Maritime cybersecurity Risk Management in the Fourth industrial revolution

JC Theron

orcid.org/0000-0002-1508-9672

Mini dissertation accepted in partial fulfilment of the requirements for the degree *Master of Law in International Trade Law* at the North-West University

Supervisor: Dr B Klaasen

Graduation : July 2023

Student number: 27084736

30 November 2022

Declaration

I, Jan-Christian Theron, do declare that "Maritime Cybersecurity Risk Management in the Fourth Industrial Revolution" is my original work and has not been submitted for any degree in any other university. While I have relied on numerous sources and materials in this mini-dissertation, I have duly and properly acknowledged all the materials and sources used.

X

Christian Theron
27084736

30/11/2022

List of Abbreviations

4IR	4th Industrial Revolution
ADP	Advanced Digital Production
AI	Artificial Intelligence
ALARP	As Low as Reasonably Practicable
BIMCO	Baltic and International Maritime Council
C-ES	Cyber-Enabled Systems
CIA	Central Intelligence Agency
CII	Critical Information Infrastructure
CIM	Computer Integrated Manufacturing
COSCO	China Ocean Shipping Company
CPS	Cyber-Physical System
DCSA	Digital Container Shipping Association
DDOS	Distributed Denial of Service
FSA	Formal Safety Assessment
GDPR	European Union's General Data Protection Regulation
GPS	Global Positioning System
HCI	Human Computing Interactions
ICCPR	International Covenant on Civil and Political Rights
IMO	International Maritime Organisation

IT	Information Technology
ISM	International Safety Management
ISPS	International Ship and Port Facility Security Code
JIT	Just-in-Time
MFA	Multi Factor Authentication
NBA	Network Behavioural Analysis
NBI	National Bureau of Investigation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PARC	Palo Alto Research Centre
PNP	Philippine National Police
SAPS	South African Police Service
SCC	Shore Control Centre
SMS	Safety Management System
SSP	Ship Security Plan
STCW	International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
TOC	Theory of Constraint
UDHR	United Nations' Universal Declaration of Human Rights
UNIDO	United Nations Industrial Development Organization
WAF	Sandboxing and Web Application Firewalls

List of Keywords

- Maritime cybersecurity
- Fourth industrial revolution
- Risk mitigation
- Risk management programmes
- Cyberattacks

1 Introduction

1.1 *Background*

The transporting of 90% of goods in the world is accounted for by the maritime industry, and this requires specially designed ships and widespread infrastructure. Because this sector is worth trillions and reaches across the world, it is exposed to a diverse range of risks.[1]

Mraković and Vojinović defines maritime cyber risks as follows:

> Maritime cyber risks refer to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in a shipping-related operational, safety or security failure as a consequence of information or systems being corrupted, lost or compromised.[2]

Cybersecurity is becoming increasingly important in the maritime industry as cyber-attacks are on the rise. Maritime cybersecurity can be defined as measures that should be taken to protect both networks and computer assets on ships, terminals and ports.[3] Based on this definition, a cyber-attack can be defined as an attempt to disrupt any communication networks or systems that control ports or ships.[4]

Hayes[5] stated that in 2020, cyber-attacks had increased by almost 400% just in the maritime sector.[6] The future of maritime transport lies in digitization brought forth by the Fourth Industrial Revolution (hereinafter the 4IR). The technology provided by the 4IR leads to a supply chain that is more effective and transparent but attracts cybercrime groups who try to steal data or sabotage equipment.[7] Cyber-Attackers use different *modus operandi* to access systems where they can then perform their business and start hacking and creating cyber risks. This *modus operandi* that are

1 Jones *Factors Affecting Cyber Risk in Maritime* 1.
2 Mrakovic and Vojinovic 2019 *TOMS* 133.
3 Hayes *MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY* 6.
4 Hayes *MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY* 6.
5 Hayes *MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY* 6.
6 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.
7 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.

being used include the use of phishing.[8] Phishing[9] can be defined in different ways, one of them being a cyber-attack that uses emails that are disguised as a form of a weapon, with the goal to lead a recipient of such a mail to believe that the disguised email is something that they need.[10]

One of the biggest and most damaging cyber-attacks occurred in 2017 when Maersk[11] lost 300 million dollars due to a cyber-attack which is now known as one of the worst cyber-attacks in the world.[12] This cyber-attack happened due to a ransomware virus infecting the company's reservation system. The effect of this cyber-attack led to a congestion of 80 ports worldwide.[13] After the NotPetya[14] attack in 2017 that cost Maersk between 250 and 300 million Dollars,[15] attacks started to increase at an alarming rate. In the year 2018 the ports of Barcelona and San Diego were under attack.[16] The Australian shipbuilder Austