existence of that State. According to Weightman,

Self-defence is that residuum of the "right of nature", which is left intact after the larger right has been restricted by law.⁴⁷⁸

It is submitted that any threat to the criteria for Statehood, as listed in the Montevideo Convention⁴⁷⁹ will necessitate the exercise of the right of self-defence. For instance, the right to self-defence may be exercised, with proportional use of force, when there is a threat or an unprovoked attack that causes a reasonable fear of or actual grave danger to lives and property in a State.⁴⁸⁰

The intention of a State acting in self-defence should be to protect its people and critical infrastructures from suffering grievous injury or extensive damage, respectively. Other purposes of acting in self-defence include preventing an attacker from succeeding in his mission, protecting the loss of lives of citizens, and preventing the destruction of critical infrastructures.⁴⁸¹ In order to prevent an attacker from succeeding, the State must perceive the imminent threat and thwart it. This can be

⁴⁷⁴ According to Shaw *International Law* 990-993, the three categories of compulsion open to states under international law are retorsion (adoption by one state of an unfriendly and harmful, but legal act, as a method of retaliation against the injurious legal activities of another state); reprisal (adopting illegal acts by one state in retaliation for the commission of an earlier illegal act by another state) and self-defence.

⁴⁷⁵ The US Secretary of State in his diplomatic correspondence with his British counterpart during the Caroline incident regarding the limitation on self-defence; letter from Daniel Webster to Lord Ashburton (27 July 1842) in *Diplomatic and Official Papers of Daniel Webster while Secretary of State 1848* 104.

⁴⁷⁶ *Ibid.*

⁴⁷⁷ Weightman “Self-Defence in International Law” 1951 37(8) *Virginia Law Review* 1095, 1109.

⁴⁷⁸ *Ibid* at 1105.

⁴⁷⁹ Article 1 of the Montevideo Convention, 1933 provides that: the State as a person of international law should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other States.

⁴⁸⁰ The *Oil Platforms (Iran v. US)*, ICJ Reports, 2003, 161, 189 and 190.

⁴⁸¹ Shah “Self-defence in International Law” in *Self-defence in Islamic and International Law* (2008) 164.

done through anticipatory self-defence and in compliance with the relevant legal requirements in international law.⁴⁸²

Scholars have debated the principle of self-defence in terms of the strictness of the ICJ's interpretation of article 51. While some scholars argue that article 51, if strictly read, does not provide for ASD, others argue that ASD is a subset of the inherent right of States to defend themselves. According to Kelson,

It is of importance to note that Article 51 does not use the term aggression but the much narrower concept of armed attack, which means that a merely imminent attack or act of aggression which has not the character of an attack involving the use of armed force does not justify resort to force as an exercise of the right established by Article 51.⁴⁸³

Henkin supports this view by stating that:

The fair reading of Article 51 permits unilateral use of force only in a very narrow and clear circumstance, in self-defence if an armed attack occurs.⁴⁸⁴

Brownlie reiterates this by affirming that:

the view that Article 51 does not permit anticipatory action is correct and that the arguments to the contrary are either unconvincing or based on inconclusive pieces of evidence.⁴⁸⁵

Other scholars have criticised these strict interpretations of self-defence. In 1952 during his Hague lectures, Sir Humphrey Waldock stated that:

If an armed attack is imminent within the strict doctrine of the Caroline, then it would seem to bring the case within Article 51. To read Article 51 otherwise is to protect the attacker's right to the first stroke. To cut down the customary right of self-defence beyond even the Caroline doctrine does not make sense in times when the speed and power of weapons of attack has enormously increased.⁴⁸⁶

It is reasonable to agree with Sir Humphrey's opinion. It is judicious to argue that the right to defend oneself must not be sacrificed at the altar of strict interpretations which do not project the fundamental objectives of the principle of self-defence. Sir Waldock's opinion is reasonable because States must have the right to stop an incoming attack if it is detectable before it materialises or causes death or destruction. It is correct to stretch the interpretation of by article 51 of the UN charter to accommodate this right because,

⁴⁸² *Ibid.*

⁴⁸³ Kelsen *The Law of The United Nations* (1950) 797.

⁴⁸⁴ Henkin *How Nations Behave* 2ed (1979) 141.

⁴⁸⁵ Brownlie *International Law and The Use of Force by States* (1963) 278.

⁴⁸⁶ Waldock "The Regulation of the Use of Force by Individual States in International Law" 1952 81 *Academie De Droit International Recueil De Cours* 451 498.

[I]t is not necessarily unlawful in all circumstances, the matter depending on the facts of the situation including, in particular, the seriousness of the threat and the degree to which pre-emptive action is really necessary and is the only way of avoiding that serious threat.⁴⁸⁷

Scholars can settle their debates despite these opposing views by relying upon the ICJ rulings on these issues. The unlawful use of force must originate externally, be directed towards a State, and meet the armed attack threshold before self-defence can be invoked.⁴⁸⁸ This means that unlawful intrusions and other forms of international law violations that fall below the threshold of armed attack cannot permit the use of force in self-defence.

Self-defence can be understood from the treaty perspective and customary international law. The treaty view refers to article 51 of the UN Charter provision for States to act in self-defence in the face of armed attack. The *Caroline case* provides credence for customary law interpretation of self-defence. The brief facts are that British troops invaded the U.S. territory and destroyed the steamboat *Caroline* in 1837.⁴⁸⁹ This incident led to the formulation of conditions to be fulfilled as justification of the British violation of U.S. territorial sovereignty, which still forms the basis for the customary principles governing the issue of self-defence in international law. In this case, Daniel Webster made a resounding statement that provides the conditions that permit anticipatory self-defence. He stated that:

while it is admitted that exceptions growing out of the great law of self-defence do exist, those exceptions should be confined to cases in which the 'necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'⁴⁹⁰

However, in maritime cyberspace, it is necessary to re-evaluate this assertion to accommodate offensive cyber intrusion with unique destructive capability as justification for invoking anticipatory self-defence. This will entail assessing whether cyber espionage and other various forms of unauthorised cyber-attacks, stealing of data and impairment of computers at sea should be treated as armed attacks necessitating self-defence. In analysing this issue, the existing conditions for

⁴⁸⁷ Jennings and Watts *Oppenheim's International Law* 9ed (1992) 421.

⁴⁸⁸ *Nicaragua* 1986 par [195]; Shah "Self-defence in International Law" in *Self-defence in Islamic and International Law* (2008) 164.

⁴⁸⁹ *Caroline Case of 1837*; facts taken from D.J. Harris, *Cases and Materials on International Law*, 5th Edition, 1998.

⁴⁹⁰ Miller Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, British-American Diplomacy, *The Caroline Case*, available at https://avalon.law.yale.edu/19th_century/br-1842d.asp (accessed 2019-08-04).

triggering anticipatory self-defence need to be adapted to reflect the unique vulnerability in cyberspace and the marine environment.

As stated in article 51 of the UN Charter, the treaty conditions provide States with the option of self-defence against unlawful armed attack.⁴⁹¹ The non-treaty conditions derived from customary international law include the requirement of imminence, necessity and proportionality when invoking self-defence.⁴⁹² These requirements need to be satisfied for an act of self-defence to be legitimate, especially in the context of maritime cyber security.

4.3. Determining the Occurrence of an Armed Attack

As stated by the ICJ in the Nicaragua case, the occurrence of an armed attack is a precondition for a victim-State to lawfully set aside the prohibition on the use of force by article 2(4) for the purpose of self-defence.⁴⁹³ What are the elements of an armed attack? In the absence of a codified definition of an armed attack, its definition can be deduced, in the absence of other sources, from customary international law.⁴⁹⁴ The court found that reliance on customary international law is necessary to explain the provision of article 51, which says:

Nothing contained 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.⁴⁹⁵

In interpreting this provision, the ICJ ruled that:

Article 51 of the Charter is only meaningful on the basis that there is a "natural" or "inherent" right of self-defence, and it is hard to see how this can be other than of a customary nature, even if its present content has been confirmed and influenced by the Charter. Moreover, the Charter, having itself recognised the existence of this right, does not go on to regulate directly all aspects of its content.⁴⁹⁶

This justifies the scholarly debates stemming from the ICJ's interpretation of the concept of armed attack as a precondition for self-defence under article 51 of the UN

⁴⁹¹ Article 51 of the UN Charter.

⁴⁹² The *Oil Platforms Case* (2003) par [61-64]; *Nicaragua case* (1986) 14.

⁴⁹³ *Ibid.*

⁴⁹⁴ *Nicaragua case* [1986] I.C.J. Rep. 3, 94, par [176]: the case was about the United States' claim that its actions in Honduras were made in collective self-defence of Honduras while Nicaragua claimed it was an armed attack. In making its decision, the ICJ stated that not all uses of force amount to an armed attack, and not all interventions by one state into the affairs of another rise to the level of a use of force.

⁴⁹⁵ Article 51 UN Charter.

⁴⁹⁶ *Ibid.*

Charter. Scholars have described an armed attack focusing on ICJ's interpretation of armed attack and incidental guiding principles.⁴⁹⁷ When viewed literally, article 51 of the UN Charter provides a simplified picture of armed attack as the incident that permits States to use force⁴⁹⁸ without providing guidance on when an action qualifies as an armed attack.⁴⁹⁹ The issues that must be considered before reaching the verdict of armed attack will be discussed below.

4.3.1. Assessment of the Attacker's Act

A more critical view of article 51 of the UN Charter brings to light the importance of assessing the attacker's act before looking at what the victim is permitted, by law, to do. Considering the impact an act must have, it seems crucial to accurately classify that attack as an armed attack. When an act causes severe breach of the peace or occurs in the form of a sophisticated and coordinated forceful invasion, it is deemed to qualify as an armed attack if attributable to a State.⁵⁰⁰ The importance of attributing the act to a State can be deduced from the joint reading of articles 2(4) and 51 of the UN Charter. The provision of article 2(4) directly points to States as the parties in the issue of prohibition of the use of force. Article 51 can be seen as a continuation of this issue because it permits States to use force when acting in self-defence without expressly stating whether the attacking party must be a State.⁵⁰¹ It expressly states that the target of an armed attack must be a State, but it is silent on whether it is only a State who can perpetrate an armed attack.

⁴⁹⁷ Article 51 of the UN Charter states 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 the measures necessary to maintain international peace and security." This provision has been interpreted by the ICJ in some cases. The court's interpretation has sparked debates among scholars who have argued from various perspectives.

⁴⁹⁸ Jensen 2002 *Stanford Journal of International Law* 207, 219.

⁴⁹⁹ Schmitt "Attack" as a Term of Art in International Law: The Cyber Operations Context' 2012 4th International Conference on Cyber Conflict Czosseck, Ottis, Ziolkowski (eds) 2012, Tallinn 286: *an "armed attack" is an action that gives States the right to a response rising to the level of a "use of force," as that term is understood in the jus ad bellum.*

⁵⁰⁰ Brownlie "International Law and the Activities of Armed Bands" 1958 7(4) *International and Comparative Law Quarterly* 712 731; *Nicaragua case* 1986 104, par [195].

⁵⁰¹ In the *Oil Platform's case*, the ICJ ruled that: "...in order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the United States has to show that attacks had been made upon it for which Iran was responsible; and that those attacks were of such a nature as to be qualified as "armed attacks" within the meaning of that expression in article 51 of the United Nations Charter, and as understood in customary law on the use of force".

Inferring that article 51 implies that the attack must only be imputed to a State to qualify as an armed attack is not accurate even though the case before the ICJ at that time was between two States. This is because article 51 focuses on the gravity of the attack felt by a State and not on the force used by the attacking party, as seen in article 2(4) of the UN Charter. This view pushes the frontier of the discussion beyond the ICJ ruling in the Nicaragua case, which stated that only States could carry out armed attacks directly and indirectly through non-State actors.⁵⁰² The possibility of the State suffering an armed attack from a non-State actor exists. Notably, the ICJ did not answer whether a victim-State can use force to defend against a large-scale attack directly launched by a non-State actor.⁵⁰³ The ICJ has always struggled to clearly address the complex issues regarding the internationally unlawful acts of non-state actors.⁵⁰⁴ Green argues that:

...the Court has purported to develop international law in a manner that accommodates the realities of non-state actor influence, ... it has done so haphazardly and arbitrarily. The Court has failed to develop a coherent conceptual framework for its approach to non-state actors and has demonstrated a lack of appreciation for the implications of its conclusions. Consequently, the Court's jurisprudence has produced a fragmentation *ratione personae* of international law.⁵⁰⁵

It is submitted that it can be implied that despite the ambiguity about the realities of non-State actors, they are capable of committing armed attacks.⁵⁰⁶ Although the law applicable may be different where the actions of the non-State actors are not attributable to a State, it does not change the fact that individuals can mastermind armed attacks, more especially in cyberspace against countries and privately owned infrastructures.⁵⁰⁷ So, when a State suffers an armed attack, irrespective of whether it is from a non-State actor or State actor, it can act in self-defence in line with the provisions of article 51 of the UN Charter. While States like the US support this view

⁵⁰² Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Merits, Judgment, 1986 ICJ 14, 103 par [195].

⁵⁰³ Armed Activities on the Territory of the Congo par [147].

⁵⁰⁴ Reparations [1949] ICJ Rep 174; Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion) [1996] ICJ Rep 66 ('WHO Nuclear Weapons'); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136 ('Israeli Wall') and Western Sahara (Advisory Opinion) [1975] ICJ Rep 12 ('Western Sahara').

⁵⁰⁵ Green "Fragmentation in Two Dimensions: The ICJ's Flawed Approach to Non-State Actors and International Legal Personality" 2008 9 *Melbourne Journal of International Law* 47 49.

⁵⁰⁶ Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ Reports 136, 139.

⁵⁰⁷ Roberts "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors" 2014 41 *Northern Kentucky Law Review* 535 536.

to use force against non-State actors lawfully in self-defence, France had reservations on this view especially in the context where the attack is not attributable to a State.⁵⁰⁸

4.3.2. The Gravity Threshold of the Attack

Determining the gravity threshold of an attack requires the application of the scale and effect principle, which originated from the *Nicaragua* case. The principle requires that the gravity of force from the act in question must be comparable to that of an attack by the armed forces of a State or State-sponsored armed group. The ICJ identified ‘the most grave forms of the use of force’ as ‘constituting armed attack’.⁵⁰⁹ Also, the victim-State has the obligation to declare that it has suffered an armed attack⁵¹⁰ or that the armed attack is imminent. The occurrence of an armed attack is judged from the perspective of the victim-State.⁵¹¹ The assessment of the attacking State on whether their act amounts to an armed attack is immaterial to determining that an armed attack has occurred.⁵¹²

Constantinou has provided a detailed description of armed attack as:

an act or the beginning of a series of acts of armed force of considerable magnitude and intensity which have as their consequence the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority...territory...and use of force which is aimed at a State’s main industrial and economic resources and which results in the substantial impairment of its economy.⁵¹³

This view depicts armed attack as a grave form of use of force such as launching missiles against a State, sending armed forces into another State, mass killing of citizens of another State. The phrase “an act or the beginning of a series of acts of an armed force of considerable magnitude and intensity” can be interpreted as encompassing an actual grievous attack as well as a threat of such an attack or less grave form of force. Suppose that ‘act’ is construed as a kinetic attack or an intangible force, or an imminent threat that precedes an actual attack. In that case,

⁵⁰⁸ Gray *International Law and the Use of Force* (2018) 237-239.

⁵⁰⁹ *Nicaragua case* 1986 101 par [191].

⁵¹⁰ *Nicaragua case* para 104 par [195]: “It is also clear that it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked...”.

⁵¹¹ *Nicaragua case* 1986 104 par [195].

⁵¹² *Ibid.*

⁵¹³ Constantinou *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (2000) 63-64.

that will be a true reflection of the position of customary international law on the State's right to self-defence. The consequence of the partial or complete attack must be extensive damage to vital infrastructures that ensures a State's sustainable existence, such as its territory, economy, population, and security.

This criterion can be used to assess the gravity threshold of the attack in determining whether it amounts to an armed attack. However, assessing the gravity threshold of an imminent attack with this criterion is challenging because it is based on the likelihood that extensive damage to vital infrastructures is reasonably expected to occur. It is more accurate to focus on the intended consequence of substantial destruction. Some scholars differ on whether economic aggression fits into the category of acts that amount to armed attacks because of substantial financial loss. Although article 51 appears to affirm armed aggression as the primary type of aggression that can amount to an armed attack, the description does not limit the right of a State to defend itself from serious injuries to its national security resulting from any type of aggression.⁵¹⁴

4.3.3. Identifying Critical Infrastructure

Another issue that is relevant in assessing the occurrence of armed attacks is the question of what qualifies as critical infrastructure. It has been argued that:

Critical infrastructure is deemed critical because its incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation.⁵¹⁵

This argument is valid to the extent that the debilitating impact threatens the peaceful existence of a State. The critical infrastructures are States' vulnerabilities that can be in the air, on land or at sea.⁵¹⁶ The threat to these infrastructures can be physical or

⁵¹⁴ Dempsey "Economic Aggression and Self-Defence in International Law: The Arab Oil Weapon and Alternative American Responses Thereto" 1977 9 *Case Western Reserve Journal of International Law* 253 267: "the fact that economic coercion has not been accepted within the definition of aggression for the purpose of organs of international security bears no relation to the question of whether, against such indirect forms of highly injurious conduct, the individual State whose own security is endangered has the legal right to resort to self-defence".

⁵¹⁵ Waters "Information Warfare Attack and Defence" in *Australia and Cyber-warfare* (2008) 50.

⁵¹⁶ The White House Washington *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003) 60. - The United States has identified the maritime shipping sector as one of their critical infrastructures by stating that: "The maritime shipping infrastructure includes ports and their associated assets, ships and passenger transportation systems, coastal and inland waterways, locks, dams and canals, and the network of railroads and pipelines that connect these waterborne systems to other transportation networks."

cyber in nature and a hybrid form of both.⁵¹⁷ For instance, an attack on a State's territorial integrity or flag ship attacks a State's sovereignty and a violation of its maritime security.⁵¹⁸ Irrespective of the form an attack takes, the destructive consequence on the critical infrastructures of a State is one of the main determining factors for declaring the occurrence of an armed attack.

Determining what can be categorised as critical infrastructure can vary among States. The U.S has stated that 'critical infrastructure' encompasses complex facilities, systems, and functions which

include human assets and physical and cyber systems that work together in processes that are highly interdependent...To complicate matters further, our most critical infrastructures typically interconnect and, therefore, depend on the continued availability and operation of other dynamic systems and functions.⁵¹⁹

The European Union (EU) has adopted a policy for identifying and designating a critical infrastructure. For the EU, critical infrastructure

means an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or wellbeing of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions. The significance of the impact is assessed against distinct cross-cutting criteria, which encompass casualties, economic and environmental effects and public effects.⁵²⁰

Based on the above description of critical infrastructure, it is safe to submit that when cyber systems of a State's maritime shipping infrastructure are targeted, a State can form its security assessment based on its vulnerability and the significant impact on its national security, economy and lives of its citizen. Identifying and designating a State's critical infrastructure helps in determining the occurrence of an armed attack.

⁵¹⁷ Cybersecurity and Infrastructure Security Agency "Infrastructure Security" (undated) <https://www.cisa.gov/infrastructure-security> (accessed 2021-08-09).

⁵¹⁸ Goettsche-Wanli "Sustainable Production of Offshore Renewable Energy: A Global Perspective" in *Sustainable Ocean Resource Governance: Deep Sea Mining, Marine Energy and Submarine Cables* (2018) 8, 60; UNGA "Report of the Secretary-General. Oceans and the Law of the Sea" (10 March 2008) UN Doc A/63/63, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N08/266/26/PDF/N0826626.pdf?OpenElement> (accessed 2020-05-08) par [39].

⁵¹⁹ The White House Washington *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003) 6.

⁵²⁰ Directive 2008/114/EC, Articles 2 and 3 (undated) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI\(2021\)662604_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf) (accessed 2021-08-09).

4.3.4. Armed Attack in the Maritime Context

The focus of this chapter is to assess when attacks on the critical cyber infrastructures of a State's maritime sector amounts to an armed attack. This will be looked at from the maritime context in this section and the cyber security perspective later in this chapter. How can it be determined that a "maritime armed attack (MAA)" has occurred? Is the weapon used the critical determinant of whether an armed attack has occurred? Is the perpetrator of the act a determining factor? Is it the intent of the attacker that determines what constitutes an MAA? Or is it the physical or immediate destructive consequence of the act that determines whether an MAA has occurred?

The ICJ described the features of an armed attack in the Nicaragua case by stating that:

The actions of the Nicaraguan-supported guerrillas have increasingly been aimed at destroying the economy and infrastructure of El Salvador'. Roads have been mined, bridges and power transmission facilities destroyed, and bombs emplaced in buses and other forms of public transportation.⁵²¹

It can be inferred from the above description that the intention of a threat or an actual armed attack is implied from the actions of an attacker. Actions aimed at destroying a State's infrastructure as described above will amount to an armed attack. It is submitted that maritime attacks with the objective to destroy ships, ports, oil rigs, or the administrative systems of maritime authorities or controllers of a State can qualify as armed attacks. Notably, the description of armed attack in the Nicaragua case does not exclude other forms of destructive acts. However, it lists those types of destructive acts that were peculiar to the case before the court at that moment.

Since article 51 does not expressly state the type(s) of weapon(s) that must be used to refer to as an armed attack, it permits an inclusive interpretation that may include all types of weapons. The list of weapons is not limited to guns and explosive devices. They may include nuclear⁵²² as well as cyber weapons. It is submitted that when these cyber weapons are used in the marine environment or against ICT-reliant maritime infrastructures of a State, it amounts to MAA. More discussions about

⁵²¹ *Nicaragua case* par [195 and 211]

⁵²² *Nuclear weapons case* par [39].

attacks carried out through the use of cyber weapons with reference to international humanitarian law principles will be done in chapter 5.

In determining whether an MAA has occurred, one can rely on the ICJ for guidance in its description of armed attack as actions by either a State's military forces against another State (or non-State actors' actions attributable to States), which cause grave destructive consequences.⁵²³ These destructive consequences include destroying a State's economy, damaging critical infrastructures and loss of lives.⁵²⁴ It is submitted that when the consequence of MAA is similar to those caused by kinetic forces attributable to a State, it is easily discerned as an armed attack.

However, the court distinguished between acts that amount to threat or use of force on the one hand and armed attack triggering self-defence on the other hand. In the *Nicaragua case*, the ICJ asserted the existence of a gap between the provisions of article 2(4) on use of force and article 51 on the right of self-defence. In the *Oil Platforms case*, it referred to the *Nicaragua case* by emphasising the necessity to distinguish between the gravest forms of the use of force which are referred to as armed attack and other less grave forms of force.

As the Court observed in the case concerning Military and Paramilitary Activities in and against Nicaragua, it is necessary to distinguish 'the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'...⁵²⁵

It clarified that the distinction could be determined by the scale and effects of the attack. The *oil platforms case* reveals attacks against Iranian oil installations with oil wells and submarine transportation pipelines.⁵²⁶ The U.S attacks on the Salman and Nasr oil complexes in 1988 involved shelling from U.S ships and air assaults. These attacks were allegedly carried out in self-defence against Iran. The U.S accused Iran of laying mines in international waters, which destroyed a U.S warship returning to Bahrain.⁵²⁷

One of the requirements for determining the occurrence of an armed attack, as can be inferred from the *Nicaragua and Oil Platforms cases*, is the use of deadly force

⁵²³ Military and Paramilitary Activities in and Against Nicaragua, para [193-5].

⁵²⁴ *Ibid.*

⁵²⁵ *Oil Platforms case (Iran v. U.S.)*, 2003 ICJ Reports 161, par[51, 64].

⁵²⁶ *Ibid* at par [65-71].

⁵²⁷ *Ibid.*

against another State. The question of attribution arose in these cases, particularly in the oil platforms case where Iran alleged that the US lacked evidence to prove that mines laid by Iran damaged a U.S warship. Also, in the *DRC vs Uganda* case, the ICJ emphasised the requirement of attribution in determining the occurrence of an armed attack by non-State actors.⁵²⁸ However, the court did not comment on the conditions that may trigger the right of self-defence in this circumstance.⁵²⁹ When a threat or use of force does not rise to the threshold of an armed attack, the option available to the victim state is proportionate countermeasures. Also, when States provide weapons to non-State actors to carry armed attacks, the State may not be held responsible for an armed attack, although the act is an internationally wrongful act.⁵³⁰

Some key facts may be deduced from the above analysis. Although there are several descriptions of an armed attack by scholars, Constantinou's description provides a complete depiction of the elements of an armed attack. It emphasises that an armed attack refers to an attacking force corresponding with the understanding of armed attack as mentioned in article 51 of the UN Charter. It can be construed that MAA against a State can be carried out by States and non-State actors. A maritime armed attack can be described as an armed attack against a State which occurs in its maritime domain. When a non-State actor acts independently of any support from any State, the victim States treat the armed attack as a crime. When a State directly or indirectly and forcefully threatens or violates the territorial sovereignty of the marine environment of another State, a maritime armed attack can occur. Also, one can apply the reasoning from the ICJ's decisions⁵³¹ that not all use of force in the marine environment qualify as MAA, but all armed attacks may qualify as the use of force.⁵³² Based on articles 2(4) and 51 of the UN Charter as well as the ICJ rulings as discussed above, it is submitted that the criteria for a maritime attack to qualify as armed attack are:

⁵²⁸ Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo v. Uganda*) par [131-135].

⁵²⁹ *Ibid*; *DRC case* par [146 and 147].

⁵³⁰ Judge Jennings's dissenting opinion in *Nicaragua Case*.

⁵³¹ Military and Paramilitary Activities (*Nicaragua v. United States*), 1986 I.C.J. 101 (June 27) (Merits).

⁵³² Waxman 2011 *Yale Journal of International Law* 421, 427.

- a. The attacker can be either a State or non-State actor, but the target must be a State.
- b. The attack can be perceived as an imminent threat to the target.
- c. The force, whether tangible or intangible, must be intense.
- d. The target element must be important maritime infrastructures of a State.
- e. The consequence of the attack must be potentially or 'actually' extensively destructive.
- f. The intended destruction can be inferred from the hostility of act and the vulnerability of the victim.

The option of 'proportional countermeasures', which is available to address attacks that fall below the armed attack threshold, may be categorised as a reprisal and not self-defence in the context of article 51. This is because it is questionable as to whether it accommodates anticipatory prevention of the threat or use of force. Bearing in mind the unique nature of MCA as previously discussed, can there be legitimate anticipatory countermeasures in the event of a maritime cyber-attack that qualifies as an armed attack? This will be discussed in the following chapters.

4.4. Cyber-Attack as Armed Attack

As previously discussed, cyber-attacks occur through alteration, destruction, or disruption of timely and reliable access to confidential information.⁵³³ These cyber-attacks may occur in the maritime context with the resultant effect comparable to those caused through armed attacks by military forces. This section will critically analyse how a cyber-attack can qualify as an armed attack. Based on the discussion above concerning the criteria for qualifying as an armed attack, it is safe to say that a cyber operation can qualify as an armed attack. Some cyber codes or malicious software can qualify as arms in some instances.⁵³⁴ Most cyber-attacks do not occur in the forms that kinetic attacks do because they can be carried out without using tangible weapons. A cyber-attack attributable to a State violates the customary principle of non-intervention, thereby justifying certain degrees of responses depending on the scale and effect of the attack.⁵³⁵

⁵³³ Dynkin and Dynkin "Derivative Liability in the Wake of a Cyber-attack" 2018 28 *Albany Law Journal of Science and Technology* 23 32.

⁵³⁴ Dunlap "Perspectives for Cyber Strategists on Law for Cyberwar" 2011 5(1) *Strategic Studies Quarterly* 81 85.

⁵³⁵ *Nicaragua case* 1986 ICJ Reports 107 par [205].

There is room for varied interpretations of the existing general principles in the absence of specific international humanitarian law principles on cyber-attack. It has been argued that international humanitarian law is obsolete and inadaptable to contemporary cyber conflicts.⁵³⁶ Applying its principles to the cyber context has created uncertainties and ambiguity, especially in determining when or which cyber-attacks are armed attacks. This determination is relevant to States in forming anticipatory or reactive responses against cyber-attacks.

Also, it is imperative to distinguish between the actions of cybercriminals from the relentless and widespread cyber-attacks with similar consequences to armed force. Persistent and extensive cyber-attacks seem to be more likely State-sponsored instead of cybercrimes by individuals, which are regulated by domestic laws.⁵³⁷ However, Schmitt argues that only extensively catastrophic and constant cyber-attacks carried out by a well-coordinated group is sufficient to amount to a universally recognised armed attack.⁵³⁸

4.4.1. Critical Analysis of Cyber Armed Attack

From the above analysis, it is implied that some cyber-attacks can be identified as armed attacks with the guidance of article 51 of the UN Charter. At the same time, other wrongful cyber usages may constitute espionage or be treated as cybercrime. This inference is made based on the guiding principles of scale and effect and attribution.⁵³⁹ In this section, it will be discussed that attribution, in this context, refers to identifying the attacker responsible for the cyber-attack suffered by a State. The attacker can be a State or non-State actor sponsored by a State or a lone wolf attack. Also, it will be argued that the principle of 'scale and effect', in this instance, refers to the severity of the attack on the targeted infrastructure and the complexity of the cyber weaponry. Cyber-attack as an armed attack can be viewed from different perspectives.

⁵³⁶ Waxman 2011 *Yale Journal of International Law* 421, 426.

⁵³⁷ Dunlap . "Perspectives for Cyber Strategists on Law for Cyberwar" 2011 5(1) *Strategic Studies Quarterly* 81 88.

⁵³⁸ Schmitt "Cyber Operations in International Law" in *Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy* (2010) 155, 176.

⁵³⁹ Weissbrodt "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347 349.

Firstly, an attempt can be made to apply the reasoning of the ICJ in the Nicaragua case where it concluded that not all uses of force amount to an armed attack, and not all interventions by one state into the affairs of another rise to the level of a use of force.⁵⁴⁰ An adapted interpretation of this conclusion to the cyber-attack context can be read as: not all cyber force amounts to an armed attack, and not all cyber intrusions can be classified as the use of force. This transliterated assertion is debatable because a cyber-attack is a unique security threat with distinct destructive potentials within the shortest time imaginable. Therefore, it can be argued that all cyber-attacks can qualify as the use of force and armed attack depending on the gravity of the hostile intent of the attacker.

As stated by the ICJ in the *Oil Platforms case*, the specific intent to cause harm is relevant in determining an armed attack.⁵⁴¹ How do you determine the hostile intent of a cyber-attacker? Is it the complexity of the cyber weaponry or the consequence of the cyber-attack that is the determining factor? According to Zemanek,

It is neither the designation of a device, nor its normal use, which makes it a weapon but the intent with which it is used and its effect. The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the condition of 'armed' attack.⁵⁴²

When a State perceives an unauthorised intrusion in its cyberspace, the cyber operation becomes an attack. When this intrusion threatens or adversely affects critical infrastructures of a State or endangers citizens' lives by adversely affecting medical devices,⁵⁴³ it can be assessed to have risen to the level of an armed attack. Specifically, suppose the adverse effects threaten or lead to enormous damage to property or loss of lives like a kinetic attack. In that case, that cyber-attack will be on the threshold of an armed attack. Due to the virtual reality of cyberspace, the intent of an attacker can mainly be determined by a presumption that any unauthorised cyber intrusion is a potential cyber-attack which can graduate, without warning, to a major attack with more serious consequences.

⁵⁴⁰ Military and Paramilitary Activities (*Nicaragua. v. United States*), 1986 ICJ Reports 119 (June 27) (Merits).

⁵⁴¹ Case Concerning Oil Platforms (*Iran v. United States*) 2003 ICJ Reports 161, 191 par [64].

⁵⁴² Zemanek "Armed Attack" 2010 *Max Planck Encyclopaedia of Public International Law* 21.

⁵⁴³ Czosseck and Geers (eds.) *Virtual battlefield: Perspectives on Cyber Warfare* (2009) 224.

The presumption of the attacker's intent to cause damage is drawn from the circumstantial evidence of unauthorised access, the critical target, and the probable destructive consequences that can arise from such unauthorised access. Schmitt, in his argument on what constitutes an armed attack, focuses on the adverse consequence of an act by stating that:

the essence of an 'armed' operation is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects.⁵⁴⁴

This means that only a cyber-attack that causes death, injury or damage to physical objects can amount to an armed attack. „Schmitt's argument can be criticised based on the fact that it does not take into account damage done to intangible objects such as communication frequencies, navigation codes, and nuclear algorithms. His view that there must be a tangible or physical manifestation of the damage caused by the cyber-attack before it can meet the threshold of armed attack invalidates the classification of the intangible damage as an armed attack. Also, it restricts the victim's reaction to the armed attack until the damage manifests overtly.

Whether a cyber-attack can be defined as an armed attack can be answered by viewing it from the expansionist and restrictive approaches.⁵⁴⁵ These two approaches comprise the instrument-based, target-based, consequence-based and sovereign-based approaches.⁵⁴⁶ The 'expansionist' approach portrays the argument that even in the absence of physical damage, a critical consequence seen in the massive disruption by the Estonian cyber incident of 2008 could qualify as an armed attack.⁵⁴⁷ This approach seeks to extend or expand the understanding of the circumstances that amount to an armed attack. It provides a broader perspective for interpreting article 51 of the UN Charter.

The 'restrictive' approach argues that a literal interpretation of the provision of article 2(4) on the use of force would portray the denial-of-service cyber-attacks as mere political or economic force since it did not cause physical destruction in Estonia. This approach creates a limitation that excludes all intangible types of adverse consequences arising from a cyber-attack. It underestimates the destructive capacity

⁵⁴⁴ Schmitt *Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy* (2010) 155.

⁵⁴⁵ Roberts 2014 *Northern Kentucky Law Review* 535, 554-555.

⁵⁴⁶ *Ibid.*

⁵⁴⁷ *Ibid.*

of political and economic force. The continued existence of a State can be threatened when the economy is crippled and the political climate is unstable due to cyber insecurity.

Schmitt reconciles these two approaches by proposing that cyber-attacks must fit into a standard consequence-based structure of orientation to qualify as an armed attack. He argues that:

by contemporary international law, qualitative indicators of attack (death, injury, damage, or destruction) are more reliable in identifying those actions likely to be characterised as an armed attack than quantitative ones (number of deaths or extent of destruction). So long as a cyber operation is likely to result in the requisite consequences, it is an armed attack.⁵⁴⁸

He explains that damage to cyber property, such as bank data alone, does not amount to an armed attack. However, when the damage manifests in physical consequences, it is realistic to classify the cyber-attack as an armed attack.⁵⁴⁹

Roscini and Lin further argue that the consequence-based approach should include cyber incidents that occur through kinetic force.⁵⁵⁰ However, Dinstein and Waxman argue that differentiating between the means of attack as kinetic or non-kinetic is unnecessary. However, the focus should be on the aggressive consequences of the deed, which bear a resemblance to the effects caused by traditional military force.⁵⁵¹

A critical assessment of these opinions highlights a pivotal point that hinges on the gravity of destruction caused by the military force as the yardstick for determining what constitutes a cyber armed attack. Having established that weaponry is not restricted to guns, it is submitted that separate consideration should be given to cyber destruction's unique nature. It should be assessed independently on a different scale of gravity. The qualitative effect of cyber-attacks may not always manifest how the damage caused by kinetic military attacks appears, but this does not minimise its severity.

⁵⁴⁸ Schmitt "Cyber Operations and the *Jus ad Bellum* Revisited" 2011 56 *Villanova Law Review* 569, 589.

⁵⁴⁹ *Ibid.*

⁵⁵⁰ Lin "Offensive Cyber Operations and the Use of Force" 2010 4 *Journal of National Security Law and Policy* 63, 73; Roscini *Max Planck Yearbook of United Nations Law* 2010 85, 115.

⁵⁵¹ Dinstein "Computer Network Attacks and Self-Defence" 2002 76 *Computer Network Attack and International Law* 99 103; Waxman "Cyber-attacks as "Force" Under UN Charter Article 2(4)" 2011 87 *International Law Studies Serv US Naval War College* 43 47).

Despite these scholarly analyses and the notable ICJ position that not all uses of force qualify as an armed attack, there is still a lacuna and an ambiguity.⁵⁵² This is because in cyberspace, not all destructions are in the form of explosions. The harmful result of the attack may be experienced in different forms.⁵⁵³ Therefore, a realistic, overarching, and open-minded assessment of cyber-attack as an armed attack is needed to prevent instances where States cannot invoke self-defence against specific armed forces such as cyber force.

For instance, article 41 of the UN Charter does not acknowledge that,

complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication⁵⁵⁴

could be done using non-kinetic force. It does not state that these interruptions could be carried out through a cyber-attack.⁵⁵⁵ It is fair to acknowledge that at the time of the drafting of the Charter, the level of sophistication of cyber-attacks was below what it is and could be in the future. Presently, complete, and partial interruption of economic and political relations can be caused by cyber-attacks, leading to quantifiable and unquantifiable damage. Although it is not a norm to legally interpret an economic attack that does not result in loss of life as an armed attack,⁵⁵⁶ the contemporary and ultramodern debilitating consequences of cyber-attack on economic and political relations necessitates an urgent review of the legal paradigm on this issue. This will clarify the international best practices for States.

Furthermore, applying the scale and effect factor to the cyber context can raise specific questions. Should the scale and effect factor be applied separately to the imminent attack and the potential consequence of the attack, respectively, in determining whether a cyber-attack is a potential armed attack that can trigger self-defence using force or other means? How can the intensity of a cyber-attack be

⁵⁵² Dever and Dever “Cyber Warfare: Attribution, Preemption, and National Self-defence” 2013 2 *Journal of Law and Cyber Warfare* 25, 28.

⁵⁵³ Schmitt “The Law of Cyber Warfare: Quo Vadis?” 2014 25 *Stanford Law & Policy Review* 269 282-284.

⁵⁵⁴ Article 41 of the UN Charter of 1948.

⁵⁵⁵ Article 41 of the UN Charter provides 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.”

⁵⁵⁶ Chayes “Rethinking Warfare: The Ambiguity of Cyber-attacks” 2015 6 *Harvard National Security Journal* 474 507-508.

determined? Should the effect be a hybrid of direct and indirect, only direct, or indirect?

In the absence of an ICJ ruling on whether the damage caused by sophisticated cyber programs constitutes an armed attack, consequence-based reasoning has been popular. However, a “perception-based” analysis could be explored to efficiently address an imminent cyber-attack with unlimited destructive potential, which would necessitate a proportional anticipatory response. This “perception-based” theory is not a law, but its legal obligation can be deduced from State practices. A technologically advanced State has a better chance to detect an imminent cyber threat through both cyber espionage and human intelligence, or either through cyber-espionage or human security intelligence. In addition to their cyber security policy, the intelligence gathered will inform their decision or approach to repel an imminent cyber-attack. The world powers perceive cyber-attacks as dangerous information weapons with the capacity to cause mass disruption, produce a devastating outcome similar to the consequence of weapons of mass destruction and potentially be an act of war.⁵⁵⁷

On May 6th, 2019, Israel’s defence forces launched an armed attack due to a cyber-attack. It released a statement saying that:

We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.⁵⁵⁸

The military strike was intended to render *Hamas* incapable of cyber-attacks. This is the first of its kind and it confirms the theoretical analysis that some States may perceive cyber-attack as a use of force necessitating a response with force. It seems to be the standard for the options available to States in responding to cyber-attacks.⁵⁵⁹ Israel is seen as one of the global leaders on issues of cyber conflict and security. Therefore, it should be expected that the assertions on viewing cyber-attacks as an armed attack will become more popular.⁵⁶⁰ This incident has expanded

⁵⁵⁷ Roscini “Worldwide Warfare – *Jus ad bellum* and the Use of Cyber Force” 2010 14 *Max Planck Yearbook of United Nations Law* 85 109.

⁵⁵⁸ <https://mobile.twitter.com/IDF/status/1125066395010699264> (accessed 2019-05-07) tweet now deleted.

⁵⁵⁹ Doffman “Israel Responds to Cyber-attack with Air Strike on Cyber-attackers in World First” (undated) <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/> (accessed 2019-05-07).

⁵⁶⁰ *Ibid.*

the understanding of cyber-attack as an armed attack. Notwithstanding, it will require State practice over a period which creates legal obligations among States before an international customary law is formed based on this incident.

It is important to juxtapose the action of the Israeli military and the interpretations of articles 2(4) and 51 of the UN Charter. Interestingly, the statement that was released by the Israeli military did not mention the potential or actual extensive destruction of property or loss of life that necessitated the use of force. However, it was generally reported that the cyber-attack was intended to harm Israeli citizens. This is in line with the assertion that a kinetic effect approach is a faulty hypothesis that should be replaced with a non-kinetic effects-based approach.⁵⁶¹ The Israeli military has proved this to be the most effective approach in justifying that a cyber-attack can be perceived as an 'armed attack'. Therefore, a cyber-attack that launches a virus with the capability of disabling an air defence system should be viewed as an armed attack, as would a kinetic force capable of causing the same effect.⁵⁶²

Notably, the US cyberspace policy suggests that it could justifiably respond to hostile cyber acts in cyberspace like it would to any other threat to its country.⁵⁶³ Due to its enormous reliance on information technology, it is more vulnerable to cyber-attacks. It is submitted that cyber-attacks that have the potential of causing damage no matter the degree of severity should amount to a grave use of force and possibly armed attack. The assessment of severity or gravity can be done by applying the principle of scale and effect.

4.4.2. Scale and Effect Principle as Determinant of Cyber Armed Attack

Applying the denotative meaning of 'scale' would mean 'the extent or size of the attack'.⁵⁶⁴ Effect will refer to the 'change which is a result or consequence' of the attack.⁵⁶⁵ The method of assessing or determining the extent and consequence of a

⁵⁶¹ Roberts 2014 *Northern Kentucky Law Review* 535 563.

⁵⁶² *Ibid.*

⁵⁶³ Hon. Koh "Remarks at the U.S. Cyber Command Inter-Agency Legal Conference" (18 September 2012), <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> (accessed 2019-05-18).

⁵⁶⁴ Merriam Webster "Scale" <https://www.merriam-webster.com/dictionary/scale> (accessed 2019-04-29)..

⁵⁶⁵ Google "Effect" (undated) https://www.google.com/search?q=meaning+of+effect&rlz=1C1CHBD_enNG735NG735&oq=meaning+of+effect&aqs=chrome..69i57j0l5.11652j1j4&sourceid=chrome&ie=UTF-8 (accessed 2019-04-29).

kinetic attack may not be the same as a cyber-attack. The intangible nature of cyber weapons may not distinctively give room for substantial visibility of its magnitude and intensity. Likewise, the extent of the potential damage that may be caused may not be accurately ascertained without prior intelligence reports about the intent of the hostile State.

However, some examples of cyber-attacks that could qualify as armed attacks in the light of the above definitions include cyber-attack on a State's power grid which leads to catastrophic loss of life and destruction of property that depends on it to function efficiently.⁵⁶⁶ Suppose computers controlling dams and water supply suffer a cyber-attack that triggers deadly floods in a populated area or alters the chlorine formula of drinking water supplied to citizens to cause poisoning. In that case, it can amount to an armed attack.⁵⁶⁷ If the information technology of a ship or aircraft suffered a cyber-attack that led to a collision or crash, that is an armed attack. If a nuclear plant experiences a cyber-attack that causes the release of radioactive materials that endangers the lives of inhabitants of that area, it is an armed attack.⁵⁶⁸ However, a cyber-attack in the form of a temporary denial of service which does not lead to loss of lives or extensive damage to property but qualifies as use of force will not amount to an armed attack.⁵⁶⁹ In addition, Chayes states that:

If critical infrastructure systems were destroyed or crippled, death and illness might result-quickly or slowly. A full-scale attack on critical infrastructure theoretically could prove as much a military attack with kinetic effects over time as bombing raids on industrial production in traditional wars. It is not a stretch to treat a situation in which people are wounded or die as a consequence of a cyber-attack as worthy of military response.⁵⁷⁰

From these examples, the emphasis for qualifying as an armed attack is on the loss of lives and extensive damage to property. Focusing on the hostile intent of a cyber-attacker to cause loss of lives and destruction of critical infrastructures is equally important. There is no universal definition of what critical infrastructures entail.⁵⁷¹ This has been emphasised by the UN General Assembly's recognition of the relative

⁵⁶⁶ Dinstein *Computer Network Attack and International Law* 2002 99, 105.

⁵⁶⁷ *Ibid.*

⁵⁶⁸ *Ibid.*

⁵⁶⁹ *Ibid.*

⁵⁷⁰ Chayes 2015 *Harvard National Security Journal* 474, 486; Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 54 *Harvard International Law Journal* 13 13.

⁵⁷¹ Roscini 2010 *Max Planck Yearbook of United Nations Law* 85, 117.

interpretation of critical information infrastructure.⁵⁷² States designate specific infrastructures as critical while others may not be so specific. Therefore, while State 'A' may claim that a cyber-attack against its critical infrastructures amounts to an armed attack, State 'B' may view the cyber-attack as mere use of force below the threshold of armed attack. While some scholars argue that economic force does not constitute the use of force,⁵⁷³ others argue that it can be considered a use of force due to the broad impact of the action.⁵⁷⁴ It is submitted that economic force that is the causal link to resultant loss of lives and destruction of property should be categorised as the use of force necessitating a proportional response.

Likewise, if a cyber-attack threatens critical infrastructure, causes grave damage or loss of lives, it must constitute an armed attack so that a victim State can respond with either cyber force or kinetic force irrespective of whether the perpetrator is a State or non-State actor sponsored by a State.⁵⁷⁵ This interpretation of articles 2(4) and 51 are in good faith and in line with the object and purpose of the UN Charter as required by the Vienna Convention on the Law of Treaties (VCLT). The VCLT provides that:

A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.⁵⁷⁶

One of the main objectives of the UN Charter is to maintain peace and security of States in their platforms of interrelationships, whether on land, airspace, at sea or in cyberspace. It is submitted that an interpretation that promotes peace and security and a legitimate justification for self-defence through the use of force by States on these platforms of interaction is reasonable.

4.5. Qualifying Maritime Cyber-attack as Armed Attack

Maritime cyber armed attack (MCAA) can be explained by analogy with the above discussion on MAA and cyber armed attack. Maritime cyber security affects mainly

⁵⁷² UN GA/RES/58/199 of 23 December 2003.

⁵⁷³ Schmitt "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" 1999 37 *Columbia Journal of Transnational Law* 885 908; Chuang "The United States as A Global Sheriff. Using Unilateral Sanctions to Combat Human Trafficking" 2006 27 *Michigan Journal of International Law* 437 459 – 460.

⁵⁷⁴ Barkham "Information Warfare and International Law on the Use of Force" 2001 34 *New York University Journal International Law and Politics* 57 68.

⁵⁷⁵ Roberts 2014 *Northern Kentucky Law Review* 535, 549.

⁵⁷⁶ Article 31 of the Vienna Convention of 1969 on the Law of Treaties.

ships, ports, shipping companies, oil rigs and administration systems. As previously discussed in chapter 1, the vulnerability of ships essentially arises from the increased risk of reliance on ICT by modern ships. An imminent threat or a complete cyber-attack on the communication systems can gravely endanger the vessel.⁵⁷⁷

MCAs do not automatically qualify as armed attacks as provided for in article 51 of the UN Charter. They have to satisfy the international law requirements for meeting the threshold of armed attack.⁵⁷⁸ They have to target a State, cause enormous damage to property and result in the loss of lives.⁵⁷⁹ When they fall below this threshold, they may be viewed as internationally wrongful acts by States in the form of MCIs or cybercrimes by States and non-state actors.⁵⁸⁰ So, a maritime cyber armed attack (MCAA) would be an MCA that is suffered by a State with the grave consequences of loss of lives or enormous damage to property and information-technology-reliant maritime infrastructures of a State.

4.5.1. Examples of Maritime Cyber-attacks

Vulnerability in a ship's Electronic Chart Display and Information System (ECDIS)⁵⁸¹ can enable cyber-attackers to gain entrance and alter files and charts on and offshore. This creates dangerously false navigation information.⁵⁸² The resultant damage of such an attack could be an environmental or a financial disaster. Environmental pollution may lead to the loss of lives and the destruction of property. An AIS⁵⁸³ attack could falsify a vessel's identity, location, speed, or direction, leading to a collision. Attackers could masquerade as maritime authorities and unlawfully instruct the crew to carry out dangerous instructions such as disabling their AIS to make the ship undetectable or operate on a certain frequency, thereby impeding

⁵⁷⁷ DiRenzo, Goward, and Roberts "The little-known challenge of maritime cybersecurity" in *Information, Intelligence, Systems and Applications (IISA)* (2015) 1-5.

⁵⁷⁸ *Nicaragua case* 1986 par 95

⁵⁷⁹ *Ibid.*

⁵⁸⁰ This can be inferred from the ICJ's reasoning in the *Nicaragua case*.

⁵⁸¹ ECDIS immediately merges different information and helps with self-operating decision making in navigation and detecting unseen threats. It processes information from electronic navigational charts, GPS, and other navigational sensors.

⁵⁸² DiRenzo *Information, Intelligence, Systems and Applications* 1-5.

⁵⁸³ AIS tracks ships mechanically by electronically connecting data with other ships, AIS base stations and satellites. It enables ships operating in maritime transport services to communicate about their location.

communication.⁵⁸⁴ This could lead to a collision. The valuable operational and communication assets of maritime administrators and internal procedures are vulnerable to attackers who may target their systems using ransomware or denial of service attacks.

The adverse effect of such attacks could inhibit effective phone or satellite communication systems which are very important to shipping operators, administrators, and other stakeholders.⁵⁸⁵ Lack of communication can lead to chaos in the shipping industry. Likewise, shipping companies may be exposed to cyber-attacks in this digital age where data and money traffic occurs mainly through the Internet. As a result of the substantial monetary loss that may occur, an economy-crippling consequence should be viewed as a grave loss. In line with the ICJ's reasoning, all the above attacks may quickly spiral out of control and lead to serious consequences that meet the armed attack threshold.

In addition, oil rigs may be vulnerable to MCAA by targeting their Dynamic Positioning (DP)⁵⁸⁶ system, which carries information about positioning, rig's sonic transponders, speed, and wind direction. This could lead to a devastating consequence of an oil rig failure. The marine environment will be adversely impacted; the safety of workers on the rig will be jeopardised and the enormity of the resultant economic loss.⁵⁸⁷ Also, modern electronic systems used for cargo handling at ports, especially for tracking cargoes, may be targeted, diverted, or altered, or information about a container may be destroyed by cyber-attackers.⁵⁸⁸

⁵⁸⁴ Balduzzi, Pasta, & Wilhoit (2014, December). A security evaluation of AIS automated identification system. In Proceedings of the 30th annual computer security applications conference 436 438.

⁵⁸⁵ Reiskind "Cyber Security and Maritime Commercial Shipping: Is Everything Ship Shape?" (2018) available at <http://natoassociation.ca/cyber-security-and-maritime-commercial-shipping-is-everything-ship-shape/> (accessed 2019-06-05).

⁵⁸⁶ DP is a computer-controlled system used by offshore oil industries which mechanically sustains the position of a vessel and stability of an oil rig.

⁵⁸⁷ Shauk "Malware offshore: Danger lurks where the chips fail" (29 April 2013) <http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/> (accessed 2019-06-10).

⁵⁸⁸ DiRenzo, Goward, and Roberts *Information, Intelligence, Systems and Applications* 1-5; CyberKeel "Maritime Cyber-Risks" 2015 <https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf> (accessed 2019-06-10).

4.5.2. Legal Theory on Maritime Cyber Armed Attack

Understanding the legal paradigm applicable in this context will help determine when or if these threats to maritime cyber security can constitute an armed attack. According to article 88 of the Law of the Sea Convention, the high seas are reserved for usage with peaceful intentions and should be protected from the threat or use of force.⁵⁸⁹ The peaceful usage of the high seas may be for ships' navigation through international straits, laying of submarine cables and maritime cyber activities.⁵⁹⁰ This implies that the threat or use of force in various forms against these peaceful activities amounts to unlawfulness.

Submarine communications cables have been described as “critical communications infrastructure” and “vitaly important to the global economy and the national security of all States.”⁵⁹¹ They are essential to global and national security. They are used for surveillance activities which may lead to issues relating to breaches of national security. When a state's submarine communication cables are attacked, it can be seen as a violation of national security.⁵⁹² Davenport explains that the attack can involve

...damage to submarine cables, cable landing sites and interference with network management systems, which involve both physical infrastructure and virtual space,⁵⁹³

The network management systems of submarine cables are prone to MCAs which can result in circumstances that threatens a State's national security. States and non-State actors can perpetrate unlawful activities at sea, including maritime cyber-attacks. These MCAs can be likened to some unlawful acts by sea pirates but with the use of information technology. The law of armed conflict may apply to States, while unlawful MCAs by non-State actors void of State sponsorship can be treated as crimes under international or domestic laws.⁵⁹⁴

⁵⁸⁹ Articles 88, 142 and 301 of UNCLOS.

⁵⁹⁰ Schmitt *Tallinn Manual 2.0* (2017) 234-235.

⁵⁹¹ G.A. Res. 65/37, 121 (Dec. 7, 2010).

⁵⁹² Davenport “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis” 2015 24(1) *The Catholic University Journal of Law & Technology* 63.

⁵⁹³ *Ibid.* at 87.

⁵⁹⁴ Schmitt *Tallinn Manual 2.0* (2017) 234-235

The UN Charter may be applied to MCAs even though it is not expressly stated.⁵⁹⁵ By implication, it can also be applied to maritime cyber-attacks and other maritime laws, especially the UNCLOS. The ambiguity and uncertainties associated with the application of international law to maritime cyber warfare also exist. The issues that arise include the determination of threat of cyber force at sea, the legal paradigm concerning State and non-state actors as victims or attackers, legitimate options available to States in anticipatory self-defence against maritime cyber-attacks and the unique standards for qualifying maritime cyber-attacks as armed attacks.

As analysed in the previous chapter, it is apparent that there are no universally acceptable answers to these questions. There are various scholarly contributions proffering answers or suggestions from different perspectives with no legally binding authority. The most referenced contribution on the subject is the Tallinn Manual. Despite it being criticised as mainly featuring the views of western scholars, it serves as a guideline for policymakers.

The Tallinn Manual defines a cyber-attack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”⁵⁹⁶ This definition reflects the international law definition of an attack as provided for in article 49(1) of Additional Protocol I to the Geneva Convention in the context of cyberspace. It focuses on the destructive consequence of the cyber operation. Applying this to the maritime context would query whether the offensive or defensive destructive cyber operation should originate from the sea or cause grievous harm to people and damage to property at sea or originate at sea and the destructive effect all felt at sea. Should MCA be defined as a cyber-attack originating from the sea with a reasonable expectation of causing damage and destruction on land, sea or air? Should it be described as a cyber-attack that originates from anywhere but causes injuries to persons and damage to property at sea? Or should it be a cyber-attack that originates at sea and causes injuries to persons and damage to property at sea?

⁵⁹⁵ Handler “The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare” 2012 48 *Stanford Journal of International Law* 209 216-219.

⁵⁹⁶ Schmitt M.N. (ed.) Tallinn Manual 2.0 on the International Law Application to Cyber Warfare 2ed (2017) 415

Article 42 of the UN Charter includes blockade among its prohibited actions that amount to illegal force. A blockade refers to the denial of a State's maritime access.⁵⁹⁷ It could occur by preventing a ship from communicating with a port. Kinetic or non-kinetic force may be employed to enforce or respond to it.⁵⁹⁸ Notably, the perception of blockades under international humanitarian law has evolved over the years, particularly on the requirement of physical destruction or death. In 1956, the international community recognised Israel's right to self-defence against a blockade by Egypt which prevented Israel's access to the Strait of Tiran.⁵⁹⁹ This denial of access was acknowledged as an act of war.⁶⁰⁰

However, the destruction caused by blockades is non-kinetic.⁶⁰¹ Therefore, a naval blockade that involves cutting off communication using cyber force will amount to an act of war subject to the authorisation of the Security Council. This authorisation might be delayed or vetoed thereby increasing the vulnerability of the victim-State to devastating maritime cyber-attacks which could occur within seconds.⁶⁰²

Furthermore, cyber operations that contravene the right of innocent passage by jeopardising peace, good order, or security of the coastal State may amount to cyber-attack.⁶⁰³ Analysing the provision of article 19(2) of the UNCLOS is relevant in determining whether maritime cyber-attacks constitute an armed attack. Based on a strict application of articles 2(4) and 51 of the UN Charter, some cyber operations may be referred to as maritime cyber-attacks. For example, cyber operations that result in unlawful threats or use of force at sea could be called maritime cyber-attack. Cyber operations that involve the use of cyberweapons beyond the ship while in another State's maritime zone may constitute a maritime cyber-attack. Cyber espionage operations launched from a ship involving acquiring confidential information that put the security of a coastal State at risk may be seen as MCA. It

⁵⁹⁷ Roberts 2014 *Northern Kentucky Law Review* 535, 563.

⁵⁹⁸ Li "When Does Internet Denial Trigger the Right of Armed Self-Defence?" 2013 38 *Yale Journal of International Law* 179 195.

⁵⁹⁹ Fink "The Gulf of Aqaba and the Strait of Tiran: The Practice of 'Freedom of Navigation' After the Egyptian-Israeli Peace Treaty" 1995 42 *Naval Law Review* 121, 125-126.

⁶⁰⁰ *Ibid.*

⁶⁰¹ Roberts 2014 *Northern Kentucky Law Review* 535, 564.

⁶⁰² Weissbrodt "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347 363.

⁶⁰³ Article 19(1) of UNCLOS.

may become more serious if it thwarts the functionality of a ship, port or oil rig and can be viewed as unlawful violation of a State's sovereignty.⁶⁰⁴

The agreed position of the International Group of Experts resonates in the Tallinn Manual:

By styling a cyber operation as a 'cyber espionage operation', a State cannot therefore claim that it is by definition lawful under international law; its lawfulness depends on whether the way in which the operation is carried out violates any international law obligations that bind the State.⁶⁰⁵

Therefore, cyber operations launched from a ship to disrupt or destroy the critical infrastructures of a coastal State may be MCA.⁶⁰⁶

4.5.3. Maritime Cyber-attack and the Threshold of Armed Attack

Although, the examples discussed above generally cite instances where cyber-attacks may constitute MCA, not all these instances meet the threshold of armed attack based on the ICJ reasoning in the *Nicaragua* case. Some of these MCAs may be potential armed attacks. This is because they possess the capability to cause enormous destruction or loss of lives in some instances. Therefore, the destructive capacity of MCAs should not be underestimated based on the *Nicaragua* case's reasoning for qualifying as an armed attack.

The significance of qualifying an MCA as an armed attack is to permit legitimate use of force by the target State in response to it.⁶⁰⁷ The ICJ jurisprudence on attaining the threshold of armed attack have identified similar factors which can be considered such as whether the attack is illegal, dangerous, costly, and destructive with varying intensity.⁶⁰⁸ These prerequisites can be applied to MCAs in determining their qualification as armed attack. However, States set the tone for their assessment of incidents based on their ideology interests and foreign policies.⁶⁰⁹ Legitimising anticipatory self-defence against MCAs may be clouded by the politics of international law. With increasing reliance on ICT by ships, the legal paradigm on

⁶⁰⁴ Schmitt *Tallinn Manual 2.0* 170.

⁶⁰⁵ *Ibid.*

⁶⁰⁶ Schmitt *Tallinn Manual 2.0* 242.

⁶⁰⁷ Schmitt *Tallinn Manual 2.0* 337.

⁶⁰⁸ Ruys 'Armed Attack' and Article 51 of the UN Charter: *Evolutions in Customary Law and Practice* (2010) 520-521.

⁶⁰⁹ Levi "Ideology, Interests and Foreign Policy" 1970 14(1) *International Studies Quarterly* 1 30.

MCA's needs urgent attention because cyber warfare is the contemporary form of conflict States are dealing with.⁶¹⁰

Applying Schmitt's consequence-based structure of orientation⁶¹¹ to the maritime cyber context requires that the effect of an MCA be overtly destructive before it meets the threshold of armed attack. This implies that a secondary effect arising from the MCA will be the determinant for assessing the occurrence of an armed attack. For instance, if the navigation system of a ship or oil rig suffers a denial-of-service cyber-attack which leaves the navigation control of the ship or oil rig in the hands of an aggressor, the assessment of the existence of armed attack will be based on the secondary consequence of such an attack. This can be the damage that occurs from loss of navigation control of the flag ship such as collision with another oil installation or with another ship.

It is submitted that the threat of losing navigation control of a flag ship should suffice as a probable disastrous consequence of such an MCA. Therefore, the determination of what constitutes a threat of, or an armed attack should encapsulate the primary effect of the aggressor's act as well as the probable secondary effect that may arise. This will create legitimacy for anticipatorily repelling such imminent MCAs. It is noted that Schmitt's consequence-based structure seems more suitable for analysing the aftermath of an MCA than justifying anticipatory self-defence.

Furthermore, a comparison between the ICJ's principle of scale and effect and the US Department of Defence's (DoD's) definition of a computer network attack suggests that the ICJ's mere frontier incidents will be viewed as armed attacks by the DoD.⁶¹² This is probably because it is precarious to strictly apply the scale and effect rule in cyberspace. A kinetic attack can produce an insufficient level of violence and not qualify as an armed attack. In contrast, the non-kinetic violence associated with cyber-attack may more quickly qualify as an armed attack.⁶¹³ MCAs are mostly non-kinetic forms of attack, which can potentially produce a grave level of damage in an

⁶¹⁰ Schneier, "It will soon be too late to stop the cyberwars" (2010-12-02) *Financial Times* <http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzz19cNCeszp> (accessed 2019-05-23).

⁶¹¹ Schmitt "Cyber Operations and the *Jus ad Bellum* Revisited" 2011 56 *Villanova Law Review* 569, 589.

⁶¹² Dunlap "Perspectives for Cyber Strategists on Law for Cyberwar" 2011 5(1) *Strategic Studies Quarterly* 81 86-87.

⁶¹³ *Ibid.*

instant. It is submitted that they can be more likely to qualify as an armed attack than kinetic attacks. Physical assessment of egregious damage in cyberspace seems to be sometimes impracticably measurable when using a similar scale of assessment used in the context of kinetic force because it might always fall short of the requirement by default.

In determining what constitutes use of force, States can rely on factors including severity, immediacy, directness, invasiveness, and measurability of effects, depending on the situation.⁶¹⁴ Likewise, in determining whether MCA amounts to an armed attack these factors can guide States in their decisions. A severe MCA which results in grave threat to critical naval military interests can constitute armed attack. For instance, damage to a State's submarine cable can be seen as an attack on the State's national security or an armed attack necessitating self-defence. When the damage to a State's submarine cables is done through a cyber-attack, it may be difficult to prove during an initial risk assessment if there is no overt manifestation of the damage.⁶¹⁵

MCA that poses an immediate and direct consequence such as loss of navigation control of a flag ship with the grave possibility of enormous destruction or loss of life may be viewed as armed attack necessitating anticipatory self-defence. Also, MCA disguised as cyber espionage, which results in technical malfunction allowing the penetration of highly classified naval military system coordinating flight operations on flight decks, may be viewed as an armed attack.⁶¹⁶ On June 25, fourteen maritime organisations sent a letter to U.S. Coast Guard Commandant Karl Schultz in which they protested the risky interference of GNSS signal and stated that:

A report recently released by the non-profit C4ADS1 clearly shows deliberate transmissions designed to block and deceive GPS and other GNSS signals affecting maritime operations in the Black Sea and Eastern Mediterranean from 2016 to 2018... In addition to degrading safety of life at sea, these transmissions violate International Telecommunications Union Radio Regulation 19.2 that stipulates 'All transmissions with false or misleading identification are prohibited.'⁶¹⁷

⁶¹⁴ Schmitt *Tallinn Manual 2.0* 334-337.

⁶¹⁵ Davenport 2015 *The Catholic University* [Vol. 24.1 *Journal of Law & Technology* 88.

⁶¹⁶ Lin 2010 *Journal of National Security Law and Policy* 63, 84.

⁶¹⁷ <https://rntfnd.org/wp-content/uploads/Multi-sig-Ltr-to-USCG-IMO-GNSS-Jamming.pdf> (accessed 2019-06-27).

This confirms the grievousness of maritime cyber-attacks and their qualification as an armed attack when a State is targeted.

4.5.4. Severity of Effect as a Determinant of Maritime Cyber Armed Attack

Sophisticated MCA may create invisible consequences that may be challenging to measure in terms of severity compared with kinetic attacks where they can be easily seen. The severity may be initially assessed by the extent of security exposure suffered by the victim-State after the MCA. The assessment can also consider the security risk of leaving the State exposed to the dangers of imminent or subsequent damages. Furthermore, MCA which causes economic loss is generally not viewed as an armed attack but when this economic loss cripples a State's economy, the resultant MCA may be viewed as a threat to the State's sustainable existence.⁶¹⁸ This may be seen as an exception to the general rule that economic loss or pressure does not amount to use of force, and by extension, armed attack.

For instance, the Estonian cyber-attack, when viewed from the result-oriented perspective, was adjudged as use of force because it disrupted the economy and key government functions.⁶¹⁹ Contrarily, since it did not result in the loss of life and destruction of property a consequence-based approach will not qualify it as an armed attack.⁶²⁰ Also, the uncertainty in attributing the attack to Russia disqualified the cyber-attack as armed attack.⁶²¹

Subsequently, it can be deduced that determining whether an MCA constitutes an armed attack should be done on a case-by-case basis. This is because there is no universal standard in the light of varying interpretations and applications of the above-discussed factors as well as the volatile nature of the politics of international law.⁶²² Determining the malicious intent of the attacker is often complex since maritime cyber-attacks and espionage can both be executed with the same

⁶¹⁸ *Ibid.*

⁶¹⁹ Schmitt 2011 *Villanova Law Review* 569, 577.

⁶²⁰ Weissbrodt 2013 *Minnesota Journal of International Law* 347, 373-375.

⁶²¹ *Ibid.*

⁶²² Koskeniemi "The Politics of International Law" 1990 1 *European Journal of International Law* 4, 32.

technology.⁶²³ However, it can be argued that MCAs that initially appear as cyber espionage can quickly become destructive leaving no time for the victim to be warned of the upgraded attack.⁶²⁴ Therefore, espionage in the cyber context should be viewed as imminent cyber threat once it is detected. This is contrary to the general interpretation of espionage as a legitimate information gathering operation.

The Internet creates a platform for numerous means of masking the identity of an aggressor. Although this makes attribution especially to States very challenging, it is necessary to create a more accountable alternative apart from applying criminal law to certain individuals even when States are involved in MCAs.

4.6. Conclusion

All the issues raised in the introduction have been discussed except the issue of State reaction to an armed attack which will be thoroughly dealt with in the next chapter. The determination of the occurrence of an armed attack is based on several factors such as the assessment of the attacker's act, the gravity of the attack, as well as the critical infrastructure that was targeted. In the context of maritime cyber security, a target-based or consequence-based approach can be applied to determine what amounts to an armed attack. When the target-based approach is applied to determine whether an MCA qualifies as an armed attack, it must be shown that the MCA threatens or has been launched at critical maritime infrastructures of a State. If this can be established, the State can lawfully invoke article 51 of the UN Charter to act anticipatorily or in actual self-defence.

The consequence-based approach, which states that an MCA only amounts to an armed attack if it results in death and destruction of property,⁶²⁵ was also discussed. The strict application of this approach to past incidents such as the Estonian cyber incident would have practically limited them to positions below the armed attack threshold. However, some States, such as the U.S.⁶²⁶ and Israel have drafted their cyber security policies such that it suggests a liberal or broad assessment of cyber-

⁶²³ Kesan and Hayes "Mitigative Counterstriking: Self Defence and Deterrence in Cyberspace" 2012 25 *Harvard Journal of Law and Technology* 429 431.

⁶²⁴ Melnitzky "Defending America Against Cyber Espionage Through the Use of Active Defences" 2012 20 *Cardozo Journal of International and Comparative Law* 537 566-568.

⁶²⁵ Li 2013 *Yale Journal of International Law* 179, 187.

⁶²⁶ Trump Administration 2017 National Security Strategy 31 available at: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> accessed 2019-06-04).

attacks to be mostly seen as armed attack despite the absence of death or physical damage to property. They view it as a threat against their national interest. They seem to have lowered the bar set by international law to determine an armed attack when assessing cyber incidents.

A strict application of international law to maritime cyber security incidents limits the possibility of holding States accountable for cyber-attacks. States are mostly left with the option of naming and shaming the perpetrators hoping that it would discourage future attacks. Not all MCAs are armed attacks, but modern cyber threat is getting more sophisticated with the possible potential of being classified as weapons of mass destruction. An MCA can be correctly described as the use of either kinetic force to destroy an Internet-reliant marine infrastructure or the use of a non-kinetic force to cause similar destruction that could lead to loss of life, physical or non-physical destruction aboard a flag ship, port, or an oil rig. However, some special instances should be treated with more sensitivity and caution, such as when cyber-attacks do not lead to kinetic destruction. The non-kinetic effects may be of such magnitude that the sustainable existence of a State is threatened by targeting its essential infrastructures. This should also constitute an armed attack.

Prioritising the importance of infrastructures is relative among States as their policies and interests might defer, thereby creating different degrees of vulnerabilities. Exposure to an MCA can have a more devastating effect on a very internet-reliant State than it would have on a State that is less reliant on information technology.⁶²⁷ When this analogy is applied to the maritime context where ships have become more vulnerable with their increasing reliance on information technology, it is safe to conclude that an MCA can lead to a devastating consequence.

Thus, due to the unique nature of maritime cyber warfare coupled with the possibility that it may be initiated at sea and its effect felt on land and vice versa, literal application of the current principles of *jus ad bellum* has become inadequate in addressing the issues arising from a maritime cyber-attack. Despite the debate surrounding qualifying an MCA as an armed attack, there is a profitable need to stretch the relevant interpretation of the UN Charter and apply the principles of customary international law to accommodate the peculiar nature of MCA.

⁶²⁷ Roberts 2014 *Northern Kentucky Law Review* 535, 568.

The vulnerability of flag ships to MCA appears to have inadequate and distinct legal clarity. Reliance is placed on scholars' analogous application of international humanitarian law principles which were conceived to address kinetic military attacks with no specific consideration for the evolving and unique threat of cyber-attacks. This justifies the difficulty in direct analysis on when MCA constitutes armed attacks. The reasonable test for qualifying an MCA as an MCAA. It should not be determined only by physical consequences. Alternatively, a destructive cyberspace consequence of an MCA can sometimes be sufficient to qualify it as an MCAA when it is backed by human and artificial intelligence cyber security reports.

Applying these arguments to practical MCAA incidents is not void of challenges. Should States wait for an attack to occur before a security assessment is conducted to determine whether it amounts to an armed attack? What are the options available to States when acting in self-defence? How can States protect themselves against imminent attacks? What are the challenges States may face in applying article 51 of the UN Charter in the context of maritime cyber security? These issues will be discussed in the next chapter.

CHAPTER 5: ANTICIPATORY SELF-DEFENCE AGAINST MARITIME CYBER-ATTACK

5.1. Introduction

It has been established in the previous chapter that MCAA is a form of armed attack that occurs in the dual setting of cyberspace and the marine environment. In the face of an imminent threat of MCAA, a State has the right to defend itself.⁶²⁸ What options are available to a State which is a victim of an MCAA? How does a State determine which option is best suited to the circumstance of the threat? These are the questions that arise when a State wants to address an MCAA which qualifies as an armed attack and, as such, amounts to a threat to its national security.

The options available to a State include self-help, measures of retorsion, countermeasures and self-defence.⁶²⁹ The option of anticipatory self-defence, which falls under the ambit of self-defence, is the crux of this research. Understanding the doctrine of self-defence is crucial to determining what States can do about a cyber threat to their maritime security. Can the State act in self-defence? How does the State prevent this threat from materialising while acting within the confines of the law? In answering these questions, it is essential to assess the legal actions carried out in self-defence against MCAA. The focus will be on the legal actions that entail the use of force and the legal principles that should apply in line with article 51 of the UN Charter. This chapter will focus on exploring the legality of anticipatory self-defence (ASD) and what it entails in the context of maritime cyber security. The options available in ASD against MCAA will be discussed. The legal requirements of imminence, necessity and proportionality will also be discussed and applied to the maritime context.

MCAA has been described based on the treaty provision of article 51 of the UN Charter in the previous chapter. The understanding of armed attack as a precondition for self-defence can be expanded to accommodate MCAAs. This assertion is predicated on the fact that armed attack, as previously construed when the charter was being drafted, did not consider the peculiarity of MCAA. The basis for proposing the assertion is hinged on the peculiarity of cyber-attacks, such as

⁶²⁸ Article 51 of the UN Charter.

⁶²⁹ Delerue *Cyber Operations and International Law* (2020) 423.

swiftness of occurrence, sophistication, which threatens attribution and inability to ascertain the attacker's intention accurately. A cyber intrusion, which ordinarily would not be considered an armed attack based on the ICJ's act-based interpretation, can swiftly upgrade to a destructive attack. At the same time, the attacker masks itself from being identified.

Defending against maritime cyber exploitation can be the first line of anticipatory self-defence based on the peculiarity of offensive cyber intrusion in maritime space. Alternatively, a delayed reaction due to an attempt to strictly comply with relevant international laws can give room for grave consequences. Wortham aptly stated that:

In order to account for cyber threats, specifically cyber exploitation and its ability to easily lend itself to cyber-attack, there needs to be a new or amended set of international laws. If the same legal regime continues to be used, the consequences could be dire.⁶³⁰

However, this assertion can be challenged if the ICJ reasoning on what qualifies as a threat of armed attack⁶³¹ is strictly applied. However, in the subsequent sections of this chapter, it can be settled by critically assessing current and upcoming principles of customary international law about attribution, imminence, necessity, and proportionality. The following sections of this chapter will make a case for anticipatory self-defence against MCAA and the challenges associated with it.

5.2. Invoking Anticipatory Self-defence against MCAA

Anticipatory self-defence has been a subject of controversy.⁶³² Although most of the definitions and explanations of anticipatory self-defence have some common ground of agreement, their perceptions vary concerning the preconditions for security assessment and actions to thwart the imminent attack. This is because invoking anticipatory self-defence is a strategic decision based on a State's national policy while taking into cognizance that it can escalate into a war.⁶³³ While some legal reasoning on invoking self-defence is narrower, others have a broad approach.⁶³⁴

⁶³⁰ Wortham "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent that May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" 2012 64(3) *Federal Communications Law Journal* 643 657.

⁶³¹ *Nicaragua case* 1986 par [195].

⁶³² Dunoff, Ratner, and Wippman *International Law Norms, Actors, Process* (3 ed) (2010) 863.

⁶³³ Mueller, Castillo, Morgan, Pegahi and Rosen *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (2006) 12-14.

⁶³⁴ Steenhoven "Conduct and Subsequent Practice by States in the Application of the Requirement to Report under UN Charter Article 51" 2019 6(2) *Journal on the Use of Force and International*

This narrow perspective is characterised by a restrictive interpretation of the provision of article 51 of the UN Charter on self-defence. In interpreting this provision, the ICJ stated that,

Article 51 of the United Nations 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 parameters⁶³⁵

It affirmed that it is yet to make a pronouncement on any form of preventative self-defence.⁶³⁶ This ICJ's narrow approach in viewing the subject of self-defence was affirmed in the *Nicaragua* case, where the court stated that it expresses no opinion on the issue of preventative self-defence.⁶³⁷ The ICJ, in its decisions in both cases, restricted itself by using the occurrence of an armed attack as the literal standard for invoking self-defence without looking further into the ambits of self-defence such as pre-emptive, anticipatory, or preventative self-defence.⁶³⁸ This legal reasoning does not resonate with most State practices because they rely on broader legal justifications to thwart an imminent attack.⁶³⁹

The U.S.⁶⁴⁰ and Israel⁶⁴¹ are examples of States that apply a broad approach to anticipatory self-defence. According to President Bush's 2003 State of the Union Address,

Law 242 266-267; Linnan "Self-Defence, Necessity and UN Collective Security" 1991 57 *Duke Journal of Comparative and International Law* 57 122.

⁶³⁵ Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo v. Uganda*), Judgment of 19 December 2005, ICJ Rep., par [148].

⁶³⁶ *Ibid.*

⁶³⁷ Case Concerning Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Judgment of 27 June 1986, ICJ Rep. 94, par [194].

⁶³⁸ *Nicaragua case* 1986 para [194]; *Oil Platforms* par [74]; Green *The International Court of Justice and Self-Defence in International Law* (2009)28.

⁶³⁹ Steenhoven "Conduct and Subsequent Practice by States in the Application of the Requirement to Report under UN Charter Article 51" 2019 6(2) *Journal on the Use of Force and International Law* 242 266-267.

⁶⁴⁰ Courtsey Media "Text of President Bush's 2003 State of the Union Address" (28 January 2003), http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/bushtext_012803.html (accessed 2021-12-01); *The National Security Strategy of the United States of America*, <http://www.state.gov/documents/organization/63562.pdf>. "The United States has long maintained the option of preemptive actions to counter a sufficient threat to our national security. ... Yet in an age where the enemies of civilization openly and actively seek the world's most destructive technologies, the United States cannot remain idle while danger gathers."

⁶⁴¹ Al-Rodhan, Herd, and Watanabe "The Six-Day War and its Consequence" in *Critical Turning Points in the Middle East* (2011) 99; Boudreau "The Bombing of the Osirak Reactor" 1993 10(2) *International Journal on World Peace* 21 21: The 1967 six-day war involving Israel, Jordan, Syria and Egypt; and the 1981 Osiraq bombing carried out by Israel on Iraqi nuclear reactor are instances where Israel has justified its actions based on the principle of anticipatory self-defence.

Some have said we must not act until the threat is imminent. Since when have terrorists and tyrants announced their intentions, politely putting us on notice before they strike? If this threat is permitted to fully and suddenly emerge, all actions, all words and all recriminations would come too late.

The U.S. has been the foremost advocate for a broad approach, as evidenced by the Bush doctrine.⁶⁴² This refers to an approach that embraces the National Security Strategy of the U.S., which overtly acknowledges the right to strike first in an instance where there is a perceived threat to national security.⁶⁴³ This is an overarching interpretation of the self-defence principle, which allows States to protect themselves before an imminent attack materialises. The difference in the use of the term pre-emptive self-defence and anticipatory self-defence has been clarified earlier on pages 49-50. The scope of anticipatory attacks broadly encompasses pre-emptive attacks which entails striking first in order to thwart a budding threat and preventative attacks, which is carried out to neutralise an adversary's capability to seize the opportunity to launch an attack.⁶⁴⁴ The other States such as China, Israel, North Korea, Australia, and Japan have been identified as examples of States who share this broad view of anticipatorily defending against an imminent attack.⁶⁴⁵ Their overt policies reflect their broad interpretation of the concept of self-defence.

For a threat to be considered imminent and necessitating anticipatory self-defence, the attacker must have the intent to attack, the capability to carry out the intended act, and the intended act must be perceptible.⁶⁴⁶ In the Oil platforms case, the U.S. perceived an imminent threat from Iran's action of laying mines in the gulf. Iran act

⁶⁴² Jervis "Understanding the bush doctrine" 2003 118(3) *Political Science Quarterly* 365 365: "The bush doctrine has four elements: a strong belief in the importance of a State's domestic regime in determining its foreign policy...; the perception of preventive war; a willingness to act unilaterally when necessary; and an overriding sense that peace and stability require the United States to assert its primacy in world politics."

⁶⁴³ *Ibid.*

⁶⁴⁴ Mueller, Castillo, Morgan, Pegahi and Rosen *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (2006) 12.

⁶⁴⁵ Bostock "Canberra Would Order Pre-Emptive Strikes" (2002-12-11) *BBC News* .18; Japan "Threatens Force Against N Korea" (2003-02-14) *BBC News* 1.

⁶⁴⁶ *Oil Platforms case* 2003 208 par [101]: "the United States filed a counter-claim, in its Counter-Memorial, against Iran. It explains that its 'counter-claim is based on actions by Iran in the Persian Gulf during 1987-88 that created extremely dangerous conditions for shipping, and thereby violated Article X of the 1955 Treaty"; Letter of Mr. Webster to Mr. Fox (April 24, 1841), in 29 *British and Foreign State Papers*, 1840-41 at 1137-38 (1857): "[u]nder these circumstances, and under those immediately connected with the transaction itself...It will be for that Government to show a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation"; Sadoff "A Question of Determinacy: The Legal Status of Anticipatory Self-Defence" 2009 40 *Georgetown Journal of International Law* 523 530; Reisman and Armstrong "The Past and Future of the Claim of Preemptive Self-Defence" 2006 100 *AJIL* 525, 526.

was seen as posing a danger to vessels, and the U.S. invoked the right to defend against it anticipatorily. While Sadoff emphasizes the demonstration of the capability and intent of the attacker to carry out an imminent attack, Reisman focuses on the victim's perception of the imminent threat. It is submitted that when read together, the victim's perception of imminent threat should be based upon a reasonable assessment of the capability and intent of the attacker. While the capability of an attacker to launch an attack can be overtly manifested through its military strength, the intent behind an attack can be deduced from either preliminary or preparatory acts by the attacker. To implement ASD against MCAA, it is pertinent to understand the criteria a victim should consider to legally determine the imminence of a threat and how to thwart it.

5.2.1. Criteria for Anticipatory Self-defence against MCAA

A State may invoke self-defence (or anticipatory self-defence) if the scale and effect of the consequence (or potential consequence) of MCAA is sufficient to qualify it as an armed attack.⁶⁴⁷ This right comes with a huge responsibility and has the potential of being abused.⁶⁴⁸ What are the criteria for assessing the consequence or potential gravity of an MCAA? The ICJ has not had cause to comment on issues arising from MCAA. Therefore, reliance on an analogy from the ICJ ruling on an armed attack can provide guidance to understand the legal implication of MCAA.

In the Nicaragua case, the ICJ ruled that mere frontier incidents in terms of scale and effect are insufficiently grave to be regarded as armed attack.⁶⁴⁹ When this rationale is applied to cybersecurity, it can be translated to mean that mere cyber intrusions are not serious enough to amount to armed attack. However, in the *Oil Platforms* case, the ICJ held that the mining of a single ship can amount to an armed attack,⁶⁵⁰ but it did not rule that the United States had suffered an armed attack because of the mine incident that was before the court. Scholars have criticised this position.⁶⁵¹ Taft argues that the ICJ's requirement for a certain level of gravity to be reached before

⁶⁴⁷ Rule 71 in Schmitt *Tallinn Manual 2.0* 399.

⁶⁴⁸ Robertson "Self-Defence against Computer Network Attack under International Law" 'Computer Network Attacks and International Law' 2002 76 *International Law Studies* 121 128.

⁶⁴⁹ Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. U.S.*), 1986 I.C.J. 14 par [195].

⁶⁵⁰ *Oil Platforms Case* par [72].

⁶⁵¹ Taft IV "Self-Defence and the Oil Platforms Decision" 2004 29 *Yale Journal of International Law* 295 300; Schmitt "Attack" as a Term of Art in *International Law: The Cyber Operations Context*, in *Proceedings of the 4th International Conference on Cyber Conflict*, 2012 283, 288.

necessitating self-defence can be read to limit the inherent right of States to defend their national interest. This is because while waiting for that level of gravity to be reached and responded to proportionally, a full-scale war can become inevitable.

It is submitted that a flag ship is critical to a State's national interest and States have the inherent right to protect it from all forms of attacks. Based on the ICJ's rationale on armed attack in the *Nicaragua* and *Oil platforms* cases, it can be deduced that the standard for determining the required extent of damage or destruction is unclear and subjective. If mining a ship can qualify as an armed attack,⁶⁵² the mining of international waters should be implied as intent to put all flag ships on that route at risk of suffering an armed attack. Since the weapons that cause armed attacks against flag ships are not limited to mines, the standard for determining the legitimate response to MCAA is open to be debated.

It has been argued that the UN Charter creates a perception of 'attacks' as requiring the use of movable force, which is reasonably foreseeable to lead to destruction.⁶⁵³ Attacks that occur with 'cyber force' move from the attacker's cyberspace to the victim's cyberspace and can lead to elusive cyber destructions may not fit into the original concept of 'attack' as provided for by the charter in article 51. The foreseeability of the destructive physical manifestation of this intangible cyber destruction can be equated to the grave consequence arising from the kinetic force. It is submitted that applying the ICJ's rationale in the *Oil Platforms* case to MCAA without considering the graveness of the physical consequence of the cyber-attack can jeopardise the objectives of upholding maritime cyber security.

Another criterion that must be considered on this subject is attribution. To defend against an attack, it is pertinent to identify the source of the attack. Attribution is relevant in determining the responsibility of a State for carrying out an MCAA. This entails determining whether an imminent MCAA is State-sponsored or beyond the State's control or passively allowed by the State. Some of the questions include whether the attacker State can be held responsible due to an omission or failure to prevent an imminent MCAA, whether the State is directly sponsoring a group or

⁶⁵² *Oil Platforms* par [72].

⁶⁵³ Van De Velde "The Law of Cyber Interference in Elections" 2017 23, SSRN <https://ssrn.com/abstract=3043828> (accessed 2019-04-01).

individuals, and whether the State had control over the occurrence of the imminent attack.

Attribution is a challenging factor in determining the right to use force in ASD against cyber-attacks.⁶⁵⁴ This is because,

While in some cases linking a state to an operation might be possible, most of the time states act through proxies – individuals or other entities – which makes establishing such a link more complicated.⁶⁵⁵

Owing to the unique nature of cyber-attacks, they may not always be conspicuously detectable.⁶⁵⁶ Attribution of an MCAA can be categorised into three: attribution to human, attribution to machine and attribution to State.⁶⁵⁷ Identifying the attacker may be more difficult if his identity is cloaked or passed through multiple operating systems of innocent people.⁶⁵⁸ It has been argued that attribution with complete certainty in cases of cyber-attacks is impossible.⁶⁵⁹ This has been rebutted by Dinstein, who believes that future advancement in the technological capabilities of States will create certainty in linking an attacker to an imminent threat.⁶⁶⁰ This confirms that although it is challenging, attribution is possible. The requirement of technical evidence may be supported by human intelligence reports which validate the certainty of an attacker's identity.⁶⁶¹

Despite using a hybrid intelligence-gathering method, it has been emphasised that timely attribution remains a challenge when a victim needs to defend against an imminent attack anticipatorily. As aptly stated by McCarthy & Russell,

⁶⁵⁴ Silver "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter" 2002 76 *International Law Studies* 73 78.

⁶⁵⁵ Bannelier, Bozhkov, Delerue, Giumelli, Moret, & Van Horenbeeck "Mission Controls: Sanctions under International Law" in *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace* (2019), 45. www.jstor.org/stable/resrep21136.8 (accessed 2020-07-20).

⁶⁵⁶ McCarthy and Russell "Roadmap for a Code of Conduct for Cyberspace" 2017 3 *Fletcher Security Review* 8 10.

⁶⁵⁷ Delerue *Cyber Operations and International Law* (2020) 55.

⁶⁵⁸ Shackelford and Andres 2011 *Georgetown Journal of International Law* 971 981-983.

⁶⁵⁹ Waxman "Cyber-attacks as "Force" Under UN Charter Article 2(4)" 2011 87 *International Law Studies Service US Naval War College* 43, 50; Graham *Journal of National Security Law and Policy* 87 92.

⁶⁶⁰ Dinstein "Computer Network Attacks and Self-Defence" in 2002 *Computer Network Attack and International Law* 99 112.

⁶⁶¹ McCarthy and Russell *Fletcher Security Review* 2017 8 10.

By combining cyber and non-cyber means authorities are developing the means to attribute on-line actors with their real world counterparts. Still, these methods typically take days or weeks, whereas cyber-attacks can be instantaneous.⁶⁶²

Attribution is more difficult in maritime cyberspace when compared with physical or kinetic attacks. The ability of attackers to render attribution inconclusive by creating diversions and cloaking their identity will always leave loopholes of reasonable doubt and plausible deniability.⁶⁶³ States mainly capitalise on these loopholes to evade responsibility for their wrongful acts.

Scholars have explored the effective and overall control tests to hold States strictly responsible for cyber-attacks emanating from their territories.⁶⁶⁴ The extent of control a State-actor has over the launch of an MCAA is relevant in determining State responsibility.⁶⁶⁵ The concept of control refers to the legal relationship between a State and other non-State actors regarding the State's responsibility.⁶⁶⁶ Christenson rightly explains the doctrine of attribution:

Properly understood, the doctrine of attribution in international law serves the purpose of allocating responsibility to the State for the consequences of certain wrongful acts or omissions of its organs and officials. It also defines the sphere of private or non-State conduct for which the State bears no responsibility.⁶⁶⁷

Apart from identifying the instances where States bear responsibility for a wrongful act, the doctrine of attribution also clarifies the unreasonableness of holding a State responsible for a self-sponsored hacker's cyber operations. A State which has effective control over a non-state actor bears responsibility for that actor's wrongful act.⁶⁶⁸ Crawford emphasised this by stating that:

So far as the law of state responsibility is concerned, this determination [the ICJ's Bosnian Genocide decision] effectively ends the debate as to the correct standard of control to be applied under Article 8. Moreover it does so in a manner that reflects the ILC's thinking on the subject from the time the term 'control' was introduced into then-Draft Article 8.⁶⁶⁹

⁶⁶² *Ibid.*

⁶⁶³ Jensen 2002 *Stanford Journal of International Law* 207.

⁶⁶⁴ Payne and Finlay "Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack" 2017 49 *The George Washington International Law Review* 535 563.

⁶⁶⁵ The role of non-State actors has been discussed earlier at page 101.

⁶⁶⁶ Boon "Are Control Tests Fit for the Future? The Slippage Problem in Attribution Doctrines" 2004 15 *Melbourne Journal of International Law* 1 2.

⁶⁶⁷ Christenson "The Doctrine of Attribution in State Responsibility" in *International Law of State Responsibility for Injuries to Aliens* (1983) 321.

⁶⁶⁸ *DRC v Uganda* (2005) 257, para [259-260].

⁶⁶⁹ Crawford *State Responsibility: The General Part* (2013) 156.

Denial by States that they have control over attacks targeting maritime cyber security has created arguments over the supposedly settled issue of control. For instance, how can the effective control of a State over a group of hackers be unequivocally determined? According to Boon:

Alternative techniques for redressing the limited reach of state responsibility have surfaced in response, such as lowering thresholds of control, attributing responsibility for omissions, establishing/developing a duty to prevent certain acts subject to a due diligence obligation and where circumstances and doctrine warrant, recognising shared responsibility between actors.⁶⁷⁰

These techniques have been confirmed as essential tools for addressing the challenge of accountability in international law.⁶⁷¹ These challenges are sometimes borne out of a shift from the State as the sole regulator of cyber activities due to liberalisation and privatisation.⁶⁷² As a result, a State cannot have absolute effective control over cyberspace. For instance, Russia and China often dissociate themselves from cyber-attacks against other States even when most of the evidence points to them. Notwithstanding the challenges associated with attribution, States cannot sacrifice their inherent right of self-defence if it can be reasonably ascertained that the State acted upon the best information available when the imminent threat was perceived.⁶⁷³

5.2.2. Options Available in Self-defence against MCAA

Over the years, States have employed various strategies in defending against cyber-attacks targeting critical cyber infrastructure.⁶⁷⁴ ICT-reliant ships, ports, and oil rigs are run by critical maritime cyber infrastructures that need to be protected from cyber-attacks. While some States have been calmer in responding to these attacks, others have reacted with force (Israel). Notable is the United States' department of defence cyber strategy which demonstrates zero tolerance for cyber-attacks against

⁶⁷⁰ Boon 2004 *Melbourne Journal of International Law* 3.

⁶⁷¹ Hoppe "Passing the Buck: State Responsibility for Private Military Companies" 2008 19 *European Journal of International Law* 989 989.

⁶⁷² Boon 2004 *Melbourne Journal of International Law* 3.

⁶⁷³ Skelrov "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defences Against States Who Neglect Their Duty to Prevent" 2009 201 *Military Law Review* 1, 77-78.

⁶⁷⁴ According to the AU Convention on Cyber Security and Personal Data Protection, critical cyber infrastructure refers to cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyber space.

US interests.⁶⁷⁵ It states that the US would choose the time, place, and manner of response with U.S power's lawful and appropriate instrument.⁶⁷⁶ Scholars have analysed this strategy as being ambiguous.⁶⁷⁷ Hatch argues that:

The value in ambiguity is that an adversary remains challenged in solving a risk vs. benefit calculus equation. If the adversary wonders what their fate might be, it would likely be deterred from launching a cyber-attack.⁶⁷⁸

This ambiguity of a non-definite list of options to be pursued when faced with MCAA gives room for flexibility in choosing anticipatory or real-time responses. The array of options may include the use of military (kinetic) force or cyber force. It has been argued 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.⁶⁷⁹

These options available in self-defence to the victim must comply with the legal requirements prescribed by customary international and the UN Charter. It has been argued that since most cyber-attacks fall below the threshold of an armed attack, other options outside the principle of self-defence can be considered as befitting in response to these attacks.⁶⁸⁰ Such options include retorsion and countermeasures.

One of the options available in self-defence is the use of military force. This refers to the use of weapons by the armed forces of a State such as guns, explosive devices, and other military gear to defend against MCAA anticipatorily or in real time. Recently, Israel bombed Hamas' cyber headquarters while defending against a cyber-attack.⁶⁸¹ Dropping a bomb on a cyber headquarters can neutralise the servers and other computer network operations used to launch a cyber-attack. This

⁶⁷⁵ Hon. Koh, "Remarks at the U.S. Cyber Command Inter-Agency Legal Conference" (18 September 2012), <http://www.state.gov/s/l/releases/remarks/197924.htm> (accessed 2019-08-02).

⁶⁷⁶ DoD Digital Modernization "Strategy 2019 Department of Defence Office of Publication and Security Review" (undated) <https://media.defence.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF> (accessed 2019-08-02).

⁶⁷⁷ Hatch "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits" 2018 11(1) *Journal of Strategic Security* 43 50-51.

⁶⁷⁸ *Ibid.*

⁶⁷⁹ Gill and Ducheine 2013 *International Law Studies* 438, 450.

⁶⁸⁰ Bannelier, Bozhkov, Delerue, Giumelli, Moret, & Van Horenbeeck 'Mission Controls: Sanctions under International Law' in *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace* (2019), 47 www.jstor.org/stable/resrep21136.8 (accessed 2020-07-20).

⁶⁸¹ Cyber Security Maintenance "Israel Responds to a Cyber Attack with Bombs" (10-05-2019) <https://www.cybersecurityintelligence.com/blog/israel-responds-to-a-cyber-attack-with-bombs-4271.html> (accessed 2020-07-31)..

has set a precedent concerning the option of using military force against a cyber-attack. It is submitted that non-cyber measures can be used in response to cyber operations with hostile intent. Kinetic forces such as bombs, and missiles targeted at servers or computer facilities can be used to thwart an imminent disastrous cyber-attack. Also, underwater cables can be cut or destroyed to interfere with the communication system of the attacker.

Not all States may choose this military option in the face of a grave cyber-attack in the marine environment. A victim-State can use cyber force. The narrow act-based interpretation of the concept of armed attack has evolved since the *Nuclear weapons* case upon the realisation that a consequence-based interpretation can accommodate non-kinetic forms of weaponry with the capability of causing grave destruction.⁶⁸² This includes unlawful cyber operations targeting a ship or underwater communication cables. Cyber force as a form of force draws credence from the *Nuclear weapon's* case. It comprises various types of cyber operations to create an adverse effect on the functionality of the adversary's cyberspace on land and at sea.⁶⁸³

Defensive cyber force is more useful when it is carried out proactively instead of reactively.⁶⁸⁴ This is because proactive cyber operations give room for protection against MCAA. It provides an opportunity to discover the adversary's intention and prepare an adequate defence against the imminent threat.⁶⁸⁵ Catie Watt explains a list of steps that can be followed anticipatorily, such as detecting and neutralising windows for cyber espionage; installing and updating codes that prevent malware codes from getting a chance to run; gathering cyber intelligence from the dark web⁶⁸⁶ in order to adequately defend against future attacks; tuning specific software to

⁶⁸² Schmitt "Attack" as a Term of Art in International Law: The Cyber Operations Context, in *Proceedings of the 4th International Conference on Cyber Conflict*. https://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf (accessed 2019-04-01) 283, 287.

⁶⁸³ *Ibid.*

⁶⁸⁴ Insight by KPMG "Moving from Reactive Cyber Security to Proactive Cyber Security: Six Steps to Achieving Prosilience" 29 July 2019 <https://federalnewsnetwork.com/kpmg/2019/07/moving-from-reactive-cyber-security-to-proactive-cyber-security-six-steps-to-achieving-prosilience/> (accessed 2019-07-31).

⁶⁸⁵ *Ibid.*

⁶⁸⁶ The Dark Web refers to the online platform where hackers test their skills and practice to execute future attacks.

swiftly detect and respond by design imminent threats.⁶⁸⁷ Also, the technical usage of remotely controlled 'inventus systems' which have cameras can conduct extensive ocean searches and transmit data to ships or ground stations.⁶⁸⁸ This is a way of protecting ships against possible attacks. Klein explains the importance of submarine surveillance by stating that:

[I]ntelligence gathering at sea has predominantly concerned the pursuit of information that may prove useful for a state's national security. In other words, what does a state need to know about the maritime areas of another state, or what may otherwise be learned about a state (including its defensive or aggressive capacity) from the water surrounding it? This intelligence enables states to make decisions about their own national defence.⁶⁸⁹

Although these suggested proactive steps do not seem like the regular use of kinetic force, they employ cyber weaponry to deter and repel adversaries in maritime cyberspace. The assessment of cyber weaponry and its effect at sea requires criteria that accommodate the unique risks and vulnerability in cyberspace and the marine environment. The UN Charter does not clearly provide for these criteria. It can be implied that States are bound by the obligation of peaceful use of the sea. They should not misuse the right to protect their national security when using technology for maritime surveillance.⁶⁹⁰

Confrontation between ships and aircraft can be justified as anticipatory self-defence where incidents at sea are perceived as armed attack. According to the ICRC commentary of 2016, an international armed conflict can occur even if the actors in the conflict are non-military personnel such as border or coast guards.⁶⁹¹ Where the actor is not a de facto or de jure organ of the State but acts as a private person, that act will not amount to armed attack⁶⁹² necessitating self-defence. In this instance, the option available to the State will exclude anticipatory self-defence.

⁶⁸⁷ Insight by KPMG "Moving from Reactive Cyber Security to Proactive Cyber Security: Six Steps to Achieving Prosilience" 29 July 2019 <https://federalnewsnetwork.com/kpmg/2019/07/moving-from-reactive-cyber-security-to-proactive-cyber-security-six-steps-to-achieving-prosilience/> (accessed 2019-07-31).

⁶⁸⁸ Roell "Maritime Security: New Challenges for Asia and Europe, (November 2011), https://www.files.ethz.ch/isn/134578/167_Roell.pdf (accessed 2019-06-20) 7.

⁶⁸⁹ Klein *Maritime Security and the Law of the Sea* 2011 214-215.

⁶⁹⁰ Lubin "The Dragon-Kings' Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum" 2018 57 *Washburn Law Journal* 17 68.

⁶⁹¹ ICRC Commentary on Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva 12 August 1949, 2nd ed., 2017, Article 2 "Application of the Convention" para 248.

⁶⁹² *Ibid.* para 251.

5.3. Conditions for Anticipatory Self-defence against MCAA

Anticipatory self-defence is an inherent right guided by certain principles to ensure that States invoke it responsibly within the confines of customary international law. A State has an inherent right to respond in self-defence when faced with an armed attack in maritime cyberspace. Harold Koh⁶⁹³ emphasised this right in his speech where he stated that:

A State's national right of self-defence, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.⁶⁹⁴

An imminent threat may be responded to through anticipatory self-defence. This means that a State should not wait to be attacked first to neutralise the impending attack. This assertion derives authority from the *Caroline* case wherein Webster⁶⁹⁵ wrote to Lord Ashburton⁶⁹⁶ stating that the right of self-defence arises when: “necessity of self-defence[is] instant, overwhelming, leaving no choice of means, and no moment of deliberation”.⁶⁹⁷ This statement was affirmed at the Nuremberg Tribunal Judgment⁶⁹⁸ and has since served as a reference for arguments for anticipatory self-defence.

Furthermore, the right of anticipatory self-defence has been explained by Oppenheim as follows:

[T]he use of armed force and the violation of another state's territory, can be justified as self-defence under international law where: (a) an armed attack is launched, or is immediately threatened, against a state's territory or forces . . . (b) there is an urgent necessity for defensive action against that attack; (c) there is no practicable alternative to action in self-defence, . . . [and] (d) the action taken by way of self-defence is limited to what is necessary to stop or prevent the infringement...⁶⁹⁹

Although there is no universally accepted cyber security strategy that permits the use of anticipatory self-defence, States are inclined towards making ambiguous policies that suggest the possibility of anticipatorily defending their interests.⁷⁰⁰ States can

⁶⁹³ A legal scholar and legal adviser of the State Department under President Obama.

⁶⁹⁴ Hon. Koh, “Remarks at the U.S. Cyber Command Inter-Agency Legal Conference” (18 September 2012), <http://www.state.gov/s/l/releases/remarks/197924.htm> (accessed 2019-08-02).

⁶⁹⁵ Daniel Webster, The US Secretary of State during the Caroline incident.

⁶⁹⁶ Daniel Webster's British counterpart.

⁶⁹⁷ *Caroline Case* 1837.

⁶⁹⁸ Nuremberg Tribunal Judgment 435.

⁶⁹⁹ Jennings and Watts (eds.) *Oppenheim's International Law* 9ed. (1992) 422.

⁷⁰⁰ Chayes 2015 6 *Harvard National Security Journal* 474 508.

apply forcible cyber or kinetic measures when faced with large-scale unlawful cyber invasion but must be guided by the requirement of imminence, necessity, and proportionality. Whatever defence option is adopted; States must comply with these legal requirements, which seem interrelated. The necessity to act proportionally in self-defence depends on the imminence of the threat.

5.3.1. The Legal Requirement of Imminence

The principle of imminence refers to the proximity of a threat aimed at violating the territorial integrity or sovereignty of a State.⁷⁰¹ Customary international law interpretation of the concept of imminence is based on the 1837 *Caroline* incident. The conditions of “instant overwhelming, leaving no choice of means, and no moment of deliberation” which act as the basis for ASD may be applied to MCAA. Applying these conditions to the context of MCAA can vary based on a case-by-case analysis since not all maritime cyber-attacks are perceived from the same perspective by States as an armed attack.

There is no universally accepted definition of imminence. Schuller emphasised this by stating that:

While it can perhaps safely be said that the idea of imminence has evolved over time, there is little evidence of any current agreed-upon standards for explaining it.⁷⁰²

In line with its explicit meaning,⁷⁰³ it has been argued that imminence arises when an attack is about to be launched. The Tallinn Manual has criticized this as leaving almost no room to anticipatorily defend against an attack, especially in maritime cyberspace, where an MCAA can be executed with a click of a button.

It has been proposed that the principle of imminence needs to be adapted to modern forms of warfare.⁷⁰⁴ The Bush doctrine asserts that:

[w]e must adapt the concept of imminent threat to the capabilities and objectives of today’s adversaries.⁷⁰⁵

⁷⁰¹ *Caroline case* 1837.

⁷⁰² Schuller “Inimical Inceptions of Imminence – A New Approach to Anticipatory Self-Defence under the Law of Armed Conflict” 2014 18 *UCLA Journal of International Law and Foreign Affairs* 161 170.

⁷⁰³ Merriam Webster “Definition of imminence: Something about to happen, especially an impending danger” <https://www.merriam-webster.com/dictionary/imminence> (accessed 2019-08-28).

⁷⁰⁴ Svarc “Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-first century” 2006 13 *ILSA Journal of International and Comparative Law* 171 186.

This assertion may be applied to the issue of determining an imminent threat, especially in the maritime cyber environment. How can this threat be assessed? How can the adversary's capability be determined in the maritime cyber environment? Will this require an assessment of the adversary's intent? How can the victim know this intent? Is the victim's vulnerability a contributing factor to the determination of imminence? Is the disparity in the victim's perception and the adversary's intent a variable factor that challenges the imminence of a threat?

For an imminent threat to be determined, an armed attack needs to be traced to its source, and the attacker's intent must be 'correctly' ascertained. This can be done by using intrusion detecting systems (IDS) to perceive cyber threats such as malware, ransomware, and other cyber-attacks on the ship and at the ports.⁷⁰⁶ Attribution is crucial in determining imminence. Due to the unique nature of MCAA, it is helpful to assess accumulated maritime cyber intrusions and the existing vulnerability of the victim in determining whether an imminent cyber-attack would trigger anticipatory self-defence. Over the years, the ICJ demonstrated consistency in considering accumulated events as constituting an armed attack.⁷⁰⁷

This implies that a series of cyber espionage operations can be cumulatively viewed as signs of imminent threat.⁷⁰⁸ For instance, cyber espionage can be prospectively harmful though it is not readily acknowledged as an armed attack.⁷⁰⁹ Indeed, an adversary will not be spying without an objective. Each time access is gained into the victim's maritime cyberspace, there are endless possibilities of what the attacker can do with that opportunity within a minimum amount of time.

Access by an attacker to the vulnerability of an ICT-reliant ship can be a red flag to initiate defence. For instance, GPS spoofing, which superficially seems harmless, can cause a disastrous consequence to the navigation system of a ship. A ship's navigation system is a critical operating system of a ship that, if tampered with, has

⁷⁰⁵ Johnson and Lee (eds.) *Law of Armed Conflict Deskbook* (2014) 38.

⁷⁰⁶ United States Coast Guard "Northern California Area Maritime Security Committee Cyber Security News Letter April 2019" (2019-04) https://www.sfmex.org/wp-content/uploads/2019/04/2019-04_AMSC-Cyber-Newsletter.pdf (accessed 2019-09-03).

⁷⁰⁷ *Nicaragua v US* at 231, *DRC v Uganda* 2005 ICJ rep 168 at 146-301 and *Oil Platforms* case 2003 ICJ Rep 16 at 64.

⁷⁰⁸ DeWeese "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence" 2015 *7th International Conference on Cyber Conflict Architectures in Cyberspace* 81 92.

⁷⁰⁹ Remus *Cyber-attacks year* 188.

severe consequences, including the collision of ships, the disappearance of the ship, and loss of lives.

The vulnerability of the computer network of a ship may be detected or created by the adversary. Lin asserts that an attacker can:

persuade vendors or willing employees of those vendors to insert vulnerabilities – secret “back doors” – into commercially available products (or require such insertion as a condition of export approval), by appealing to their patriotism or ideology, by bribing, blackmailing, or extorting them, or by applying political pressure.⁷¹⁰

It can be deduced that the victim can perceive access by an attacker in the form of espionage or exploitation as an imminent attack depending on the victim’s vulnerability. For instance, if the administrative network of a submarine connects at sea to a ship’s operational network, which controls weapons and propulsion, an adversary can seize this blinking opportunity.⁷¹¹ The victim can reasonably envisage an MCAA in this circumstance.

Also, a constant pattern of the previous actions of an attacker can be viewed cumulatively and interpreted as imminence.⁷¹² An increase in the number of times an adversary gains access to a particular ship’s navigation system, communication system, or other crucial ICT-controlled parts of a ship can lead to a high probability in the likelihood of a damaging future consequence stemming from that seemingly harmless espionage.

Consequently, ships should defend themselves from cyber threats that threaten certain maritime operations, especially navigation and communication. Failure to act anticipatorily against cyber intrusions that affect navigation and communication can be hazardous and jeopardise the opportunity to act in self-defence effectively. This creates a platform for adapting the principle of an imminent threat to the capabilities of modern maritime cyber adversaries.

⁷¹⁰ Lin “Offensive Cyber Operations and the Use of Force” 2010 4 *Journal of National Security Law and Policy* 63 66.

⁷¹¹ *Ibid.*

⁷¹² Klaidman *Kill or Capture: The War on Terror and the Soul of the Obama Presidency* (2012) 219-220.

One of the features of MCAA is MCA with potentially violent consequences. The victim can perceive this as an imminent armed attack.⁷¹³ It could be rightly asserted that the victim and not the attacker can only judge the principle of imminence. The victim's assessment of the attacker's intent and destructive capability determines imminence. For instance, the Israeli Defence Force (IDF) destroyed the cyber headquarters of Hamas with an airstrike in response to a cyber-attack that was aimed at "harming the quality of life of Israeli citizens".⁷¹⁴ The victim must reasonably believe that the attacker has decided to conduct the MCAA, and failure to defend the ship anticipatorily will jeopardise the effectiveness of the defence. This resonates with the drafters of the Tallinn Manual, who agreed that:

even if one State has the intent and opportunity to conduct a cyber armed attack against another, the right of the victim State to take forceful defensive measures does not mature until such time as failure to act would deprive the State of its ability to defend itself effectively against the attack.⁷¹⁵

Furthermore, calculation of the likelihood of the success of an attack is one of the factors considered in determining imminence.⁷¹⁶ Hayward argues that:

Thus, when evaluating whether an attack is imminent, a state should consider whether the enemy state can reach the intended target remotely, or locally. All else being equal, a local attack is less likely to be 'imminent' because it is less likely to succeed, and vice versa.⁷¹⁷

Although this assertion might be generally correct, it can be specifically wrong. In certain instances, locally executed attacks such as inserting a USB loaded with malware can cause enormous damage, as was seen in the *Stuxnet* incident. The imminence of a physical breach of a maritime cyber system can sometimes be more accurately perceived and assessed than a remotely triggered one. A remotely triggered MCAA leaves almost no time for perception, attribution of the impending

⁷¹³ Dunlap "Perspectives for Cyber Strategists on Law for Cyberwar" 2011 5(1) *Strategic Studies Quarterly* 81 86.

⁷¹⁴ Gross "IDF says it thwarted a Hamas cyber-attack during weekend battle" (2019-05-05) <https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/> (accessed 2019-08-17).

⁷¹⁵ Schmitt *Tallinn Manual 2.0* 353.

⁷¹⁶ Schmitt "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" 1999 37 *Columbia Journal of Transnational Law* 885 931.

⁷¹⁷ Hayward "Evaluating the 'Imminence' of a Cyber-attack for Purposes of Anticipatory Self-Defence" 2017 117 *Columbia Law Review* 399 430.

attack and effective response in ASD. Also, the type of cyber weaponry will determine the possibility of success either when launched remotely or locally.⁷¹⁸

In addition to the non-universal definition of imminence, state practices are not sufficient to form a legal obligation to abide by specific standards for determining imminence.⁷¹⁹ Notwithstanding, Schmitt notes that applying 'restrictive approaches' to understanding imminence in the face of contemporary threats (such as MCAA) opposes the rationale behind ASD.⁷²⁰ It is submitted that imminence can be perceived when an attack is about to be launched or before a launched attack reaches its target. The former perception seems more realistic than the latter in the context of maritime cyber security due to the swift nature of conducting cyber-attacks and the vulnerability of critical infrastructures in the marine environment. For instance, if malicious software is embedded in the operating system of a ship, it will be more prudent to assess its potential destructive capability and thwart the activation of this malware upon discovering it. Waiting for an MCAA 'to be launched' but acting before it reaches its target seems unrealistic because of the swift nature of cyber-attacks. This can make efforts to anticipatorily defend an attack futile.

5.3.2. The Legal Requirement of Necessity

The provision of Article 51 of the UN Charter presupposes the use of force when acting in self-defence against an armed attack.⁷²¹ This umbrella of self-defence also covers ASD as a subsection. Necessity is one of the prerequisite criteria for lawfully invoking self-defence using force.⁷²² According to the Tallinn Manual,

Necessity requires that a use of force, including cyber operations that amount to a use of force (Rule 69), be needed to successfully repel an imminent armed attack or defeat one that is underway. This does not mean that force has to be the only available response to an armed attack.⁷²³

The principle of necessity entails that:

⁷¹⁸ Svarc "Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-first century" 2006 13 *ILSA Journal of International & Comparative Law* 171 186.

⁷¹⁹ Rockefeller "The 'Imminent Threat' Requirement for the Use of Preemptive Military Force: Is it Time for a Non-Temporal Standard?" 2004 33 *Denver Journal of International Law and Policy* 131 134-135.

⁷²⁰ Schmitt "Preemptive Strategies in International Law" 2003 24 *Michigan Journal of International Law* 513 534.

⁷²¹ Weissbrodt "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347 364.

⁷²² *Nicaragua case* and *Oil Platforms case*.

⁷²³ Schmitt *Tallinn Manual 2.0* 348.

non-forcible remedies must either prove futile in limine or have in fact been exhausted in an unsatisfactory manner.⁷²⁴

It refers to an instantaneous situation that is overwhelming and requires the choice to defend where there is no moment for deliberation. This is a description of the moment a maritime cyber armed attack occurs. It characterises the feature of the swiftness of cyber weaponry. The overwhelming nature of the attack encapsulates the threat, which gives rise to the unequivocal option of launching a defence to thwart the imminent attack leaving no time to negotiate with the attacker. It is submitted that MCAA is the perfect situation that requires ASD because it readily meets the requirement of necessity.

While acting in self-defence, resort to force, whether cyber or kinetic, must be the reasonable option available to thwart an MCAA. This implies that instances where non-forceful acts, whether cyber, economic, or diplomatic, may be sufficient to address an MCAA. Therefore, necessity arises from the insufficiency in the capability of non-forcible measures to thwart MCAAs.⁷²⁵

How can it be determined that certain non-forcible measures will be inadequate to thwart an MCAA? The victim judges necessity and perception of what is required to repel the attack is hinged on reasonableness.⁷²⁶ Therefore, if an attacker decides to end an ongoing MCAA without the victim's knowledge, an act in self-defence deemed necessary by the victim would still be reasonable in the circumstance.⁷²⁷

However, certain cyber-attacks seem to fall below the threshold of an armed attack, but when they are carried out coupled with computer network vulnerability,⁷²⁸ they can necessitate ASD in line with the criteria set out in the *Caroline* case.⁷²⁹ For instance, cyber espionage might not meet the threshold of use of force or armed

⁷²⁴ Dinstein "2002 *Computer Network Attack and International Law* 99, 109; Todd "Armed Attack in Cyberspace: Detering Asymmetric Warfare with an Asymmetric Definition" 2009 64 *Air Force Law Review* 65 98: "Necessity involves whether effective peaceful means of resolution exist the nature of the aggression, each party's objectives, and the likelihood of effective intervention by the international community".

⁷²⁵ Jennings "The *Caroline* and *McLeod* Cases" 1938 32 *American Journal of International Law* 82 89; the requirement of "instant, overwhelming, leaving no choice of means, and no moment for deliberation" as formulated in the *Caroline* case confirms this.

⁷²⁶ Schmitt *Tallinn Manual 2.0* 349.

⁷²⁷ *Ibid.*

⁷²⁸ Vulnerability refers to a part of the system that can be used to interfere in that system as defined in Lin "Offensive Cyber Operations and the Use of Force" 2010 4 *Journal of National Security Law and Policy* 63 65.

⁷²⁹ Weissbrodt "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347 384.

attack⁷³⁰ but when a flagship has some crucial ICT vulnerability that puts the State at immediate risk due to the information acquired by the attacker, use of force can be deemed necessary.

Furthermore, the unwillingness or inability of a State to suppress an imminent threat of MCAA from its territory⁷³¹ can necessitate the use of force in ASD.⁷³² Weissbrodt⁷³³ agrees with Dinstein⁷³⁴ that it is imperative to trace an imminent attack to a specific source whose intention can be perceived as hostile, thereby necessitating the use of force in ASD.

5.3.3. The Legal requirement of Proportionality

The principle of proportionality refers to the requirement that a necessary amount of force, whether cyber or kinetic, must be used when acting in self-defence against an armed attack. According to Rule 72 of the Tallinn Manual:

The criterion limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defence...Therefore a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa.⁷³⁵

The rationale behind this principle is to match the victim's response to the scale of the attack launched by the attacker.⁷³⁶ This is because the intensity of the response should be commensurate and capable of repelling or defeating the attacker. Applying this principle to an MCAA will require a level of precision such that the effect should be felt by the attacker and not by innocent cyberspace users whose cyber infrastructures may have been used by the attacker. This can be very cumbersome

⁷³⁰ Applying the Schmitt approach cyber-espionage would rarely, if ever, trigger the ability to use anticipatory self-defence.

⁷³¹ DoD OGC *An Assessment of International Legal Issues in Information Operations*. 2ed (1999) ; Arlington: Department of Defence, Office of General Counsel available at: <http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc> (accessed 2019-08-15) .

⁷³² Koh, "The Obama Administration and International Law," *American Society of International Law*, (2010-03-25), <http://www.state.gov/s//releases/remarks/139119.htm> (accessed 2019-08-15) on

⁷³³ Weissbrodt "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347 364.

⁷³⁴ Dinstein *Computer Network Attack and International Law* 2002 99, 116.

⁷³⁵ Schmitt *Tallinn Manual 2.0* 349; DoD Manual par [16.3.3.2].

⁷³⁶ Jennings "The Caroline and McLeod Cases" 1938 32 *American Journal of International Law* 82 89.

depending on the type of response, the extent of force they intend to deploy and the incident at hand.⁷³⁷

Suppose the defensive response is non-kinetic such as the use of cyber force. In that case, it can be challenging to precisely target the attacker because information technology interconnects users who share Internet service providers.⁷³⁸ However, if kinetic force is used in response to an MCAA, proportionality might be less difficult to determine due to the overt consequence of the kinetic force used. This is because non-combatants can be excluded through surgical precision of the kinetic force carried out in anticipatory self-defence. This is important because the use of weapons that cannot distinguish between civilian and military targets is prohibited by customary international law.⁷³⁹ States must be mindful to act in accordance with the law.

The assessment of proportionality can be done by matching the scale of the anticipatory act with the intention to create the effect of repelling an imminent attack.⁷⁴⁰ This helps to determine reasonableness and prevents excessive use of force. However, it has been argued that:

The relatively amorphous nature of cyber-attacks further complicates the task of analyzing the magnitude of an initial armed attack to determine a suitably proportionate response.⁷⁴¹

This raises the issue of the challenges that States can face when trying to invoke their right to anticipatory self-defence against MCAAs.

5.4. Challenges of Invoking ASD against MCAA

In the absence of a universally accepted understanding of the definition of anticipatory self-defence (ASD), there is a vacuum that needs to be filled. While

⁷³⁷ Limnell "Proportional Response to Cyberattacks" 2017 1 *Cyber, Intelligence, and Security* 37 49-51.

⁷³⁸ Gjelten "Extending the Law of War to Cyberspace" (2010-09-22) <https://www.npr.org/templates/story/story.php?storyId=130023318> (accessed 2019-03-22) ; given all the indirect effects that might arise from a cyber-attack, victims of MCAA could easily be confounded by the legal considerations of proportionality when acting in self-defence.

⁷³⁹ *Advisory Opinion on the Legality of the Threat and Use of Nuclear Weapons* 1996 ICJ Reports, par [78].

⁷⁴⁰ Randelzhofer "Article 51" in *The Charter of The United Nations: A Commentary* (1994) 661, 662-663.

⁷⁴¹ Payne and Finlay 2017 *George Washington International Law Review* 535, 553.

some scholars⁷⁴² believe ASD and pre-emptive self-defence are similar,⁷⁴³ others see them as differing on the issue of the immediacy of the threat.⁷⁴⁴ Notably, there are various perspectives on invoking ASD lawfully. While some scholars argue that the attack must have been launched,⁷⁴⁵ others believe waiting for the attack to be initiated can rob the victim of the opportunity to repel the attack effectively.⁷⁴⁶ These views are reasonable, but when applied in the context of MCAA, the rationale behind self-defence might be defeated.

The concept of ASD as a subset of self-defence has been discussed above. The legal requirements of imminence, necessity and proportionality have been analysed. During the analysis, it became pertinent that applying the principles of ASD and its legal requirement in repelling MCAA can be challenging in practice. This section will critically analyse the challenges that may arise in complying with the international law principles on ASD in the context of maritime cyber security. The focus will be on the States' expectations to strike a balance between compliance with IMO guidelines and requirements on maritime cyber security on the one hand and the international principles on ASD against MCAA on the other hand. Recommendations will be made to address these challenges in the following chapter.

When States act in ASD against MCAA, they are faced with some challenges. These challenges may be technical or socio-political. They can threaten the efficiency and effectiveness of maritime cyber security. Notably, international law is evolving based on powerful actors whose interpretations of the law affect future practice. Identifying the problems associated with applying international law on self-defence to States' maritime cyber security is a step towards finding solutions.

⁷⁴² Gill and Ducheine 2013 *International Law Studies* 438, 452-53; Gill and Ducheine defined ASD as defensive measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future.

⁷⁴³ *Ibid.*

⁷⁴⁴ Sadoff 2009 *Georgetown Journal of International Law* 523, 530; Reisman states that "those contemplating anticipatory self-defence can point to a palpable and imminent threat." in Reisman & Armstrong "The Past and Future of the Claim of Preemptive Self-Defence" 2006 *100 American Journal of International Law* 525 526.

⁷⁴⁵ Bowett *Self-Defence in International Law* (1958) 187-192.

⁷⁴⁶ US Justice Department White Paper "Lawfulness of a Lethal Operation Directed against a US Citizen Who is a Senior Operational Leader of Al-Qa'da or an Associated Force" (2011) available at <https://fas.org/irp/eprint/doj-lethal.pdf> (accessed 2019-08-17) 7.

5.4.1. Intent and Timeline of Attacker's Act

Determining the intent and timeline of an attacker's act is challenging. How can the timeline for the attacker's decision to activate the malware or click the button to initiate an attack be determined? Why is it important to determine intent and timeline of the attack? This is important for the purpose of meeting the requirements of article 51 of the UN Charter. The victim-State must perceive the threat of an armed attack to be able to lawfully use force in self-defence. Determining the intent and timeline of an attack helps the victim State to assess and understand the threat posed by the attack through risk assessment.⁷⁴⁷ Subsequently, an appropriate response to thwart the attack can be put together. At what point can an attacker's act be perceived as imminent? The onus is on the victim-State to discharge the burden of proving the evidence of the perceived imminence. In some cases, when States remain neutral by not condemning an action taken by another State in self-defence, it can be interpreted as approval or a reflection of their position on the issue.⁷⁴⁸ This proof must be strong enough to pass any scrutiny by the Security Council. This is an onerous task, especially when justifying the 'the last window of opportunity to repel attack'.

Applying the "last window of opportunity to effectively repel attack" approach to an MCAA might be exigent. This is one of the challenges of determining the imminence of an attack in maritime cyberspace. It could be done through either verified human or cyber intelligence or both. However, kinetic attacks tend to allow for more time to gather these intelligence reports instead of cyber-attacks, which are mostly planned in the shadows and sometimes inferred from the dark web.

According to Robertson,

The difficulty with the application of this principle is in determining that in fact an attack is imminent. In the case of an attack by kinetic means, there are usually (but certainly not always) intimations of an impending attack. Some may be ambiguous...others may carry a clearer threat-movement of troops to the border...⁷⁴⁹

⁷⁴⁷ Zimmerman *Ten Strategies of a World-Class Cybersecurity Operations Center* 2014 252.

⁷⁴⁸ For instance, when the Israeli Defence Forces bombed Hamas' cyber headquarters, no country issued a statement of condemnation.

⁷⁴⁹ Robertson "Self-Defence against Computer Network Attack under International Law" in *Computer Network Attacks and International Law* 2002 76 *International Law Studies* 121 138.

Other times, cyber-attacks are discovered in real-time. This leaves the victim with the only option of making a quick assessment of the probable intent of the adversary and repelling it effectively. For instance, the IDF bombed the cyber headquarters of Hamas after assessing that the impending cyber-attack would jeopardise the quality of life of Israeli citizens, as stated by the spokesperson of the IDF.

It has been argued that cyberweapons capable of causing an imminent armed attack are usually highly customised to a specific target.⁷⁵⁰ This can give a victim with high technological capability, a better chance to detect this attack in the planning and development phase due to the intensive resources required to build the weapon.⁷⁵¹ Many States do not have advanced technological capacity. Therefore, not all States can make correct reasonable 'imminent threat assessment'. The reasonable assessment based on their technological capacity and other factors creates an ambiguity concerning what is a reasonable perception of imminent threat.

Notwithstanding, cyber weaponry is evolving quickly with attackers making improvements on cloaking their identity and surprising their victims. The element of surprise makes gauging the timeline of the attacker's actions to determine the best defence against the incoming MCAA impracticable. Libicki summarily explains the issue associated with assessing the intent of the cyber attacker by stating that:

Cyber operations lack precedents or much expressed declared intent to fall back on, and the normal human intuition about how things work in the physical world translates poorly into cyberspace. Because their effects and sometimes even their existence are not directly visible, the nature and ramifications of cyberoperations begs for explanation—generally by the target. Even the source of the attacks may be unclear and have to be claimed by the attacker or assigned by the defender.⁷⁵²

States find it difficult to attribute an intended threat and efficiently execute processes to anticipatorily defend against MCAA. In the light of the unique speed with which cyber-attacks occur coupled with the vulnerabilities of the marine environment, there is limited time for efficient assessment of the intent of the attacker. Waiting for a cyber-attack to overtly manifest certain features for it to potentially qualify as MCAA before acting is likely to guarantee that the victim will not escape from various degrees of damage to their maritime cyberspace.

⁷⁵⁰ Hayward "Evaluating the 'Imminence' of a Cyber-attack for Purposes of Anticipatory Self-Defence" 2017 117 *Columbia Law Review* 399 421.

⁷⁵¹ *Ibid.*

⁷⁵² Libicki *Crisis and Escalation in Cyberspace* (2012) 39.

Furthermore, there is the challenge of determining the intent of the attacker. Lin depicts this by stating that:

When it is discovered that something is happening, the target of an offensive cyber operation is not likely to be able to distinguish between an offensive cyber operation that seeks to cause large-scale damage (a cyber-attack that would almost certainly constitute an armed attack) and one that seeks to cause only very limited damage (a cyber-attack that might constitute a use of force but not an armed attack).⁷⁵³

In maritime cyber space, the intent of the attacker might be ambiguous and difficult to ascertain. The onus is on the victim to determine whether an MCAA is imminent and intended to cause extensive damage. Despite this inevitable uncertainty, a victim needs to reasonably envisage the probable intent of the attacker through cyber-espionage without giving an impression of hostility.⁷⁵⁴

Despite espionage being viewed by most scholars as harmless and beneath the threshold of an armed attack; in cyberspace, it should be perceived as a grave preliminary attack, invasion, or intrusion from which devastating consequences can arise. When an attacker gains non-consensual access through a systematic and calculated means into the operating system of a ship, it can be implied or reasonably speculated that he or she intends to alter or damage critical infrastructures on the ship. Some States, such as the US, have policies that seem to be more stringent in determining an attacker's intent.⁷⁵⁵ Their broad approach acknowledges the gravity of cyber espionage, and they understand the probable destructive consequence that can stem from it.

Cyber espionage in the maritime space should not be underestimated but viewed as a red line for invoking ASD. This can seem questionable, but it is important given the high vulnerability of ships that rely on information technology for their navigation system, cargo holding, communication system. It is a colossal decision-making burden requiring a high degree of discretion given to individuals to reasonably perceive an attacker's hostile intent.⁷⁵⁶ For instance, only the attacker knows when he or she wishes to remotely activate malware embedded in the operating system of

⁷⁵³ Lin "Offensive Cyber Operations and the Use of Force" 2010 4 *Journal of National Security Law and Policy* 63 83.

⁷⁵⁴ Buchanan *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (2017) 5.

⁷⁵⁵ Lt. Col. W.A. "Stafford How to Keep Military Personnel from Going to Jail for Doing the Right Thing: jurisdiction, ROE & the Rules of Deadly Force" (2000-11-05) http://www.au.af.mil/au/awc/awcgate/law/roe_deadlyforce.pdf (accessed 2019-09-02).

⁷⁵⁶ Solis *The Law of Armed Conflict* (2010) 506.

a ship. The victim may not know the extent of damage an attacker wishes to cause. So, the post-exploitative activities of an attacker can only be speculated by the victim, although the attacker knows it. The victim's risk assessment of the attacker's capability depends on many factors, including its computer network vulnerability.

This may not accurately reflect the attacker's intention. The victim needs to defend itself based on the possible destructive consequence that is reasonably likely to occur if the attacker is not repelled or defeated.

5.4.2. Application of the Legal Requirements of Anticipatory Self-Defence to MCAA

The conventional legal framework for ASD tends to lose focus on the intended objective of self-defence when literally applied to MCAA. The legal requirements of necessity, proportionality and imminence were forged in the context of kinetic attacks. The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Act reflects the customary international law requirements of necessity, imminence, and proportionality by permitting the use of force when it:

is the only way for the State to safeguard an essential interest against a grave and imminent peril; and 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...⁷⁵⁷

This implies that the use of force is permitted to repel threats against maritime security including cyber security which threaten lives and can cause grave or irreversible damage to the marine environment especially at offshore oil rigs. A realist's approach will be used to assess the implementation of these legal requirements in the context of maritime cyber security.

The element of imminence has mainly been analysed as the most vacillating of them all.⁷⁵⁸ It has been argued that applying the doctrine of preemption based on perceived imminence of MCA tends to lead to a preventive defence which seems difficult to implement in international law.⁷⁵⁹ The difficulty mainly stems from the

⁷⁵⁷ Article 25 ILC's Draft Articles on the Responsibility of States for Internationally Wrongful Acts, 2001.

⁷⁵⁸ Svarc 2006 *ILSA Journal of International and Comparative Law* 171, 182.

⁷⁵⁹ Sklerov 2009 *Military Law Review* 1 6.

timely and correct perception of the imminence of an attack.⁷⁶⁰ When applied to MCAA, it could challenge the legality to act in self-defence against an attack. This is because the criteria for passing the tests of necessity, proportionality and imminence for kinetic attacks may not be or appear reasonable when applied in defending maritime cyberspace. It is submitted that legal guidance on issues relating to ICT and IT in maritime security has a lacuna that needs to be filled.

The law seems to be evolving at a languid pace compared to the speed of technological advancement. There are no restrictions or limits to innovation on cyber operations. Conversely, victims of MCAA might seem powerless to act while trying to fit into the box of restrictive interpretation for legitimacy. For instance, it has been argued that:

It is unlikely an Iranian response would meet the requirements of necessity, proportionality, and immediacy, therefore, an armed response to Stuxnet would not be lawful.⁷⁶¹

This view was analysed by the drafters of the Tallinn Manual, where they elucidated the accompanying challenges with applying the existing *jus ad bellum* principle of international law.⁷⁶² More specifically, they debated about whether the consequence of harm to persons and physical damage to property should justify using force in self-defence. Some argued that:

it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects...illustrating this division of opinion in a cyber incident directed against a major international stock exchange that causes the market to crash...⁷⁶³

While some experts argued that a market crash would not legitimise ASD since it would not qualify as an armed attack, others argued that the catastrophic consequence of a market crash can qualify it as an armed attack.⁷⁶⁴ Also, a third

⁷⁶⁰ Under customary international law, the concept of imminence as reflected in the 1837 *Caroline* incident occurs within the conditions of “instant overwhelming, leaving no choice of means, and no moment of deliberation”. British troops invaded the U.S. territory and destroyed the steamboat *Caroline* in 1837. This incident led to the formulation of conditions to be fulfilled for the justification of the British violation of U.S. territorial sovereignty and which still form the basis for the customary principles governing the issue of self-defence in international law. The application of these conditions to the context of MCA may vary based on a case-by-case analysis since not all cyber-attacks are perceived from the same perspective by States.

⁷⁶¹ Weissbrodt “Cyber-Conflict, Cyber-Crime and Cyber-Espionage” 2013 22 *Minnesota Journal of International Law* 347-378.

⁷⁶² Schmitt *Tallinn Manual 2.0* 342-348.

⁷⁶³ Schmitt *Tallinn Manual 2.0* 342-343.

⁷⁶⁴ *Ibid.*

section argued that a cyber-attack on the critical infrastructures of a State with severe, but not destructive effects can legitimise ASD.⁷⁶⁵ These competing views showcase the challenge of determining the universally accepted criterion for ascending to the threshold of armed attack. Applying the analysis to maritime cyber security further complicates the debate on what qualifies as an armed attack. It is reasonable to argue that the catastrophic consequence of an MCAA is a justification for anticipating it and defending against it.

To understand the complexity of imminence, a comparative analysis may be drawn regarding the U.S drone strike that killed Qasem Soleiman in January 2020. The President of the U.S at that time justified the drone strike by stating that:

Soleimani was plotting imminent and sinister attacks on American diplomats and military personnel but we caught him in the act and terminated him.⁷⁶⁶

This perception of imminence of an attack necessitating anticipatory self-defence has been criticised as being unlawful.⁷⁶⁷ These conflicting perspectives on the perception of anticipatory self-defence exhibit the real challenge associated with applying the invoking anticipatory self-defence against MCAA. Schmitt argues that when a cyber operation is the first part of a larger attack, such as taking down the airspace defence system of a State, it can be rightly inferred as an armed attack necessitating self-defence. He acknowledges the challenge of determining imminence in cyberspace but advocates for the reasonableness of the victim's perception of an imminent attack.⁷⁶⁸

The customary international law on self-defence provides for the normative requirement of proportionality. Applying this to maritime cyber security creates a unique challenge. A cyber response to an impending MCAA can have its

⁷⁶⁵ *Ibid.*

⁷⁶⁶ Hosenball "Trump says Soleimani plotted 'imminent' attacks, but critics question just how soon" (2020-01-04) <https://www.reuters.com/article/us-iraq-security-blast-intelligence/trump-says-soleimani-plotted-imminent-attacks-but-critics-question-just-how-soon-idUSKBN1Z228N> (accessed 2020-01-07).

⁷⁶⁷ Stephanie Nebehay "U.N. expert deems U.S. drone strike on Iran's Soleimani an 'unlawful' killing" <https://www.reuters.com/article/us-usa-iran-un-rights-idUSKBN2472TW> (accessed 2020-07-06); <https://www.aljazeera.com/news/2021/6/17/us-congress-chips-away-at-law-used-to-justify-soleimani-strike> (accessed 2021-06-17).

⁷⁶⁸ Schmitt "Cyber Operations and the *Jus ad Bellum* Revisited" 2011 56(3) *Villanova Law Review* 569 589-590.

advantages; it can also pose serious challenges to the principle of proportionality.⁷⁶⁹ Since the principles of necessity and proportionality are intended to ensure that reasonable and non-excessive force is used,⁷⁷⁰ how can this be determined when cyber weaponry is used? In the *Legality of the Threat or Use of Nuclear Weapons*, the ICJ stated that in exercising the right of self-defence,

Respect for the environment is one of the elements that go to assessing whether an action is in conformity with the principles of necessity and proportionality.⁷⁷¹

It is submitted that acts carried out in ASD, whether through cyber or kinetic force, need to respect the cyber and marine environments.

In line with the objectives of ASD, if a victim-State wants to thwart an imminent threat, its action must be intended to effectively thwart the imminent threat and prevent the threat from being re-launched. This can be achieved using cyber weaponry or kinetic force, such as dropping a bomb on the attacker's server. The principle of proportionality seeks to ensure that a defensive measure targeting the attacker is commensurate to the reasonably foreseeable damage the imminent threat can have caused.⁷⁷²

It also requires distinguishing the attacker's network from civilian networks even when botnets are being used.⁷⁷³ Harold Koh asserts that proportionality in the cyber context must consider certain factors:

... (1) the effects of cyber weapons on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians; (2) the potential physical damage that a cyber-attack may cause, such as death or injury that may result from effects on critical infrastructure; and (3) the potential effects of a cyber-attack on civilian objects that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are military objectives.⁷⁷⁴

⁷⁶⁹ Roberts "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors" 2014 41 *Northern Kentucky Law Review* 535 552.

⁷⁷⁰ Newton and May *Proportionality in International Law* (2014) 2.

⁷⁷¹ *Legality of the Threat or Use of Nuclear Weapons* ICJ Reports, 1996, 226, 242.

⁷⁷² Schaap "Cyber Warfare Operations: Development and Use Under International Law" 2009 64 *Air Force Law Review* 121 156–57: "First, the target must make an effective contribution to the enemy's military action. Second, its destruction must provide a definite military advantage to the attacker."

⁷⁷³ Eric "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners" 2017 50 *Vanderbilt Journal of Transnational Law* 217 230.

⁷⁷⁴ Hon. Koh, "Remarks at the U.S. Cyber Command Inter-Agency Legal Conference" (2012-09-18), <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> (accessed 2019-05-18).

In theory, these factors are ideal and conform with international law standards. This can be complicated to consider. The difficulty lies in the empirical assessment of the circumstance. As stated by Dinniss:

Some systems initially designed for military use have become so integrated into civilian society that any interference or disruption caused by computer network attacks would have serious effects on civilians.⁷⁷⁵

It is submitted that the immeasurable collateral damage to civilian networks makes it problematic for MCAA in ASD to pass the proportionality test perfectly.⁷⁷⁶ When acting in ASD, a victim-State cannot always determine the exact consequence of a launched cyber defensive measure.⁷⁷⁷ Sometimes, the pathway used by cyber-attackers cuts through different jurisdictions. The victim State's response in self-defence will be reasonable if the physical consequence of the cyber-attack is manifested in its jurisdiction.⁷⁷⁸

Also, Lin argues that there is:

the inconsistency between economic sanctions, avowedly not a use of force and thus an entirely permissible unilateral action under the U.N. Charter, and blockades, avowedly a use of force and thus a violation of Article 2(4) ...

When naval blockades occur using maritime cyber operations in response to an MCAA, it can appear to be a legitimate use of force in ASD. On the contrary, the use of cyber operations that provide similar effects, such as economic sanctions, will not qualify as the use of force. MCAA can result in enormous damage to property at sea and seriously affect the shipping industry, a loss that can be valued economically in the form of millions of dollars. For instance, the recent maritime insecurity facing ships in the Strait of Hormuz has attracted the joint effort of Australian, UK, Bahrain, and US forces to ensure safe passage of ships.⁷⁷⁹

Although these are not cyber operations, it can be deduced that the economic threat to the oil tankers being shipped through the Strait of Hormuz has been perceived as

⁷⁷⁵ Dinniss *Cyber Warfare and the Laws of War* (2012) 194.

⁷⁷⁶ Eric (2017) *Vanderbilt Journal of Transnational Law* 217 232-233.

⁷⁷⁷ Fenton III "Proportionality and its Applicability in the Realm of Cyber-Attacks" 29 2019 *Duke Journal of Comparative and International Law* 335 352: "Stuxnet was never intended, nor expected to spread beyond the nuclear facility at Natanz. Nevertheless, the malware infected an Internet-connected computer and began to spread uncontrollably outside the facility".

⁷⁷⁸ Schmitt "Cyber Operations and the *Jus ad Bellum* Revisited" 2011 56(3) *Villanova Law Review* 569 590.

⁷⁷⁹ Aljazeera "Australia Joins US-led Naval Mission in Strait of Hormuz" (2019-08-21) <https://www.aljazeera.com/news/2019/08/australia-joins-led-naval-mission-strait-hormuz-190821071113310.html> (accessed 2019-08-21).

an imminent threat that needs to be tackled with the use of force. This inconsistency, when applied in cyberspace becomes more complex.⁷⁸⁰ A comparative assessment of the real threat in marine cyber space and kinetic space shows a significant disparity in substance and form.⁷⁸¹ For instance, a cyber-attack that tampers with the GPS of a ship can be dismissed as a threat superficially unless the grave technical implication of the consequence of such an attack is understood and appreciated.⁷⁸² MCAA need unique legal requirements that will not arm-twist a victim into suffering an attack that could have been repelled or defeated only if the legal requirements were more suitable for addressing threats in the maritime cyberspace. The *jus ad bellum* principles need to be adapted to suit the unique nature of the maritime cyber conflict.

Agreeably, some scholars suggest that for the requirement of imminence to be effectively satisfied, it should not be strictly qualified within a specific time frame. However, its narrow interpretation should be expanded to consider other factors that may collectively point towards imminence and necessity by extension.⁷⁸³ Totten argues that:

it is now plausible to imagine a situation where a state has exhausted all reasonable alternatives outside the use of force to secure the legitimate end of self-defence, but the threat is not imminent, as narrowly conceived.⁷⁸⁴

Adapting these legal requirements to the era of modern technology and non-conventional threats (such as MCAA) requires a unique set of factors to effectively determine, in each case, when the standards of imminence, necessity and proportionality have been met. These factors can include the sophistication of the maritime cyber weapon, the maritime cyber strength of the attacker, the vulnerabilities of the victim and the potential damage that could occur to lives and properties in the marine environment. They must be viewed in line with the objective of attaining efficient and effective maritime cyber security.

⁷⁸⁰ Lin 2010 *Journal of National Security Law and Policy* 63 84.

⁷⁸¹ Lund, Hareide, and Jøsok "An Attack on an Integrated Navigation System" 2018 3(2) *Necesse* 149 161.

⁷⁸² *Ibid.*

⁷⁸³ Totten "Using Force First: Moral Tradition and the Case for Revision" 2007 43 *Stanford Journal of International Law* 95 109; Rockefeller 2004 *Denver Journal of International Law and Policy* 131 144; Schmitt 'Responding to transnational terrorism under the Jus ad Bellum: A Normative Framework'. In *International Law and Armed Conflict: Exploring the Faultlines* (2007) 170.

⁷⁸⁴ Totten "Using Force First: Moral Tradition and the Case for Revision" 2007 43 *Stanford Journal of International Law* 95 96.

5.4.3. Secrecy Surrounding MCAA Reports

In addition to the above challenges, cyber-attack victims tend to withhold information concerning the nature and target of an attack. It was reported that:

organisations...may not be required to or even want to disclose the attack, as many fear reputational damage from doing so. It is this lack of reporting that is providing a false sense of security within the maritime industry.⁷⁸⁵

When ships experience cyber-attacks, not all the incidents are reported. These reports can be done manually or automatically using suitable data models.⁷⁸⁶ Alerts from security and network monitoring systems and analysis of log information from devices are sources for reporting maritime cyber security incidents.⁷⁸⁷ Many shipping companies keep these incidents in-house away from outside observers for different reasons. Some try to deal with these issues quietly to prevent further economic losses or losses to their reputation.⁷⁸⁸ The rationale behind this decision can be rooted in the fact that insurance companies do not cover maritime cyber security losses.

There are instances where that incident is made public, but the details of the nature of the attack and the target of the offensive remain classified. Notably, when the IDF bombed the cyber headquarters of Hamas, it did not give details about the nature and target of the cyber-attack that Hamas launched. It was reported by the media that:

The military said much of the information about the attempted attack cannot be published as it might reveal to Hamas details of about Israel's cyber capabilities.⁷⁸⁹

There is a sense of patriotic interest that supersedes the desire for public knowledge about the details of the attack. This secrecy can be due to the need to protect the State's cyber security capability and consideration for the political impact of their

⁷⁸⁵ Furness-Smith "Maritime industry must open up about cybercrime" (2019-08-12) <https://loydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime> (accessed 2019-09-03) .

⁷⁸⁶ Danyliw "The Incident Object Description Exchange" (2016-11), <https://tools.ietf.org/html/rfc7970> (accessed 2019-12-03) 172.

⁷⁸⁷ Tøndel, Line, and Jaatun "Information Security Incident Management: Current Practice" (undated) 42–57. <http://www.sciencedirect.com/science/article/pii/S0167404814000819> (accessed 2019-12-03).

⁷⁸⁸ Ezekiel "Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft" 2013 26(2) *Harvard Journal of Law and Technology* 649 653.

⁷⁸⁹ Gross "IDF says it thwarted a Hamas cyber attack during weekend battle" (2019-05-05) <https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/> (accessed 2019-08-17)..

allegations.⁷⁹⁰ However, this might be exploited to exaggerate the imminence of a threat, the necessity for use of force and a miscalculation of proportionality.

5.4.4. Technology Capacity for Early Detection of MCAA

Failure to detect an impending MCAA can be disadvantageous to the victim. Some types of dangerous cyber operations such as the *Stuxnet* worm may not be initially perceptible until their destructive consequences begin to manifest and are identified.⁷⁹¹ A victim who suffers this type of cyber-attack is already a step behind the attacker. Defending against such an attack anticipatorily becomes nearly impossible. This is because the attacker may be detected or identified only after the consequences of such cyber-attacks manifested⁷⁹² in the form of damages to the ship's navigation or communication systems which are crucial systems of the ship. Due to the swift nature of cyber-attacks, often, there is minimal time between the launching of an attack and when a target is hit.⁷⁹³

Consequently, a unique standard for determining imminence, necessity and proportionality is required to defend against MCAA effectively. Identification of imminence can be made during the planning and development phase.⁷⁹⁴ This might create a better chance at thwarting an incoming MCAA. For instance, the US launched a program with the capability:

to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants...⁷⁹⁵

In 2018, the Cybersecurity and Infrastructure Security Agency Act was enacted. This significant legislation created the Cybersecurity and Infrastructure Security Agency which has the following mandate:

coordinates security and resilience efforts using trusted partnerships across the private and public sectors and delivers technical assistance and assessments to

⁷⁹⁰ Czosseck "State Actors and their Proxies in Cyberspace" in *Peacetime Regime for State Activities in Cyberspace: International Law*, (2013) 21.

⁷⁹¹ Schmitt *Tallinn Manual 2.0* 354.

⁷⁹² Schuller "Inimical Inceptions of Imminence: A New Approach to Anticipatory Self-Defence Under the Law of Armed Conflict" 18 2014 *UCLA Journal of International Law and Foreign Affairs* 161 200.

⁷⁹³ Hayward "Evaluating the 'Imminence' of a Cyber-attack for Purposes of Anticipatory Self-Defence" 2017 117 *Columbia Law Review* 399, 418.

⁷⁹⁴ Hayward 2017 *Columbia Law Review* 399, 419.

⁷⁹⁵ Gorman "U.S. Plans Cyber Shield for Utilities, Companies" Wall Street Journal (2010-07-08) <https://www.wsj.com/articles/SB10001424052748704545004575352983850463108> (accessed 2019-08-26).

federal stakeholders as well as to infrastructure owners and operators nationwide.⁷⁹⁶

This technical capacity signifies the ability of the US to tackle cyber security issues. This is a recent standard which many countries have not yet attained. Applying this standard will leave the victim constantly disadvantaged and seldom able to lawfully defend the critical maritime infrastructure against cyber armed attacks. Notwithstanding, the Security Council can invoke its authority pursuant to its duty to maintain international peace and security⁷⁹⁷ to alleviate the unjust position victims may find themselves due to the modern standard.

Another issue is the use of artificial intelligence (AI) in cyber-attack and cyber defence. When cyber-attackers use AI, it is intended to:

(1) make cyber-attacks more insidious, disruptive, and long-lasting; (2) reduce the effectiveness of conventional defensive measures; and (3) make powerful attacks more accessible for the median malicious online actor... AI portends unprecedented adaptability, rapidity, and opportunity for unexpected malicious behavior than has previously been the case.⁷⁹⁸

When used in defence, AI can be used as a tool to reliably detect imminent threats, assess the potential damage that could be caused and defuse the threat immediately before a vulnerability is exploited. AI can be used to carry out an attack anonymously and more discretely. As much as this technology is helpful for the early detection of an imminent attack, it can also be used to develop more complex threats.⁷⁹⁹ Ramachandran explains that:⁸⁰⁰

As technology evolves, the adversaries are also enhancing their attack methods, tools, and techniques to exploit individuals and organizations. There's no doubt that Artificial Intelligence is incredibly useful, but it is somewhat of a double-edged sword.⁸⁰¹

Some of the abilities of AI include behavioural analysis of an attacker's pattern of online activities, gathering network security intelligence, identifying possible

⁷⁹⁶ Cybersecurity and Infrastructure Security Agency "Infrastructure Security" (undated) <https://www.dhs.gov/topic/critical-infrastructure-security> (accessed 2020-10-23).

⁷⁹⁷ Chapter VII of the UN Charter.

⁷⁹⁸ Whyte "Poison, Persistence, and Cascade Effects: AI and Cyber Conflict" 2020 14(4) *Strategic Studies Quarterly* 18 23.

⁷⁹⁹ Ramachandran "How Artificial Intelligence is Changing Cyber Security Landscape and Preventing Cyber-attacks" (2019-09-14) <http://www.entrepreneur.com/article/339509> (accessed 2019-09-16).

⁸⁰⁰ Remesh Ramachandran is a security researcher and an ethical hacker.

⁸⁰¹ Ramachandran "Entrepreneur India" <http://www.entrepreneur.com/article/339509> (accessed 2019-09-16).

pathways an attacker could use to target the vulnerabilities in the operating system of a ship, and detecting cyber threats before vulnerabilities are exploited.⁸⁰²

5.4.5. Attribution

Attribution of a State's responsibility for the breach of an international obligation plays a crucial role in determining the requirements of necessity, proportionality, and imminence. Identifying an adversary is the first step in determining liability for armed attack, which is a breach of an international obligation, and the appropriate reaction to address it.⁸⁰³ An internationally wrongful act of a State occurs when a conduct consisting of an action or omission is attributable to the State under international law and it constitutes a breach of an international obligation of the State.⁸⁰⁴ An act can be unlawful within a State but not may not violate an international obligation.⁸⁰⁵ Determining the lawfulness of a State's conduct in practice can be difficult despite the provisions of the Draft Articles of State Responsibility for Internationally Wrongful Act (ARSIWA) of 2001.

This difficulty can be seen in the 2011 judgment concerning the case of *Nuhanovic v The Netherlands*,⁸⁰⁶ where the Court of Appeal provided a clear jurisprudential affirmation of the concept of effective control in determining State responsibility by overturning the decision of the District Court of the Hague. By ruling that the conduct of Dutchbat, UN peacekeeping force UNPROFOR, in Srebrenica, was attributable to the Netherlands, the Court of Appeal established that the concept of effective control

⁸⁰² *Ibid.*

⁸⁰³ Chayes 2015 *Harvard National Security Journal* 474 486.

⁸⁰⁴ Article 2 of the Articles of State Responsibility for Internationally Wrongful Act (ARSIWA) of 2001.

⁸⁰⁵ Article 3 of ARSIWA 2001.

⁸⁰⁶ *Gerechtshof's-Gravenhage, Nuhanovic v The Netherlands*, Judgment LjN: BR 5388 (5 July 2011) ('*Nuhanovic Court of Judgment*'): On 11 July 1995, after the Bosnian Serb armed forces took control of the "safe area", thousands of Bosnian Muslims sought refuge at the UN compound. On 13 July, while outside the compound men were being killed and abused, the Dutchbat command decided to expel from the compound three Bosnian Muslims, including a UN interpreter. They were subsequently killed in the Srebrenica massacre. The families of these three victims sued the Netherlands for its alleged responsibility for the events. On 10 September 2008 the District Court of The Hague dismissed the claims, considering that Dutchbat were operating under a UN mandate in Bosnia and did not have the operational command and control of the area, which was in the hands of the UN. However, on 5 July 2011, in an unprecedented ruling, the Court of Appeal overturned this decision, recognizing that in this case, there was dual responsibility between the UN and Dutchbat which implied a shared effective control over the same wrongful conduct. Therefore, the Dutch government was found responsible for what happened to the three Bosnian Muslims.

entails giving orders and having the capacity to prevent the wrongdoing.⁸⁰⁷ This decision was affirmed by the Supreme Court.⁸⁰⁸

Based on the judgment in the *Nuhanovic* case, it can be implied that when a cyber-attack comes from a vessel under charter or flagged in an open registry State, the effective control by the flag State is presumed over the flagged vessel. In the context of maritime cybersecurity, attribution is a more challenging task which has been described as:

an insoluble technical problem with current network protocols. In this vision of the cyber environment, individuals or groups can “spoof” their identities and the location of their computers on the network.⁸⁰⁹

Attribution in the cyberspace of marine environment may not occur through the same mechanism as obtainable in a physical military attack. It appears to be more challenging in maritime cyberspace. While some experts view timely attribution to thwart a cyber-attack as technically challenging,⁸¹⁰ others view it as a policy challenge.⁸¹¹ This is due to several factors, including hackers’ ability to act swiftly and cloak their identity by routing their cyber operations through computer networks of innocent people.⁸¹² Another factor is the marine location of these ICT-reliant ships. Investigation at sea might be restrictive, especially if the impending threat targets the ship's communication system.

The anonymous feature of maritime cyber-attack poses a major threat to the effective implementation of ASD mechanisms.⁸¹³ Geer emphasises this by stating that:

⁸⁰⁷ Dannenbaum “Killings at Srebrenica, Effective Control, and the Power to Prevent Unlawful Conduct” (2012) 61(3), *The International and Comparative Law Quarterly* 713 715; https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/caseLaw.xsp?documentId=DD1F57EC48A29629C1257D250050B800&action=openDocument&xp_countrySelected=NL&xp_topicSelected=GVAL-992BUA&from=state&SessionID=DZM89NQJK2 accessed on 4th March, 2022.

⁸⁰⁸ The State of Netherlands v. Hasan Nuhanovic, 12/03324, Supreme Court, 06 September 2013.

⁸⁰⁹ Yannakogeorgos “The Cyber Environment” in *Strategies for Resolving the Cyber Attribution Challenge* (2013) 9-34.

⁸¹⁰ Libicki *Cyberdeterrence and Cyberwar* 2009 44.

⁸¹¹ Healey “The spectrum of national responsibility for cyberattacks” 2011 18(1) *The Brown Journal of World Affairs* 57 60; Kanuck “Sovereign Discourse on Cyber Conflict under International Law”; and Yannakogeorgos *Strategically Using Global Norms to Resolve the Cyber Attribution Challenge* 2013 12.

⁸¹² Gill and Ducheine 2013 *International Law Studies* 438, 467-468.

⁸¹³ Brantly *The decision to attack: Military and intelligence cyber decision-making* (2016) 89.

The challenge of cyber attack attribution means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion.⁸¹⁴

Maritime reliance on ICT has increased the risk associated with the original purpose of the Internet. Most hackers have the toolkits to exploit this risk namelessly, thereby making their identity unknown or uncertain. Tracking and tracing cyber-attackers can be an onerous task due to the speed and global connectedness of cyberspace.⁸¹⁵ This does not underscore the importance of gathering electronic evidence.

Despite the importance of tracking and tracing for uncovering relevant information for security assessment, developing defensive measures is frustrated by incomplete details when an attacker is untraceable.⁸¹⁶ This may arise from the fact that attackers use cyber pathways which cut across jurisdictions. Robertson aptly captures this challenge:

But difficult questions remain. Response against whom? Can the attacker be identified? The originator of the attack may have sent his electronic attack through multiple switches and servers in several different countries.⁸¹⁷

Without cooperation from all the States through which this cyber-attack is being channelled, tracking and tracing becomes challenging. Interrupting such an attack becomes almost impossible. The victim may be left with the option to later assign blames and claim damages. Accuracy in attribution is crucial in making the decision to invoke ASD. This is because wrongful attribution can lead to an escalation of conflicts among the States involved.⁸¹⁸ This is a significant challenge especially when the attacker is skilled in cloaking his identity or misleading the victim to blame someone else using botnets.

⁸¹⁴ Geers "Challenges of Cyber Attack Deterrence" 2010 26(3) *Computer Law and Security Review* 298 302.

⁸¹⁵ Lipson *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (2002) 4.

⁸¹⁶ *Ibid.*

⁸¹⁷ Robertson "Self-Defence against Computer Network Attack under International Law" in *Computer Network Attacks and International Law* 2002 76 *International Law Studies* 138.

⁸¹⁸ Pihelgas "Back-tracing and Anonymity in Cyberspace" in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (2013) 58.

5.4.6. Lack of Consensus in Treaty Provisions on MCAA

Ruys argues that the Charter norms on use of force are not self-reliant with the capability to stop States from using force against each another. Instead, it broadly accords States with the opportunity for justification and determination of the use of force.⁸¹⁹

Fragmentation of maritime cyber security policies and governance prevents uniformity in standardization for determining legal liability and appropriate legitimate ASD measures. Most of the existing policies focus on physical attacks and safety in the marine environment with minimal provisions on issues of ASD measure as part of maritime cyber security. The IMO guidelines give liberty to stakeholders to set their own cyber security standards in accordance with the guidelines.⁸²⁰ This creates a non-uniformity of standards for determining the imminence of an MCAA or the standardized ASD measures to apply.

UNCLOS provides for the obligation not to engage in activities “prejudicial to the peace, good order, or security of the coastal [s]tate.”⁸²¹ This is a customary international law obligation. It includes actions such as the gathering of information, misinformation, or other forms of interference with the structure of communication. Also, UNCLOS proscribes the interference with the security and peaceful existence of coastal States and flagships on the high sea,⁸²² especially attacks that damage submarine cables.⁸²³ Article 113 provides that:

Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence. This provision shall apply also to conduct calculated or likely to result in such breaking or injury...

⁸¹⁹ Ruys “Divergent Views on the Charter Norms on the Use of Force—A Transatlantic Divide?” 2015 109 *Proceedings of the Annual Meeting (American Society of International Law): Adapting to a Rapidly Changing World* 67 70.

⁸²⁰ BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUML, “The Guidelines on Cyber Security Onboard Ships” (2017) <http://www.ics-shipping.org/docs/default-source/resources/safety-security-andoperations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14> accessed 2019-12-03) 51.

⁸²¹ Article 19 of UNCLOS.

⁸²² Articles 86 to 115 of UNCLOS.

⁸²³ Article 113 of UNCLOS.

When read together, these UNCLOS provisions create a certain standard for international maritime law, which encompasses codes being sent through submarine cables to coastal States.⁸²⁴ Based on the above provision, the occurrence of issues relating to damages to submarine cable will clearly be a breach of the established standard. This standard has been criticised for lacking enforcement mechanisms against States.⁸²⁵ Enforcement is limited to the provisions in domestic laws criminalising damages to submarine cables carried out by non-State actors.

Also, States take advantage of the undefined regulation of cyberspace to pursue their agenda⁸²⁶ while conducting surveillance over EEZs. Gao argues that

The frequent visit by foreign naval survey vessels and routine flight of military intelligence planes over the EEZs of the coastal States in the region certainly represents a major source of tension and instability. There is also the likelihood for them to cause surface and air traffic control problems, and increase the chances of accidents, if not conflicts. Countries subject to these intrusive navigation and over-flight off their coastal waters are likely if not inevitably to take counter-measures to safeguard their maritime jurisdiction and interests.⁸²⁷

States such as Cuba, Russia and China have expressed their reservation about applying the international law provision on self-defence to cyber security after attending the 2016-2017 sessions of the UN Group of Government Expert.⁸²⁸ A unified approach by States on the issue of regulating cyberspace will be a step in a positive direction in tackling issues surrounding MCAA.

5.4.7. Lack of Universal Cyber Security Expertise

Not all persons aboard a ship are required to have high-level cyber security expertise. An attacker can easily exploit the ignorance of a computer user on board a ship to infiltrate the Internet network of an ICT-reliant ship. Using botnets, a ship's navigation and communication systems can be hacked and taken control of by an

⁸²⁴ Shackelford "From Nuclear War to Net War: Analogizing Cyber-attacks in International Law" 2009 27 (1) *Berkeley Journal of International Law* 192 227.

⁸²⁵ *Ibid.*

⁸²⁶ Fritz "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness" (2008) 8 *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* 1 1.

⁸²⁷ Gao "China and the Law of the Sea" in Nordquist et al. (eds) *Freedom Of Seas, Passage Rights and the 1982 Law of the Sea Convention* 2009 291.

⁸²⁸ Schmitt and Vihul "International Cyber Law Politicized: The UN GGE Failure to Advance Cyber Norms" (2017-06-30) www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ (accessed 2020-07-20). .

attacker. All ICT-reliant ships must train all persons aboard a ship to be highly cautious of exposing the ship's network to attackers by using their personal devices.

5.4.8. Defence against Non-State Actors without Violating Sovereignty

As previously discussed, there are instances where a State suffers an imminent threat of MCAA from a non-State actor. Thwarting this threat is the State's priority. To do this successfully, the attacker's host country needs to cooperate. This may not be enough as attackers can coordinate their attack through various jurisdictions in their bid to avoid detection. Should all the servers the attacker bounced through be destroyed? Should the host States of these servers be held responsible? Determining liability in the event of a kinetic attack can be clearly determined by the effective control test.

A hypothetical scenario can be helpful to understand this issue in the maritime cyber context: A country (hereinafter referred to as B) has carried out due diligence within its technical capacity to secure its cyberspace, but a hacker penetrates and manipulates this secured cyberspace to launch his/her private attack against the shipping industry of another State (hereinafter referred to as A). Should the attacker's host country B be held accountable or be treated as a victim as well? Country A's preliminary perception of and reaction to the imminent threat, will require a risk assessment and defensive measures to neutralize the imminent attack. Most of the time, country B dissociates itself from the attacker by stating that it did not sponsor him/her.

The main challenge is determining whether the attacker acted alone, or country 'B' was just denying sponsorship to avoid liability. This has been the common practice in modern times where States back cyber-attacks and deny sponsorship to avoid liability. If country 'A' must carry out a defensive measure, how can the sovereignty of country 'B' be lawfully preserved from violation? Is country B exculpated from merely issuing a statement of denial?

Applying the principles of self-defence as contained in article 51 of the UN Charter clearly raises questions with no definite answers. Country A has an inherent right to protect itself from attack and should not be blamed for responding to a perceived

imminent threat. This scenario showcases the imperfect and challenging nature of acting in ASD against MCAA within the parameters of existing laws.

5.5. Conclusion

The existing ICJ interpretation of article 51 of the UN Charter, IMO guidelines, provisions of SOLAS and academic writings which are incidental to the issue of ASD in maritime cyber security lack a uniform approach thereby leaving many stakeholders with uncertainty about imminent risks and legitimate actions to take.⁸²⁹ Despite the scholarly debates about the principle of anticipatory self-defence, there is a point of agreement on the fact that States possess an inherent right of self-defence against MCAAs. In response to these imminent armed attacks, States have the option to either use military force or cyber force capable of proportionate destruction which must be necessary to repel or neutralise the threat. Determining imminence, necessity and proportionality are crucial to legally defend against an MCAA. This is particularly challenging in cyberspace and more complex in the context of the maritime environment.

Applying these legal requirements, which were created from conflicts occurring outside maritime cyberspace, may create an asymmetrical outcome for upholding maritime cyber security. This is evidenced in the challenges pertaining to determining the intent of the attacker, the requirement of early detection to determine imminence, swiftness in the timeline of the attacker act as well as timely decision to carry out the necessary and proportional acts in self-defence.

However, it is pertinent to consider a legal alternative. This entails adapting these requirements through interpretations that reflect the unique nature of maritime cyberspace and the hazardous consequences of MCAA. This creates a positive step towards improving the maritime cyber security of States, preserving the inherent right of States to self-defence, and increasing accountability of attackers.

This legal alternative will provide a suitable interpretation of the imminence of MCAA which will take into consideration the vulnerability of an ICT-reliant ship. Cyber

⁸²⁹ Bothur D., Zheng G., and Valli C. "A critical analysis of security vulnerabilities and countermeasures in a smart ship system". In Valli C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December 2017, Edith Cowan University, Perth, Western Australia. (pp.81-87), 86.

exploitation or intrusions which target vulnerabilities in the navigation, cargo, or communication systems, as well as systems controlling weapons aboard a ship, can potentially lead to disastrous consequences and should be deemed as imminent threats. It is safer in maritime cyberspace to presume an intruder has immediate or long-term hostile intent. The intruder has either found a vulnerability or is searching for an opportunity to carry out a cyber-attack. Similarly, non-consensual military presence in the territory of another State will not be perceived as harmless just because a single shot has not yet been fired.

Consequently, non-consensual interference, intrusion, invasion of maritime cyberspace should be considered a threat to maritime cyber security and should be repelled. The use of cyber force or military force will depend on the victim's perception that hazardous destruction of lives, data or other property is reasonably imminent. An attacker is presumed to intend the probable consequence of his action. The airstrike on Hamas cyber headquarters by the Israeli Defence Force sets a precedent for ASD against a cyber-attack. This use of force by Israel did not draw global condemnation. This could be implied as States being at liberty to apply the legal requirements for ASD against MCAA based on their subjective perception of the threat. As Svarc rightly points out "[S]tate practice is too scarce and inconsistent to allow any clear conclusion about the legality and scope of anticipatory self-defence."⁸³⁰

Notwithstanding, it is imperative to clarify the necessary standard to be upheld in terms of ASD against MCAAs. Although Israel did not provide details of the credibility of the threat, States faced with MCAA's should be required to submit the report of acts conducted in ASD to the International Maritime Organization or relevant regional bodies. This will ensure accountability and best state practices.

ASD depends on a victim's ability to anticipate an MCAA. This requires the use of advanced technologies which can calculate the immediacy of an impending armed attack and possibly determine the proportional defensive measure necessary to thwart the attack. The legal requirement for lawfully invoking ASD against maritime can depend on artificial intelligence because the cyber nature of the attack appears to be a more dominant factor than the marine environment where the attack occurs.

⁸³⁰ Svarc 2006 *ILSA Journal of International and Comparative Law* 171, 180.

CHAPTER 6: CONCLUSION

6.1. Introduction

This research examined the legality of anticipatory self-defence against a maritime cyber-attack. Unlawful cyber incidents that threaten maritime cyber security were analysed with reference to relevant international laws to determine whether these cyber-attacks can be referred to as armed attacks, which is a precondition for States to invoke anticipatory self-defence. The analysis entailed examining the legal framework of maritime cyber security; assessing maritime cyber-attack as the use of force; investigating how maritime cyber-attack can qualify as an armed attack; and examining whether and if so, to which extent the international law principle on anticipatory self-defence can be applied to repel a maritime cyber armed attack. The summary of findings and arguments below establishes how these aims have been achieved in the preceding chapters.

6.2. Summary of Key Issues

The maritime industry is decades behind other industries on the issue of cyber security.⁸³¹ Cyber security threats can adversely affect the navigation, communication and cargo systems on a ship, oil rigs or ports⁸³² and other critical maritime infrastructures of a State. The attacks can be launched using a USB, smart phones, and laptops aboard a ship or remotely by hackers from a different cyberspace jurisdiction. The attacker can be State-sponsored, political groups, rival companies, or freelance hackers. When the victim of a cyber-attack is a State, it has a right to defend itself in accordance with the provision of article 51 of the UN Charter. In line with this provision, when a State suffers a maritime cyber armed attack, the use of force is allowed in self-defence. When the attack is imminent, ASD can be used proportionally to repel the attack. Applying the international law principles on ASD to maritime cyber security raises these following questions:

1. Can a maritime cyber-attack qualify as the use of force?
2. When does maritime cyber-attack meet the threshold of an armed attack?
3. When is a maritime cyber-attack imminent for the purpose of invoking anticipatory self-defence as stipulated by customary international law?

⁸³¹ AS discussed in 1.1 above.

⁸³² As discussed in 1.2 above.

4. When are the requirements for necessity met in terms of satisfying the required conditions for invoking anticipatory self-defence?
5. What form(s) of anticipatory self-defence against MCAs meet the requirement of proportionality?
6. Is anticipatory self-defence against MCAs attainable?

In answering these questions, the relevant legal instruments applicable to maritime cyber security were identified in chapter 2. MCAA is a modern type of threat, and it is important for States to know the lawful approach to repel imminent attacks from States and non-State actors. Attributing an attack is a key factor in determining the options available to a victim-State. When the attacks are carried out by non-State actors in a manner that is beyond the control of their host State(s), domestic laws can apply. However, when the host State is unwilling and unable to act, the victim State can act in ASD as was seen in the use of force by Israeli Defence Forces against Hamas. When the attacks are State-sponsored, a victim State can use force in ASD.

Most of the terminologies in maritime cyber security are used interchangeably thereby creating confusion in determining legal liabilities. As discussed in chapter 3, all maritime cyber activities can be referred to as maritime cyber operations. Cyber operations that invade or intrude another maritime cyberspace without consent is maritime cyber interference. Maritime cyber interference that causes damage can amount to a maritime cyber-attack. An MCA that threatens to or causes the loss of lives and enormous damage to property (tangible or intangible) is an MCAA.⁸³³ Article 51 of the UN Charter may be invoked in ASD to thwart such attacks when they meet the threshold of an armed attack.

In determining when an MCA meets the threshold of an armed attack, it is important to first consider whether an MCA can amount to the use of force. This general prohibition on the use of force was discussed in chapter three. In chapter four, the exception to this prohibition was discussed by showcasing the occurrence of armed attack as a precondition for using force in self-defence. As ruled by the ICJ in the *Nicaragua case*, all armed attacks amount to use of force but not all use of force amounts to an armed attack. This is because the scale and effect of the attack must

⁸³³ As discussed in 4.5 above.

be so grave as to result in enormous damage to property or the loss of lives. This implies that the possibility of a high degree of damage or grave consequence of MCAs determines the legal response in ASD.⁸³⁴

It has been argued that intercepting an unlawful cyber-attack that targets a State's critical maritime infrastructures is an example of the normative international law interpretation of ASD when the MCAA can be equated to an armed attack. This expansive interpretation is crucial to guarantee efficient and effective maritime cyber security. It will accommodate the contemporary subjective interpretations by States thereby clarifying the laws and principles for ASD against MCAA. In chapter 5, the international law principle of self-defence was explored in the context of maritime cyber security. The legal requirement for invoking ASD against MCAAs was discussed.

During the discussion, it became clear that the expansive interpretation of article 51 on ASD is very relevant to the effect-based interpretation of MCAA. Focusing on the potential gravity of an imminent MCAA accommodates the intangible nature of the scale and effect of cyber destruction. For instance, when the critical systems of a ship, oil rig, or port experiences a cyber-attack, their GPS signals can be lost, communication system jammed, and cargo system can be manipulated to traffic drugs or nuclear materials through barcode specific crates. These can lead to grave consequences such as oil rig explosions, oil spillage, loss of lives. The non-physical damage which brings about these grave consequences, but usually falls below the normative threshold of an armed attack, can now become recognised, acknowledged, and accorded the required legal consequence.

It was submitted in chapter five that the implementation of the principle of ASD against MCAA is riddled with challenges that need to be addressed to enhance maritime cyber security. These challenges were discussed in chapter five and some recommendations were made. States applying the IMO guidelines and regulations must be guided by the international law principles on self-defence, especially on the issue of identifying and mitigating grave threats to maritime cyber security. The IMO's risk management approach seeks to minimize danger to crew and from cyber-attack resulting in financial loss and environmental safety. Its updated cyber security

⁸³⁴ As discussed in 4.5.4 above.

requirements state that all stakeholders should comply by January 1, 2021. More specifically, stakeholders need to have a structure that provides guidance and processes for identifying and mitigating cyber threats. It behooves ship owners, operators, and other stakeholders to ensure that the application of these processes and guidance does not contradict the peremptory norms of international law on ASD.

Notably, the UN Charter is not explicit in its provision for self-defence against non-kinetic attacks. Resolving to use an analogy to justify the legality of the use of force against armed attack in the nuclear weapon's context has extended the discussion to include nuclear weapons and other weapons as the means through which armed attack may occur.⁸³⁵ A further extension of this analogy to maritime cyber security exposes the non-comprehensive nature of article 51 of the UN Charter.⁸³⁶ It brings to light the challenges of invoking article 51 against maritime cyber armed attacks.⁸³⁷

Article 51 and its interpretation by the ICJ focuses on an armed attack by States or armed groups sponsored by States. It is equally important to address the circumstances where States need to act in self-defence against non-State actors. The incident where the Israeli Defence Force bombed Hamas' headquarters is the latest precedent for using force against non-State actors in self-defence against a cyber-attack. This confirms Judge Higgins's dissenting opinion that force may be used in self-defence against non-State actors who perpetrate an armed attack.⁸³⁸ This can involve determining the host State's commitment, capability, and willingness to hold the attacker liable. The issue of State responsibility is relevant to determine attribution and the best option for ASD.

Notably, there are instances where a group of hackers in a State may hijack the hacking system of another State. This has been reported as the new mode of cyber-attack by Russian hackers who wear the mask of hackers residing in another State and use their cyber weaponry to carry out an attack.⁸³⁹ These are generally referred to as crimes and subject of national legal proceedings despite the interstate effect of most cyber-attacks. Also, States have the habit of denying connections with cyber

⁸³⁵ *Nuclear weapons' case* par 95

⁸³⁶ As discussed in 5.4 above.

⁸³⁷ As discussed in 5.4.2 above.

⁸³⁸ The dissenting opinion of Judge Higgins in the ICJ Advisory Opinion on *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004 ICJ Report, par [33-34].

⁸³⁹ Financial Times "Russian Cyberattack Unit 'Masqueraded' as Iranian Hackers, UK Says" <https://www.ft.com/content/b947b46a-f342-11e9-a79c-bc9acae3b654> (accessed 2019-10-21).

groups to avoid liability. These challenges have prevented States from successfully addressing the problem of maritime cyber insecurity.

Specifically, the global effect of maritime insecurity at the Gulf of Guinea, the Gulf of Aden and the Indian Ocean is severe despite the existing institutions⁸⁴⁰ and policy framework.⁸⁴¹ Enhancing maritime domain awareness (MDA), especially by understanding the scope, nature, and potential effects of maritime cyber armed attacks, is crucial to addressing maritime cyber insecurity. States will be more alert to perceive more efficiently imminent attacks and take the proportional and necessary steps in ASD to prevent the actual occurrence of the threat.

Applying a positivist approach to determining the legality of ASD against MCAA will require focusing on doctrines without a concrete understanding of the application of these doctrines to maritime cyber security. The realist's school of thought has been extensively applied during this thesis to demystify the issues surrounding the use of force in an armed attack. This approach has laid bare the challenges of applying the principle of ASD against MCAA and recommendations for more effective maritime cyber security policies. The maritime industry needs to be legally prepared for the era of computer-controlled vessels. Hoisington rightly submitted that:

Serious threats to international peace will result unless states have the ability to respond in self-defence to cyberattacks without being restrained by outdated interpretations of international law governing the use of force.⁸⁴²

This submission emphasizes the challenge of applying Schmitt's result-oriented approach in determining the legitimacy of States to act in self-defence against an MCAA. The current interpretation of international law principles on self-defence mostly limits States' legitimate capacity to repel evolving threats of MCAA. The UN Charter's prohibition of and exception to the use of force did not consider the contemporary threat of MCAA. As argued in the previous chapters, when a cyber-

⁸⁴⁰ Maritime Organisation of West and Central Africa, Gulf of Guinea Commission, Gulf of Guinea Guard, etc.

⁸⁴¹ Such as the UN Resolutions 2018 and 2039, 2050 Africa Integrated Maritime Strategy (AIMS), ECOWAS and Integrated Maritime Strategy (EIMS).

⁸⁴² Hoisington "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence" 2009 32 *Boston College International and Comparative Law Review* 439 454.

attack threatens the critical infrastructures of a State,⁸⁴³ especially in the marine domain, States are justified to reasonably act in anticipatory self-defence.

Based on the discussions from the preceding chapters, two main questions should be asked just before a victim responds to a threat of MCAA: Is there a critical vulnerability in the victim's cyberspace that this imminent attack can exploit? Is there a reasonable probability that this imminent threat can lead to loss of lives and destruction of property immediately or consequently? If the answers to these questions are positive, the victim State can lawfully act in anticipatory self-defence according to article 51 of the UN Charter. If the answers are negative, the self-defence option available to the State can be countermeasures that do not amount to the use of force but proportional and necessary to repel the imminent attack. This rejoinder is premised on the joint reading of the ICJ ruling on the Nicaragua case and the Oil Platform case on the issue of self defence as discussed in the previous chapter.⁸⁴⁴

However, suppose the answers are uncertain or undetermined. In that case, a reasonable decision must be taken by the State to protect its interests with utmost caution and focus on compliance with international shipping regulations for protecting lives and ships at sea. The victim States' right to anticipatorily defend against an MCA launched at its critical infrastructures can be reasonably implied. This research has pushed the frontiers of the law of sea on the issue of maritime cyber security by exploring other options available to victim States outside IMO guidelines.

6.3. Recommendations

Maritime law and international law are two branches of law that are interconnected on the issue of States defending against attacks on their maritime cyber security. The scholarly debates in the preceding chapters demonstrate that applying international law principles on self-defence against an armed attack on maritime cyber security creates uncertainties. The uncertainties include the determination of a universally acceptable definition of MCAA; the interpretation of the jus ad bellum

⁸⁴³ Condrón "Getting it Right: Protecting American Critical Infrastructure in Cyberspace" 2007 20 *Harvard Journal of Law and Technology* 403 416.

⁸⁴⁴ As discussed in 5.2.1 and 5.2.2 above.

principles of imminence, necessity and proportionality in defending against MCAs; and the cyber technicality required for an equitable assessment of a State's perception of threat and legitimate actions to repel it. Also, this is reflected in identifying the legal framework which applies to maritime cyber security.

These uncertainties can be demystified by reaching a global consensus in the form of a multilateral treaty that addresses the challenges of maritime cybersecurity.⁸⁴⁵ According to the UK government:

Promoting a secure international maritime domain will help to strengthen global peace, security and governance and promote global prosperity.⁸⁴⁶

The adoption of a multilateral treaty on the MCAA issue is in every country's interest because of the global relevance of the maritime domain to commerce and national security. The treaty can provide solutions to address the issues discussed in this thesis, particularly the challenges of invoking anticipatory self-defence against MCAA, as discussed in chapter five. The central issue which cuts across other issues is the lack of consensus among States on the standard for determining imminence, attribution, and defining MCAA. Uniformity in maritime cybersecurity policy directives on defending against MCAs among States can pave the way for a universally acceptable multilateral treaty. When States begin to pay more attention to the security threat posed by MCAA and commit resources to advancing their technological capabilities to detect imminent maritime cyber threats, maritime cyber security will be enhanced, and victim States will be better positioned to protect themselves. The treaty should provide for the legal obligation of States to assist each other in investigating MCA originating from their jurisdiction.

The international law principles on self-defence which are regularly applied through analogies, need to be revisited to address most of the challenges discussed in chapter five. Chayes emphasizes this by stating that:

However, until international agreements alter the law, or the International Court of Justice rules on such issues, many of the novel legal questions that cyber-

⁸⁴⁵ Hathaway Crootof, Levitz, Nix, Nowlan, Perdue and Spiegel "The Law of Cyber-Attack" 2012 100 *California Law Review* 817 877

⁸⁴⁶ Foreign and Commonwealth Office "Strengthening Maritime Security: objectives 2019 to 2020" (2019-09-19).
<https://www.gov.uk/government/publications/official-development-assistance-oda-fco-international-programme-spend-objectives-2019-to-2020/strengthening-maritime-security-objectives-2019-to-2020> (accessed 2019-10-10).

attacks pose will be answered by creative, if contrived, adaption of historic doctrines.⁸⁴⁷

It has been established by customary international law that even when an armed attack is yet to occur, the right of self-defence can be invoked anticipatorily if the attack is perceived as imminent.⁸⁴⁸ According to Waldock,

[w]here there is convincing evidence not merely of threats and potential danger but of an attack being actually mounted, then an armed attack may be said to have begun to occur, though it has not passed the frontier.⁸⁴⁹

On the issue of imminence, it has been established that it is practically impossible to read the mind of an aggressor to determine his intent. Hence, a victim has to reasonably perceive the likely gravity of the incoming or probable attack.⁸⁵⁰ It is a considerable burden for a victim to determine the imminence of the threat and decide whether a use of force is required to neutralise it. This challenge confirms that the treaty and international customary law principles on the issue of self-defence may be theoretically correct but practically inefficient when applied to maritime cyber security. It is pertinent to have tangible understanding of the gravity and effect of MCAA to create a platform for effective and efficient maritime cyber security.

As previously suggested, cyber espionage should be seen as the announcement of an imminent attack based on the reasonably foreseeable damage that could be done with the information the aggressor has gathered from the victim's network.⁸⁵¹ As aptly stated by Robertson,

It would seem, then, that the most likely application of the doctrine of anticipatory self-defence to computer network attacks would be in the case of such attacks that in and of themselves do not constitute an armed attack but rather are evaluated as precursors of an armed attack by kinetic means and/or further, more severe cyber-attacks.⁸⁵²

So, when a victim-State reasonably assesses that an incident of cyber espionage has made the critical infrastructures of the State vulnerable to a probable and devastating attack, it may act in anticipatory self-defence before the aggressor takes advantage of that vulnerability. The evidence of an impending and devastating

⁸⁴⁷ Chayes 2015 6 *Harvard National Security Journal* 474 510.

⁸⁴⁸ Bowett *Self-Defence in International Law* (1958) 188-189.

⁸⁴⁹ Waldock "The Regulation of the Use of Force by Individual States in International Law," 1952 81 *Recueil des Cours* 451 498.

⁸⁵⁰ See discussion in 5.3.1 on 'imminence'.

⁸⁵¹ As discussed in chapter 5.4.2 above.

⁸⁵² Robertson "Self-Defence against Computer Network Attack under International Law" in *Computer Network Attacks and International Law* 2002 76 *International Law Studies* 139.

cyber-attack is required as corroboration to the incident of cyber espionage to justify ASD.⁸⁵³ In some delicate circumstances, it is submitted that the attacker's knowledge of the vulnerabilities of the victim's critical infrastructure is sufficient proof of imminence.

Furthermore, the decision to act in ASD should be carried out with the following objectives in mind:

1. To prevent the imminent attack from occurring
2. To prevent the aggressor from further intrusion into the victim's network
3. To ensure that the aggressor loses its capability to re-launch the attack

Since the circumstances of MCAAs are relative, these objectives should guide victims when acting in ASD. This will ensure legitimate application of the principles of self-defence. For instance, the DHS Cyber Hunt and Incident Response Teams Acts (s.315) were passed to empower the Department of Homeland Security (DHS) to address cyber-attack issues.⁸⁵⁴ They include identifying cyber security risks and providing mitigation strategies to prevent, deter and protect victims.⁸⁵⁵ These responsibilities are attuned to the above-listed objectives. It is a step in the right direction to ensure that the law does not limit victims in their effort to reasonably protect themselves from cyber-attacks.

Likewise, the IMO and other related regional bodies need to clarify the maritime cyber incidents that will justify the use of force in self-defence. This needs to be codified to prevent relative application and analogical interpretation of the UN Charter to address maritime cyber security issues. An unambiguous meaning of anticipatory self-defence, armed attack and use of force in the context of maritime cyber security is necessary to improve the effectiveness and efficiency of the defence strategy against MCAA.

⁸⁵³ *Ibid.* Robertson argues that: "While these preliminary CNAs may not themselves rise to the level of armed attack, they may, if combined with other evidence of an impending attack, be sufficient to authorize armed measures of self-defence-not against the CNAs themselves, but rather as an exercise of the right of anticipatory self-defence against the impending kinetic or more serious cyber-attack."

⁸⁵⁴ Gatlan "US Senate Passes Bill in Response to Rampant Ransomware, CyberAttacks" (2019-09-27) www.bleepingcomputer.com/news/security/us-senate-passes-bill-in-response-to-rampant-ransomware-cyberattacks/ (accessed 2019-10-01).

⁸⁵⁵ *Ibid.*

Despite the challenges of applying existing treaty provisions on maritime cyber security, it is important to review and upgrade them to become capable of addressing issues arising from MCAA. Fenton III argues in favour of:

calls for the creation of an international treaty that builds on existing international law and provides the international community with a more efficient and tangible means for conducting cyberwar by resolving the current ambiguities and complexities existing today.⁸⁵⁶

This will also ensure accountability among States engaging in maritime cyber wars. Enactment of legislations that specifically address maritime cyber security must be carried out by States in addition to the obligation of the IMO guidelines on maritime security. This creates a legal foundation for improving legal duties and obligations on maritime cyber security at the international level among States. The legislation will include “a requirement for vessels and facilities to create, test, and maintain plans to address cybersecurity vulnerabilities and responses to cyber-attacks.”⁸⁵⁷

This mandatory exercise will help to shape State practice and regulate *jus in bello* decisions for upholding maritime cyber security. Legislations that protect undersea infrastructure will provide legal standing to act in ASD with proportionate use of force against any threat to the security of undersea pipelines or cables.⁸⁵⁸

Also, there is a need to regulate the issue of perception of imminence by victims. A cyber-attack that poses a potential threat to the critical infrastructure of a ship, port, and oil rig should always be treated as a grave cyber armed attack. The gravity of damage that could occur to these critical infrastructures is worth preventing with the strictest measure. Professor Schmitt proposes in support of Dinstein’s ‘interceptive self-defence’ that the tests to determine when ASD will be justified are: if the preliminary attack is part of an armed attack, cannot be reversed and the victim is acting within the last window of opportunity to thwart the attack effectively.⁸⁵⁹ It is submitted that this is a logical theory but challenging to implement in maritime cyber security.

⁸⁵⁶ Fenton III “Proportionality and its Applicability in the Realm of Cyber-Attacks” 29 2019 *Duke Journal of Comparative and International Law* 335 359.

⁸⁵⁷ Foote “Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities and Vessels Safe from Cyber Threats” 2017 8 *Cybaris Intellectual Property Law Review* 231 263.

⁸⁵⁸ Wrathall “The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward” 2010 12 *San Diego International Law Journal* 223 251.

⁸⁵⁹ Schmitt “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework” 1999 37 *Columbia Journal of Transnational Law* 993 993.

It is essential to strike a balance while seeking to uphold maritime cyber security. The polarized interpretation of imminence (proportionality and necessity) and armed attack gives no room for a single formula to be applied. Therefore, a case-by-case analysis in line with the above-listed objectives and previously discussed principles of *jus ad bellum* will subsequently birth a pattern of State practices on the subject. Not many States have publicly affirmed the legality of the use of force against MCAA, but it is becoming gradually popular among States to view cyber-attacks that threaten lives and critical IT networks as armed attacks.⁸⁶⁰

In addition, one of the objectives of ASD is to repel the imminent threat and deter the aggressor from launching another threat against critical infrastructures. To achieve these objectives in maritime cyberspace, the use of force (cyber or military) is the loudest language of deterrence to speak to an aggressor. A non-forceful measure of ASD only gives the aggressor more time to work on a better plan to achieve their hostile intent.⁸⁶¹ Even when defensive software is upgraded and updated, it is just a matter of time before the aggressor can devise a clever means of circumventing these defence walls. When force is used, as seen in the incident of Israel's strike on Hamas' cyber headquarters, the threat is completely neutralized. The aggressor loses the capacity to re-launch the threat and the critical infrastructures will be realistically protected.

However, this is a risky approach due to the complex and evasive nature of some cyber-attacks that use botnets and pass through several domain servers or jurisdictions to avoid detection.⁸⁶² The challenges of precision in executing the defence measures and the issue of attribution are crucial.⁸⁶³ Previous physical or cyber intelligence gathering on the preparatory stage of the imminent attack can help to address the issues of tracking and tracing quickly. However, it will be reasonable to defend against a perceived imminent threat irrespective of the attacking State's

⁸⁶⁰ When Israeli Defence Forces bombed Hamas' cyber headquarters in response to a cyber-attack, there was no unanimous condemnation by other States. This can be interpreted as acquiescence.

⁸⁶¹ Brantly "The Cyber Deterrence Problem" in *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, 31, 36.

⁸⁶² Valeriano and Maness *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (2015) 57-60.

⁸⁶³ The challenge of tracking and tracing was discussed in 5.4 above.

denial of sponsorship if there is no genuineness in assisting the victim State with identifying the attacker.

Every State should demonstrate a high and universal standard of responsibility in securing its cyberspace and preventing its use as a breeding hub for hackers. The rationale behind this analogy stems from the acceptance of the US post 9/11 invasion of Afghanistan as justifiable. States will always debate about how international law should apply to them until a common practice is established. Maritime cyber security is clearly an area of maritime law with many legal uncertainties.

The provision of article 3(1) of the Convention on the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988 SUA Convention) can provide a right of action for States who have suffered an MCAA. It does not provide for the right of ASD. Like this provision, the language of most of these guidelines and conventions suggest that the threat must have come to fruition, and the victim must take steps to recover. Others provide for general safety guidelines that keep the ship, port, or oil rig safe until the aggressor figures out how to break down that wall of defence.

An expansive approach to the issue of maritime cyber security will create a holistic means to apply ASD against MCAA legally. The provisions of these conventions can be built upon to regulate States' acts of ASD against the modern threat technology poses to maritime security. This is a critical modern approach to enhance the effectiveness and efficiency of maritime cyber security. From the preceding discussion, it has been found that the existing interpretation of article 51, when applied to maritime cyber security, limits the State's ability to invoke its right to self-defence without fearing to fall short of the requirements stated by the existing precedents formed from cases such as the Nicaragua case, Oil platforms case, Nuclear Weapons case. Article 51 needs to be interpreted by taking cognizance of the peculiar nature of MCAs.⁸⁶⁴

⁸⁶⁴ As discussed in 5.4.2 especially at page 158.

TABLE OF INTERNATIONAL INSTRUMENTS

The Additional Protocol I to the Geneva Conventions, 1949.

The African Union Convention on Cyber Security and Personal Data Protection, 2014.

The Budapest Convention on Cybercrime 2001.

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) 1988.

The Convention on the International Maritime Organization, 1948.

The ILC's Draft Articles on the Responsibility of States for Internationally Wrongful Acts, 2001.

The International Convention for the Safety of Life at Sea, 1974.

The International Maritime Organization, Guidelines on Maritime Cyber Risk Management, 2017.

The Montevideo Convention, 1933.

The Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 2005.

The International Maritime Organization (IMO) Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships, 2010.

The Statute of the International Court of Justice, 1945.

The United Nations Charter, 1945

The United Nations Convention on Law of the Sea, 1982.

TABLE OF LEGISLATION

Act on the Marine Areas of the Islamic Republic of Iran in Persian Gulf and the Oman Sea 1993.

Australian Sea Installations Act, 1987.

Cybercrimes Act 19 of 2020

Electronic Communications and Transactions (ECT) Act, 2002.

Law of the Territorial Sea and the Contiguous Zone of the Republic of China, 1992.

Nigerian Maritime Administration and Safety Agency Act, 2007

Protection of Personal Information Act., 2013.

South African Electronic Communications and Transactions Act 25 of 2002.

TABLE OF CASES

Armed Activities on the Territory of the Congo, Congo, the Democratic Republic of the v Uganda, Judgment, Merits, ICJ GL No 116, [2005] ICJ Rep 168, ICGJ 31 (ICJ 2005), 19th December 2005, International Court of Justice [ICJ]

Caroline Case of 1837; facts taken from D.J. Harris, Cases and Materials on International Law, 5th Edition, 1998.

Corfu Channel, United Kingdom v Albania, Judgment, Merits, ICJ GL No 1, [1949] ICJ Rep 4, ICGJ 199 (ICJ 1949), 9th April 1949, United Nations [UN]; International Court of Justice [ICJ]

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ GL No 131, [2004] ICJ Rep 136, (2004) 43 ILM 1009, ICGJ 203 (ICJ 2004), 9th July 2004, United Nations [UN]; International Court of Justice [ICJ]

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996.

Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States, Merits, Judgment, (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ].

Oil Platforms, Iran v United States, Judgment, merits, ICJ GL No 90, [2003] ICJ Rep 161, ICGJ 74 (ICJ 2003), 6th November 2003, International Court of Justice [ICJ]

BIBLIOGRAPHY

Books

Al-Rodhan N.R.F, Herd G. P., Watanabe L. "The Six-Day War and its Consequences". In Al-Rodhan N.R.F, Herd G. P., Watanabe L. (eds), *Critical Turning Points in the Middle East: 1915-2015*. 2011 London: Palgrave Macmillan.

Arend A.C. and Beck R.J. *International Law and the Use of Force: Beyond the UN Charter Paradigm* (2014).

Armistead L. *Information Operations: Warfare and the Hard Reality of Soft Power* (2004) Potomac Books Inc.

Bateman S. and Ho J. (eds.), *Southeast Asia and the Rise of Chinese and Indian Naval Power: Between Rising Naval Powers* (2010) Routledge.

Bory *The Internet Myth: From the Internet Imaginary to Network Ideologies* (2020) London: University of Westminster Press.

Bowett D. *Self-Defence in International Law* (1958) Manchester University Press.

Brantly A.F. *The Decision to Attack: Military and intelligence cyber decision-making* (2016) University of Georgia Press.

Brownlie I. *International Law and the Use of Force by States* (1963) Clarendon Press.

Buchanan B. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (2017) Oxford: Oxford University Press.

Christenson G. 'The Doctrine of Attribution in State Responsibility' in Lillich R. (ed) *International Law of State Responsibility for Injuries to Aliens* (1983) University Press of Virginia.

Clarke R. and Knake R. *Cyber War* (2010) HarperCollins.

Constantinou A. *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (2000) Ant. N. Sakkoulas.

Corten O. *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (2021) Bloomsbury Publishing.

Crawford J. *State Responsibility: The General Part* (2013) Cambridge University Press.

Danilenko G.M. *Law-Making in the International Community* (1993) Martinus Nijhoff Publishers.

Delerue F. *Cyber Operations and International Law* (2020) Cambridge: Cambridge University Press.

Dinniss H.H. *Cyber Warfare and the Laws of War* (2012) Cambridge University Press.

Dinstein Y. *War, Aggression and Self-Defence* (2011) Cambridge University Press.

Dobbins J., Solomon H.R., Chase M.S., Henry R., Larrabee F.S., Lempert R.J., Liepman A.M., Martini J., Ochmanek D., and Shatz H.J. *Choices for America in a Turbulent World: Strategic Rethink* (2015) Rand Corporation.

Dunoff J.L., Ratner S.R., and Wippman D. *International Law Norms, Actors, Process* 3ed (2010) Wolters Kluwer.

M.D. Evans (eds.) and Galani S. *Maritime Security and the Law of the Sea* (2020) Edward Elgar Publishing.

Gray C.D. *International Law and the Use of Force* 4ed (2018) Oxford University Press.

Green J.A. *The International Court of Justice and Self-Defence in International Law* (2009) Bloomsbury Academic.

Hawkes K.G. *Maritime Security* (1989) Cornell Maritime Press.

Henkin L. *How Nations Behave* 2ed (1979) Council on Foreign Relations.

Hoffman W. and Levite A. (2017). *Private Sector Cyber Defence: Can Active Measures Help Stabilize Cyberspace?* Carnegie Endowment for International Peace.

Jasper S. (ed.) *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security* (2012) Georgetown University Press.

Jennings R. and Watts A. *Oppenheim's International Law* 9ed (1992) Oxford University Press.

Johnson W. and Lee D.H. (eds.) *Law of Armed Conflict Deskbook* (2014) CreateSpace Independent Publishing Platform.

Juma L. and Strydom H. 'Maintaining International Peace and Security: The Enforcement of International Law' 226 in Strydom H., Gevers C., Ruppel O., Juma L., Vrancken P., Kemp G., Scholtz W., and Viljoen F. *International Law* (2016) Oxford University Press.

Kelsen H. *The Law of the United Nations* (1950) London: Stevens & sons Limited.

Klaidman D. *Kill or Capture: The War on Terror and the Soul of the Obama Presidency* (2012) Houghton Mifflin Harcourt.

Klein N. *Maritime Security and the Law of the Sea* (2011) Oxford University Press.

Kotzur M., Matz-Lück N., Proelss A., Verheyen R., and Sanden J. (eds.) *Sustainable Ocean Resource Governance: Deep Sea Mining, Marine Energy and Submarine Cables* (2018) Leiden, Boston: Brill Nijhoff.

Kramer F.D., Starr S.H., and Wentz L.K. *Cyberpower and National Security* (2009) Washington DC: National Defence University Press.

Kraska J. and Pedrozo R.A. *International Maritime Security Law* (2013) Martinus Nijhoff, Leiden and Boston.

Lauterpacht H. (ed.) *Disputes, War and Neutrality* 7ed (1952) London: Longmans Green & Co.

Libicki, M. C. *Crisis and Escalation in Cyberspace* (2012) Rand Corporation.

Libicki M. C. *Cyberdeterrence and Cyberwar* (2009) RAND Corporation.

Mauroni A.J. *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy* (2016) New York: Rowman and Littlefield.

Michel D. and Sticklor R. (eds.) *Indian Ocean Rising: Maritime Security and Policy Challenges* (2012) Washington: STIMSON.

Mueller K.P., Castillo J.J., Morgan E.F., Pegahi N., and Rosen B. *Striking First: Pre-emptive and Preventive Attack in U.S. National Security Policy* (2006) Santa Monica, CA: Rand Corporation.

O'Connell M. E. The prohibition of the use of force. In *Research Handbook on International Conflict and Security Law* (2013) Edward Elgar Publishing.

Orakhelashvili A. *Peremptory norms In International Law* (2009) Oxford University Press.

Quigley C. *Tragedy and Hope* (1966) New York: Macmillan Company.

Russell A.L. *Cyber Blockades* (2014) Georgetown University Press.

Schmitt M.N. (ed.) *Tallinn Manual 2.0 on the International Law Application to Cyber Warfare* 2ed (2017) Cambridge University Press.

Schmitt M. N. Responding to transnational terrorism under the Jus ad Bellum: a normative framework. In *International Law and Armed Conflict: Exploring the Faultlines* (2007) Brill Nijhoff.

Scott S.V., Billingsley A.J., Michaelsen C. *International Law and the Use of Force: A Documentary and Reference Guide* (2009) Praeger.

Shah N.A. 'Self-defence in International Law' in *Self-defence in Islamic and International Law* (2008) Palgrave Macmillan, New York.

Sharp G. (Sr.) *Cyberspace and the Use of Force* (1999) Falls Church, Va.: Aegis Research Corp.

Shaw M.N. *International Law* 9ed (2021) Cambridge University Press.

Simma B., Khan D., Nolte G., Paulus A., and Wessendorf N. (eds.) *The Charter of the United Nations: A Commentary* (2012) Oxford University Press.

Solis G.D. *The Law of Armed Conflict* (2010) Cambridge University Press.

Tanaka Y. *The International Law of the Sea* 2ed (2015) Cambridge University Press.

UK Chamber of Shipping *A Master's Guide to Cyber Security* 2015 Witherby Seaman's International Ltd.

Ülgen S. and Kim G. (eds.) *A Primer on Cyber Security in Turkey: And The Case of Nuclear Power* (2015) Centre for Economics and Foreign Policy Studies.

Uzer F.B. (ed.). *Maritime Security and Defence against Terrorism* (2012) Washington, DC: IOS Press.

Valeriano B. and Maness R.C. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (2015) New York: Oxford University Press.

Vecchio A. (ed.) *International law of the sea: Current trends and controversial issues* (2014) Eleven International Publishing.

Walzer M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations* 2ed (1997) New York: Basic Books.

Waters G. "Information Warfare Attack and Defence" in Waters G., Ball D. and Dudgeon I. *Australia and Cyber-warfare* 2008 The Australian National University E Press.

Zemanek K. "Armed Attack" *Max Planck Encyclopaedia of Public International Law* 2010 Oxford University Press.

Zimmerman C. *Ten Strategies of a World-Class Cybersecurity Operations Center* 2014 The MITRE Corporation.

Ziolkowski K. (ed.) *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (2013) Tallinn, Estonia: NATO CCD COE Publications.

Journal Articles

Ahmed A. "International Law of the Sea: An Overlook and Case Study" 2017 8 *Beijing Law Review* 21.

Aldrich R.W. "How do you know you are at war in the information age?" 1999-2000 22 *Houston Journal of International Law* 223.

Banks W.C. and Criddle E.J. "Customary Constraints on the Use of Force: Article 51 with an American Accent" 2016 29(1) *Leiden Journal International Law* 67.

Barkham J. "Information Warfare and International Law on the Use of Force" (2001) 34 *New York University Journal International Law and Politics* 57.

Benatar M. "The Use of Cyber Force: Need for Legal Justification?" 2009 1 *Göttingen Journal of International Law* 375.

Boon K.E. "Are Control Tests Fit for the Future? The Slippage Problem in Attribution Doctrines" 2004 15 *Melbourne Journal of International Law* 2.

Boudreau D.G. "The Bombing of the Osirak Reactor" 1993 10(2) *International Journal on World Peace* 21.

Boyle A. "Further Development of the Law of the Sea Convention: Mechanisms for Change" 2005 54(3) *The International and Comparative Law Quarterly* 563-584.

Brownlie I. "International Law and the Activities of Armed Bands" 1958 7(4) *International and Comparative Law Quarterly* 712-735.

Brunstetter D. and Braun M. "From Jus ad Bellum to Jus ad Vim: Recalibrating Our Understanding of the Moral Use of Force" 2013 27(1) *Ethics and International Affairs* 87-106.

Bueger C. "What is maritime security?" 2015 53 *Marine Policy* 159-164.

Chayes A. "Rethinking Warfare: The Ambiguity of Cyber Attacks" 2015 6 *Harvard National Security Journal* 474.

Chuang J. "The United States as A Global Sheriff. Using Unilateral Sanctions to Combat Human Trafficking" 2006 27 *Michigan Journal of International Law* 437.

Condon S. "Getting it Right: Protecting American Critical Infrastructure in Cyberspace" 2007 20 *Harvard Journal of Law and Technology* 403.

Dannenbaum T. "Killings at Srebrenica, Effective Control, and the Power to Prevent Unlawful Conduct" (2012) 61(3) *The International and Comparative Law Quarterly* 713-728.

Davenport T. "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis" 2015 24(1) *The Catholic University Journal Of Law & Technology* 57-109.

DeBenedetti C. "Borah and the Kellogg-Briand Pact." 1972 63(1) *The Pacific Northwest Quarterly* 22-29.

DeLuca C.D. "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors" 2013 3(9) *Pace International Law Review Online Companion* 278.

Dempsey P.S. "Economic Aggression & Self-Defence in International Law: The Arab Oil Weapon and Alternative American Responses Thereto" 1977 9 *Case Western Reserve Journal of International Law* 253.

Dever J. and Dever J. "Cyber Warfare: Attribution, Preemption, and National Self-defence" 2013 2 *Journal of Law & Cyber Warfare* 25.

Dinstein Y. "Computer Network Attacks and Self-Defence" 2002 76 *Computer Network Attack and International Law* 99.

Dombrowski P. and Demchak C.C. "Cyber War, Cybered conflict and the Maritime Domain" 2014 67(2) *Naval War College Review* 70-96.

Dunlap C.J. "Perspectives for Cyber Strategists on Law for Cyberwar" 2011 5(1) *Strategic Studies Quarterly* 81-99.

Dynkin and Dynkin "Derivative Liability in the Wake of a Cyber-attack" 2018 28 *Albany Law Journal of Science and Technology* 23.

Egan B.J. "International Law and Stability in Cyberspace" 2017 35 *Berkeley Journal of International Law* 169.

Eric B. "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners" 2017 50 *Vanderbilt Journal of Transnational Law* 217.

Ezekiel A.W. "Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft" 2013 26(2) *Harvard Journal of Law and Technology* 649.

Feldt L., Roell P., and Thiele R.D. "Maritime Security – Perspectives for a Comprehensive Approach" 2013 222 *ISPSW Strategy Series: Focus on Defence and International Security*.

Fenton H. III "Proportionality and its Applicability in the Realm of Cyber-Attacks" 29 2019 *Duke Journal of Comparative and International Law* 335.

Fenwick C.G. "The 'Failure' of the League of Nations" 1936 30(3) *The American Journal of International Law* 506.

Fink J.E. "The Gulf of Aqaba and the Strait of Tiran: The Practice of 'Freedom of Navigation' After the Egyptian-Israeli Peace Treaty" 1995 42 *Naval Law Review* 121.

Fleck D. "Rules of Engagement of Maritime Forces and the Limitation of the Use of Force Under the UN Charter", 1989 31 *German Yearbook of International Law* 165.

Foote R. "Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities and Vessels Safe from Cyber Threats" 2017 8 *Cybaris Intellectual Property Law Review* 231.

Fritz J "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness" 2008 8 *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* 1.

Gable K.A. "Cyber-Apocalypse Now: Securing the Internet Against Cyber-terrorism and Using Universal Jurisdiction as a Deterrent" 2010 43 *Vanderbilt Journal of Transnational Law* 57.

Geers K. "Challenges of Cyber Attack Deterrence" 2010 26(3) *Computer Law and Security Review* 302.

Gill T.D. "The Forcible Protection, Affirmation and Exercise of Rights by States Under Contemporary International Law" 1992 23 *Netherlands Yearbook of International Law* 105.

Gill T.D. and Ducheine P.A.L. "Anticipatory Self-Defence in the Cyber Context" 2013 89 *International Law Studies* 438.

Gordon E. "Article 2(4) in Historical Context" 1985 10(2) *Yale Journal of International Law* 271.

Graham D.E. "Cyber Threats and the Law of War" 2010 4 *Journal of National Security Law and Policy* 87.

Green F. "Fragmentation in Two Dimensions: The ICJ's Flawed Approach to Non-State Actors and International Legal Personality" 2008 9 *Melbourne Journal of International Law* 47.

Handler S.G. "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare" 2012 48 *Stanford Journal of International Law* 209.

Hatch B.B. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits" 2018 11(1) *Journal of Strategic Security* 43.

Hathaway O. A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W. and Spiegel J. (2012). "The law of cyber-attack" *California Law Review* 817.

Hayward R.J. "Evaluating the 'Imminence' of a Cyber-attack for Purposes of Anticipatory Self-Defence" 2017 117 *Columbia Law Review* 399.

Healey J. "The spectrum of national responsibility for cyberattacks" 2011 18(1) *The Brown Journal of World Affairs* 57-70.

Heinegg W.H. "The difficulties of conflict classification at sea: Distinguishing incidents at sea from hostilities" 2016 98 (2) *International Review of the Red Cross* 449 - 464.

Helmersen S.T. "Finding 'the Most Highly Qualified Publicists': Lessons from the International Court of Justice" 2019 30(2) *European Journal of International Law* 509–535.

Hoisington M. "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence" 2009 32 *Boston College International and Comparative Law Review* 439.

Hollis D.B. "Why States Need an International Law for Information Operations" 2007 11 *Lewis and Clarke Law Review* 1023.

Hoppe C. "Passing the Buck: State Responsibility for Private Military Companies" 2008 19 *European Journal of International Law* 989-1014.

Jennings R.Y. "The Caroline and McLeod Cases" 1938 32 *American Journal of International Law* 82-99.

Jensen E.T. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defence" 2002 38 *Stanford Journal of International Law* 207.

Jervis R. "Understanding the Bush Doctrine" 2003 118(3) *Political Science Quarterly* 365.

Jurich J.P. "Cyberwar and Customary International Law: The Potential of a 'Bottom-Up' Approach to an International Law of Information Operations" 2008 9 *Chicago Journal of International Law* 275.

Kanuck S. "Sovereign Discourse on Cyber Conflict Under International Law" 2010 88 *Texas Law Review* 1571.

Kesan J.P. and Hayes C.M. "Mitigative Counterstriking: Self Defence and Deterrence in Cyberspace" 2012 25 *Harvard Journal of Law and Technology* 429.

Kilovaty I. "Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare" 2015 4(3) *Journal of Law and Cyber Warfare* 210.

Kindt J.W. "Vessel-Source Pollution and the Law of the Sea" 1984 17 *Vanderbilt Journal of Transnational Law* 287.

Knopová M. and Knopová E. "The Third War in The Cyberspace? Cyber Warfare in the Middle East" 2014 3(1) *Acta Informatica Pragensia* 23.

Koskenniemi M. "The Politics of International Law" 1990 1 *European Journal of International Law* 4.

Kretzmer D. "The Inherent Right of Self-Defence and Proportionality in Jus ad Bellum" 2013 24 *European Journal of International Law* 235 282.

Levi W. "Ideology, Interests and Foreign Policy" 1970 14(1) *International Studies Quarterly* 1-31.

Li S. "When Does Internet Denial Trigger the Right of Armed Self-Defence?" 2013 38 *Yale Journal of International Law* 179.

Lin H.S. "Offensive Cyber Operations and the Use of Force" 2010 4 *Journal of National Security Law and Policy* 63.

Linnan D.K. "Self-Defence, Necessity and UN Collective Security" 1991 57 *Duke Journal of Comparative and International Law* 122.

Lotrionte C. "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law" 2018 3(2) *The Cyber Defence Review* 73-114.

Lubin A. "The Dragon-Kings' Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum" 2018 57 *Washburn Law Journal* 17-75.

Lund M.S., Hareide O.S., and Jøsok Ø. "An Attack on an Integrated Navigation System" 2018 3(2) *Necesse* 149.

McCarthy T. and Russell A. "Roadmap for a Code of Conduct for Cyberspace" 2017 3 *Fletcher Security Review* 8.

McGhee J.E. "Hack, Attack or Whack: The Politics of Imprecision in Cyber Law" 2015 4 *Journal of Law and Cyber Warfare* 13-41.

Melnitzky A. "Defending America Against Cyber Espionage Through the Use of Active Defences" 2012 20 *Cardozo Journal of International and Comparative Law* 537.

Merriam J.J. "Natural Law and Self-Defence" 2010 206 *Military Law Review* 43.

Mraković I. and Vojinović R. "Maritime Cyber Security Analysis – How to Reduce Threats?" 2019 13 *Transactions on Maritime Science* 132-139.

Naughton J. "The evolution of the Internet: from military experiment to General Purpose Technology" 2016 1(1) *Journal of Cyber Policy* 5-28.

Nguyen R. "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare" 2013 101(4) *California Law Review* 1079.

Nielsen S. "The Role of the U.S. Military in Cyberspace" 2016 15(2) *Journal of Information Warfare* 27-38.

Ozubide A. "How the Use of Force Against Non-State Actors Transformed The Law of Self-defence After 9/11" 2016 *SA Yearbook of International Law* 1-29.

Paquin L.G. "Why Did the League of Nations Fail?" 1943 34(3) *The Social Studies* 121-124.

Payne C.N. and Finlay L. "Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack" 2017 49 *George Washington International Law Review* 535.

Reisman W.M. and Armstrong A. "The Past and Future of the Claim of Preemptive Self-defence" 2006 100(3) *American Journal of International Law* 525-550.

Rid T. and Buchanan B. "Attributing Cyber-attacks" 2015 38 (1-2) *Journal of Strategic studies* 4-37

Roberts S. "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors" 2014 41 *Northern Kentucky Law Review* 535.

Robertson H.B. "Self-Defence against Computer Network Attack under International Law" 2002 76 *International Law Studies* 121 138.

Rockefeller M.L. "The 'Imminent Threat' Requirement for the Use of Preemptive Military Force: Is it Time for a Non-Temporal Standard?" 2004 33 *Denver Journal of International Law and Policy* 131.

Roell "Maritime Terrorism. A threat to world trade" 2009 *Institut für Strategie-Politik-Sicherheits-und Wirtschaftsberatung Berlin* 1-6

Roscini M. "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force" 2010 14 *Max Planck Yearbook of United Nations Law* 85-130.

Ruys T. "The Meaning of 'Force' And the Boundaries of the *Jus Ad Bellum*: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?" 2014 108(2) *The American Journal of International Law* 159-210.

Sadoff D.A. "A Question of Determinacy: The Legal Status of Anticipatory Self-Defence" 2009 40 *Georgetown Journal of International Law* 523.

Schaap A.J. "Cyber Warfare Operations: Development and Use Under International Law" 2009 64 *Air Force Law Review* 121 156.

Schmitt M.N. "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework" 1999 37(3) *Columbia Journal of International Law* 898.

Schmitt M.N. "Cyber Operations and the Jus ad Bellum Revisited" 2011 56(3) *Villanova Law Review* 569.

Schmitt M.N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 54 *Harvard International Law Journal* 18.

Schmitt M.N. "Preemptive Strategies in International Law" 2003 24 *Michigan Journal of International Law* 513.

Schmitt M.N. "The Law of Cyber Warfare: Quo Vadis?" 2014 25 *Stanford Law and Policy Review* 269.

Schuller A.L. "Inimical Inceptions of Imminence – A New Approach to Anticipatory Self-Defence under the Law of Armed Conflict" 2014 18 *UCLA Journal of International Law and Foreign Affairs* 161-206.

Shackelford S.J. "From Nuclear War to Net War: Analogizing Cyber-attacks in International Law" 2009 27 (1) *Berkeley Journal of International Law* 192.

Shackelford S.J. "The Law of Cyber Peace" 2017 18(1) *Chicago Journal of International Law* 1.

Shackelford S.J. and Andres R.B. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem" 2011 42 *Georgetown Journal of International Law* 971.

Silver D.B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter" 2002 76 *International Law Studies* 73.

Simmons A.J. "On the Territorial Rights of States" 2001 11 *Philosophical Issues* 300-326.

Skelrov M. J. "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defences Against States Who Neglect Their Duty to Prevent" 2009 201 *Military Law Review* 1.

Stahl W.M. "The Unchartered Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cyber Security" 2011 40 *Georgia Journal of International and Comparative Law* 247.

Steenhoven N. "Conduct and Subsequent Practice by States in the Application of the Requirement to Report under UN Charter Article 51" 2019 6(2) *Journal on the Use of Force and International Law* 242-272.

Stevens S.R. "Internet War Crimes Tribunals and Security in an Interconnected World" 2009 18(3) *Transnational Law and Contemporary Problems* 657-720.

Svarc D. "Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-first century" 2006 13 *ILSA Journal of International and Comparative Law* 171.

Taft IV W.H. "Self-Defence and the Oil Platforms Decision" 2004 29 *Yale Journal of International Law* 295.

Todd G.H. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition" 2009 64 *Air Force Law Review* 65.

Tøndel I.A., Line M.B., and Jaatun M.G. "Information security incident management: Current practice as reported in the literature" 2014 45 *Computers & Security* 42-57.

Totten M. "Using Force First: Moral Tradition and the Case for Revision" 2007 43 *Stanford Journal of International Law* 95.

Tsagourias N. "Cyber-attacks, Self-defence and the Problem of Attribution" 2012 *Journal of Conflict and Security Law* 229-244.

Uma M. and Padmavathi G. "A Survey on Various Cyber-attacks and Their Classification" 2013 15 (5) *International Journal of Network Security* 390-396.

Waldock H. "The Regulation of the Use of Force by Individual States in International Law" 1952 81 *Academie De Droit International Recueil De Cours* 451.

Waxman M.C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" 2011 36 *Yale Journal of International Law* 421.

Weightman M.A. "Self-Defence in International Law" 1951 37(8) *Virginia Law Review* 1095-1115.

Weissbrodt D. "Cyber-Conflict, Cyber-Crime and Cyber-Espionage" 2013 22 *Minnesota Journal of International Law* 347.

Wortham A. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent that May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" 2012 64(3) *Federal Communications Law Journal* 643.

Wrathall L.R. "The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward" 2010 12 *San Diego International Law Journal* 223.

Yang W. "The Freedom of Navigation in the South China Sea: An Ideal or a Reality?" 2012 3 *Beijing Law Review* 137, 140–41.

Conference Papers, Seminars, Symposia and Lectures

Scott S. 'The UNCLOS as an International Regime', Paper presented at the 3rd Verzijl Symposium, Utrecht, 2004.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A security evaluation of AIS automated identification system. In Proceedings of the 30th annual computer security applications conference (pp. 436-445).

Bateman "Regional Maritime Security: Threats and Risk Assessments" 2010 University of Wollongong Research Online, Faculty of Law - Papers (Archive).

Benard “Port security - Threat and Vulnerability, Case: Takoradi Port” *Thesis from Degree Programme in Security Management* Laurea University of Applied Sciences, Leppävaara 2015

Bothur D., Zheng G., & Valli C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In Valli, C. (Ed.). (2017). *The Proceedings of 15th Australian Information Security Management Conference*, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.81-87).

Brantly A.F. “The Cyber Deterrence Problem” in Minárik *et al* (Eds.) 2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects, NATO CCD COE Publications, Tallinn 31.

DeWeese G.S. “Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence” 2015 7th International Conference on Cyber Conflict Architectures in Cyberspace 81, 92.

Hayes C.R. “Thesis Titled ‘Maritime Cybersecurity: The Future of National Security’” 2016 *Naval Postgraduate School Monterey, California* 6.

Hon. Harold Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012), <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> accessed 18th May, 2019.

Remarks by TB Koh, reproduced in UN *The Law of the Sea: Official Text of the UNCLOS* (London 1983) xxxiii.

Tom Ruys. (2015). Divergent Views on the Charter Norms on the Use of Force—A Transatlantic Divide? *Proceedings of the Annual Meeting (American Society of International Law)*, 109, 67–70.

Schmitt M.N. “Attack” as a Term of Art in International Law: The Cyber Operations Context’ 2012 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.

Reports, Policies and Draft Policies

2050 Africa Integrated Maritime Strategy (AIMS),

Abdyraeva C. *The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends* 2020 Report. OIIP - Austrian Institute for International Affairs 32.

Bannelier, K., Bozhkov, N., Delerue, F., Giumelli, F., Moret, E., & Van Horenbeeck, M. (2019). MISSION CONTROLS: Sanctions under international law. In P. Pawlak & T. Biersteker (Eds.), *GUARDIAN OF THE GALAXY: EU cyber sanctions and norms in cyberspace* (pp. 43–51). European Union Institute for Security Studies (EUISS). www.jstor.org/stable/resrep21136.8 accessed on 20 July 2020

Bruner T. “Double Standard on Due Diligence in Cyberspace” 2020 *Peace Research Centre Prague Policy Brief*.

Council of the European Union, European Union Maritime Security Strategy (11205/14) (24 June 2014).

Daigle L. ‘On the Nature of the Internet’ in Global Commission on Internet Governance Report *A Universal Internet in a Bordered World* 2016 Centre for International Governance Innovation

Department of Homeland Security “National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security” October, 2005 https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf

DoD Digital Modernization Strategy 2019 Department of Defence Office of Publication and Security Review 29 available at <https://media.defence.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>

ECOWAS and Integrated Maritime Strategy (EIMS)

Fink J.E. *Meeting the Challenge: A Guide to United Nations Counterterrorism Activities*. Report of International Peace Institute, (2012) 80.

Government Accountability Office, Weapons Systems Cybersecurity GAO-19-128 (October 18, 2018) Report to the Committee on Armed Services, U.S. Senate 41.

IHS Markit *Maritime Cyber Security Results 2018*

Lipson H.F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy* (Special Report) (2002) Carnegie Mellon University 13.

Rahman C. *Concepts of Maritime Security: A Strategic Perspective on Alternative Visions for Good Order and Security at Sea, with Policy Implications for New Zealand* (2009) Wellington, NZ: Centre for Strategic Studies: New Zealand, Victoria University of Wellington.

Schmitt M.N. *Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy* 2010 Washington: National Academies Press 155.

Schmitt, M. N. (2007). Responding to transnational terrorism under the Jus ad Bellum: a normative framework. In *International Law and Armed Conflict: Exploring the Faultlines* (pp. 157-195). Brill Nijhoff/Siman-Tov et al *A New Level in the Cyber War between Israel and Iran*. Report. Institute for National Security Studies, 2020.

Special Committee on the Question of Defining Aggression, UN GAOR, 4th Session, 82nd meeting at 20 (Mexico), UN Doc. A/AC.134/SR.82 (June 7, 1991).

UN resolutions 2018 and 2039,

UNGA "Oceans and the Law of the Sea: Report of the Secretary General" (10 March 2008) UN Doc A/63/63

United Nations Secretary General 2004 High Level Panel Report on Threats, Challenges and Change, A more Secure World: Our Shared responsibility.

US Justice Department *White Paper* "Lawfulness of a Lethal Operation Directed against a US Citizen Who is a Senior Operational Leader of Al-Qa'da or an Associated Force" 2011 7 available at <https://fas.org/irp/eprint/doj-lethal.pdf> accessed on 17th August, 2019.

Yannakogeorgos P.A. "The Cyber Environment" in *Strategies for Resolving the Cyber Attribution Challenge* (2013) (pp. 9-34, Report). Air University Press.

Newspapers, Radio Broadcast and Newsletters

Bostock I. "Canberra Would Order Pre-Emptive Strikes" *Jane's Defence Weekly* December 11, 2002, p.18.

Gjelten T. "Extending the Law of War to Cyberspace" National Public Radio, Aired on September 22, 2010.

Japan Threatens Force Against N Korea" *BBC News World Edition*, February 14, 2003.

Websites

Australia Joins US-led Naval Mission in Strait of Hormuz
<https://www.aljazeera.com/news/2019/08/australia-joins-led-naval-mission-strait-hormuz-190821071113310.html> (accessed 2019-08-21).

BBC News World Edition, 16 October 2002,
http://news.bbc.co.uk/2/hi/middle_east/2334865.stm (accessed 2019-06-20)

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, The Guidelines on Cyber Security Onboard Ships, Ver. 2.0, 2017, p.51 <http://www.ics-shipping.org/docs/default-source/resources/safety-security-andoperations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14> (accessed 2019-12-03).

Caroline Glick, Column One: The lessons of Stuxnet. Jerusalem Post. (1 October 2010) <http://www.jpost.com/Opinion/Columnists/Article.aspx?id=189823>).

Chronis Kapalidis "Cyber Security Challenges for the Maritime Industry" 30/07/2019.
<https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/>
(accessed 2020-01-22).

Cyber bits – Hackers deployed to facilitate drugs smuggling (available at www.europol.europa.eu (accessed 2018-03-25)).

CyRiM Project 2009 *Shen Attack: Cyber risk in Asia Pacific Ports* 13 https://www.msg-asia.com/sites/msg_asia/files/downloads/CyRiM_ShenAttack_FinalReport.pdf (accessed 2019-12-19).

Danyliw RFC 7970: The Incident Object Description Exchange Format Version 2, IETF, Nov 2016, p.172 <https://tools.ietf.org/html/rfc7970> (accessed 2019-12-03).

Department of Defence Cyberspace Policy Report, A Report to Congress Pursuant to the National Defence Authorization Act for Fiscal Year 2011, Section 934 (November 2011) (available at www.defence.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20section%20934%20Report_For%20webpage.pdf).

Dewar R.S. “The ‘Triptych of Cyber Security’: A Classification of Active Cyber Defence” (6th Annual Conference on Cyber Conflict, 2014), NATO Cooperative Cyber Defence Centre of Excellence, https://www.ccdcoe.org/uploads/2018/10/d1r1s9_dewar.pdf (accessed 2018-10-20).

Directive 2008/114/EC, Articles 2 and 3 [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI\(2021\)662604_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf) (accessed 2021-08-09).

DiRenzo J., Goward A.D., and Roberts F.S. “The little-known challenge of maritime cybersecurity” in *Information, Intelligence, Systems and Applications (IISA) 2015 6th International Conference* 1-5 IEEE. <http://dimacs.rutgers.edu/archive/People/Staff/froberts/MaritimeCyberCorfuPaper.fina.pdf> (accessed 2019-06-05).

DoD OGC (1999). An Assessment of International Legal Issues in Information Operations. Second edition; November. Arlington: Department of Defence, Office of General Counsel. Available at: <http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc> (accessed 2019-08-15).

Doffman Z. "Israel Responds to Cyber-attack with Air Strike on Cyber-attackers in World First" <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/> (accessed 2019-05-07).

European Network and Information Security Agency (ENISA) 2011 Report on 'Analysis of Cyber Security Aspects in the Maritime Sector' 1-2 (available at https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport (accessed 2018-03-12)).

Furness-Smith "Maritime industry must open up about cyber crime" <https://loydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime> (accessed 2019-09-03).

Gorman S. "U.S. Plans Cyber Shield for Utilities, Companies" Wall Street Journal (July 8, 2010, 12:01 AM), <https://www.wsj.com/articles/SB10001424052748704545004575352983850463108> (accessed 2019-08-26).

Harold Koh, "The Obama Administration and International Law," speech, American Society of International Law, 25 March 2010, <http://www.state.gov/s/l/releases/remarks/139119.htm> (accessed 2019-08-15).

Hon. Harold Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012), <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> (accessed 2019-05-18).

Hosanee "A Critical Analysis of Flag State Duties as Laid Down under Article 94 of the 1982 United Nations Convention on the Law of the Sea" *The United Nations-Nippon Foundation Fellowship Programme 2009–2010*, 23, https://www.un.org/Depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/hosanee_0910_mauritius.pdf (accessed 2020-07-18).

<http://ccdcoe.org/organisations/au/> (accessed 2020-06-10).

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.694.7968&rep=rep1&type=pdf> (accessed 2019-06-10).

<http://www.al-bab.com> (accessed 2019-06-20).

<http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx> (accessed 2020-06-05).

[http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/Pages/Cyber-security.aspx](http://www.imo.org/en/OurWork/Security/Guide%20to%20Maritime%20Security/Pages/Cyber-security.aspx) (accessed 2020-02-11).

http://www.nato.int/docu/review/2010/maritime_security/end_of_naval_era/en/index.htm (accessed 2019-06-26).

<http://www.navy.mil/maritime/Maritimestrategy.pdf> accessed on 2019-06-26.

<http://www.sciencedirect.com/science/article/pii/S0167404814000819> accessed on 2019-12-03.

http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm accessed on 2019-06-25.

<https://dryadglobal.com/maritime-cyber-security-threats-december-2019-week-five/> accessed on 2019-12-16.

<https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html> accessed on 2019-06-26.

<https://history.state.gov/milestones/1937-1945/un> accessed on 2021-03-24.

<https://iclg.com/practice-areas/shipping-laws-and-regulations/2-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels> accessed on 2020-06-04.

<https://mobile.twitter.com/IDF/status/1125066395010699264> accessed on 2019-05-07.

<https://oceanexplorer.noaa.gov/technology/tools/scs/scs.html> accessed on 2019-12-19.

<https://perma.cc/P8V5-VVYD> accessed on 2018-05-21.

<https://rntfnd.org/wp-content/uploads/Multi-sig-Ltr-to-USCG-IMO-GNSS-Jamming.pdf> accessed on 2019-06-27

<https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/> accessed on 2019-12-14.

<https://safety4sea.com/cm-security-measures-a-brief-review-of-isps-code-implementation/> accessed on 2020-01-31.

<https://seanews.co.uk/security/cyber-security/naval-dome-receives-dnv-gls-cyber-security-certification/> accessed on 2019-04-04.

<https://thelaodstar.com/alert-to-logistics-and-shipping-as-digital-detectives-uncover-new-cyber-attack/> accessed on 2019-10-01.

<https://thelawdictionary.org/crime/> accessed on 2020-09-08.

<https://thelawdictionary.org/motive/> accessed on 2019-03-14.

<https://us.norton.com/Internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html>

<https://www.cisa.gov/infrastructure-security> accessed on 2021-08-09.

<https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyber-attack-will-lead-to-a-shift.html> accessed on 2019-05-07.

<https://www.cybersecurityintelligence.com/blog/israel-responds-to-a-cyber-attack-with-bombs-4271.html> accessed on 2020-07-31.

<https://www.dhs.gov/topic/critical-infrastructure-security> accessed on 2020-10-23.

https://www.google.com/search?q=meaning+of+effect&rlz=1C1CHBD_enNG735NG735&oq=meaning+of+effect&aqs=chrome..69i57j0l5.11652j1j4&sourceid=chrome&ie=UTF-8 accessed on 2019-04-29.

<https://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx> accessed on 2020-11-11.

<https://www.marineinsight.com/guidelines/a-guide-to-types-of-ships/> accessed on 2020-04-03.

<https://www.maritime-executive.com/article/maib-overheated-cargo-caused-stolt-groenland-explosion> accessed on 2021-07-23.

<https://www.maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports> accessed on 2019-12-20.

<https://www.merriam-webster.com/dictionary/imminence> accessed on 2019-08-28.

<https://www.merriam-webster.com/dictionary/permissive> accessed on 2019-03-14.

<https://www.merriam-webster.com/dictionary/scale> accessed on 2019-04-29.

<https://www.npr.org/templates/story/story.php?storyId=130023318> accessed on 2019-03-22.

<https://www.oceancouncil.org/event/global-maritime-security-conference/> accessed on 2020-07-18.

<https://www.reuters.com/article/us-iraq-security-blast-intelligence/trump-says-soleimani-plotted-imminent-attacks-but-critics-question-just-how-soon-idUSKBN1Z228N> accessed on 2020-01-07.

https://www.sfmex.org/wp-content/uploads/2019/04/2019-04_AMSC-Cyber-Newsletter.pdf accessed on 2019-09-03.

<https://www.strath.ac.uk/research/strathclydecentreenvironmentallawgovernance/our-work/research/labsincubators/lawandgovernanceoftheglobalcommonsincubator/> accessed on 2020-10-28.

<https://www.techopedia.com/definition/24152/information-and-communications-technology-ict> accessed on 2020-10-14.

<https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/> accessed on 2019-08-17.

<https://www.un.org/un70/en/content/history/index.html> accessed on 2020-02-21.

<https://www.ungeneva.org/en/history/league-of-nations> accessed on 2021-08-02.

Ivezic “Defeating 21st Century Pirates: The Maritime Industry and Cyber-attacks” (8 January 2018) (available at www.csoonline.com (accessed on 2018-03-25)).

Koh ‘A Constitution of the World’s Oceans’ Remarks of the President of the Third United Nations Conference on the Law of the Sea at the Conference at Montego Bay

(December 1982)
http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm accessed on 2020-10-28.

Koskenniemi M. 'Iraq and the "Bush Doctrine" of Pre-emptive Self-Defence. Expert analysis', Crimes of War Project, 20 August 2002, www.crimesofwar.org/expert/bushkoskenniemi.html Accessed on 2021-04-06.

Krasny "Chinese hacked U.S. military contractors: Senate panel" (18 September 2014) (available at www.reuters.com/article/us-usa-military-cyberspying/chinese-hacked-u-s-military-contractors-senate-panel-idUSKBN0HC1TA20140918 (accessed on 2018-03-25)).

Kuehn B.M. "Pacemaker Recall Highlights Security Concerns for Implantable Devices" www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.118.037331 accessed on 2020-02-17.

League of Nations *Covenant of the League of Nations*, 28 April 1919, available at: <https://www.refworld.org/docid/3dd8b9854.html> (accessed on 2021-03-22).

Look "Two Major Cyber-attacks Have Targeted Kuwait Transportation and Shipping Industry This Year" Published on October 1, 2019 <http://www.marsecreview.com/2019/10/two-major-cyber-attacks-have-targetted-kuwait-transportation-and-shipping-industry-this-year/> accessed on 2019-12-16.

Lt. Col. W.A. "Stafford How to Keep Military Personnel from Going to Jail for Doing the Right Thing: jurisdiction, ROE & the Rules of Deadly Force" 2000 *Army Law* November 5 http://www.au.af.mil/au/awc/awcgate/law/roe_deadlyforce.pdf accessed on 2019-09-02.

Malware, Norton (available at http://us.norton.com/security_response/malware.jsp (accessed 2018-01-24)).

Miller *Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, British-American Diplomacy, The Caroline Case*, at https://avalon.law.yale.edu/19th_century/br-1842d.asp accessed on 2019-08-04.

O'Connell 'Cyber Mania' in *Cyber Security and International Law: Meeting Summary*
2012 Chatham House 5

<https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf> accessed on 2019-02-19.

Paganini "Hacking Ships: Maritime Shipping Industry at Risk" (31 March 2015)
(available at <http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html> (accessed on 2018-03-12)).

President Bush's 2003 State of the Union Address,
http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/bushtext_012803.html

Ramachandran "How Artificial Intelligence is Changing Cyber Security Landscape and Preventing Cyber-attacks" Entrepreneur India 14th September 2019 available at <http://www.entrepreneur.com/article/339509> accessed on 2019-09-16.

Randrianantenaina "Maritime Piracy and Armed Robbery against Ships: Exploring the Legal and the Operational Solutions. The Case Of Madagascar" 2013 Division For Ocean Affairs and the Law of the Sea Office of Legal Affairs, The United Nations New York 18-19
https://www.un.org/depts/los/nippon/unff_programme_home/fellows_pages/fellows_papers/Randrianantenaina_1213_Madagascar.pdf accessed on 2019-06-26.

Reiskind "Cyber Security and Maritime Commercial Shipping: Is Everything Ship Shape?" 2018 NAOC NATO Association of Canada available at <http://natoassociation.ca/cyber-security-and-maritime-commercial-shipping-is-everything-ship-shape/> accessed on 2019-06-05.

Roberts "A New Frontier: Defining Cyber-Attack and the Ramifications for Jus ad Bellum and Jus in Bello Law" 2017 12 (Available at <https://ssrn.com/abstract=3009377> (accessed on 10th December, 2018)).

Roell "Maritime Security: New Challenges for Asia and Europe" 2011 167 Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) Berlin, ISPSW Strategic Series <http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=134578> (accessed on 2019-06-20).

Russian Cyberattack Unit ‘Masqueraded’ as Iranian Hackers, UK Says” <https://www.ft.com/content/b947b46a-f342-11e9-a79c-bc9acae3b654> accessed on 2019-10-21.

Safire “The Farewell Dossier” *New York Times*, 2 February 2004, <http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsafire> accessed on 2019-04-15.

Sakhuja “Security threats and challenges to maritime supply chains” https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2959.pdf accessed on 2019-12-12.

Schmitt & Vihul “International Cyber Law Politicized: The UN GGE Failure to Advance Cyber Norms” *Just Security* 30 June, 2017 www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ accessed on 2020-07-20.

Schneier, “It will soon be too late to stop the cyberwars” *Financial Times*, 2 December 2010, <http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzz19cNCeszp> accessed on 2019-05-23.

Shah “The Bush Doctrine of Pre-emptive Strikes; A Global Pax Americana” *Global Issues* (24 April 2004) (available at <http://www.globalissues.org/article/450/the-bush-doctrine-of-pre-emptive-strikes-a-global-pax-americana> (accessed on 2018-09-18)).

Shauk “Malware offshore: Danger lurks where the chips fail” April 29, 2013 <http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/> accessed on 2019-06-10.

Sofaer *et al* ‘Cyber Security and International Agreements’ Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy (available at <http://www.nap.edu/catalog/12997.html> (accessed on 2018-02-20)).

Strengthening Maritime Security: objectives 2019 to 2020” published on 19th September, 2019 by the Foreign and Commonwealth Office <https://www.gov.uk/government/publications/official-development-assistance-oda->

[fco-international-programme-spend-objectives-2019-to-2020/strengthening-maritime-security-objectives-2019-to-2020](#) accessed on 2019-10-10.

The National Security Strategy of the United States of America, <http://www.state.gov/documents/organization/63562.pdf>

The White House Washington *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* 2003 60. Available at https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf .

Trump Administration 2017 National Security Strategy 31 available at: <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> accessed on 2019-06-04.

UAE confirms oil tanker attack, Al Jazeera, <http://www.aljazeera.com/news/middleeast/2010/09/20108683953783853.html> (accessed on 2019-06-20).

UNGA “Report of the Secretary-General. Oceans and the Law of the Sea” (10 March 2008) UN Doc A/63/63, para.39, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N08/266/26/PDF/N0826626.pdf?OpenElement> accessed on 2020-05-08.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015, p.12 <https://undocs.org/A/70/174> accessed on 2020-06-03.

UNODC “UNODC Global Maritime Crime Programme” United National Office on Drugs and Crime, 2016, <https://www.unodc.org/unodc/en/piracy/index.html?ref=menuside> accessed on 2020-02-12.

US Department of Defence, Cyber Command Fact Sheet (25 May 2010) (available at www.defence.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%202010%20fact%20sheet.pdf).

US GAO – Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cyber Security (available at www.gao.gov (accessed on 2018-03-25)).

Van De Velde “The Law of Cyber Interference in Elections” (2017) available at SSRN: <https://ssrn.com/abstract=3043828> accessed on 2019-04-01.

Watt “Moving from Reactive Cyber Security to Proactive Cyber Security: Six Steps to Achieving Resilience” <https://federalnewsnetwork.com/kpmg/2019/07/moving-from-reactive-cyber-security-to-proactive-cyber-security-six-steps-to-achieving-resilience/> accessed on 2019-07-31.

Waxman “5 Things to Know About the League of Nations” (25 January 2019) <https://time.com/5507628/league-of-nations-history-legacy/> accessed on 2021-03-24.

World Briefing | Asia: The Philippines: Bomb Caused Ferry Fire <https://www.nytimes.com/2004/10/12/world/world-briefing-asia-the-philippines-bomb-caused-ferry-fire.html> (accessed on 2019-06-20).

www.maritimeterrorism.com/definitions/ accessed on 2019-06-20.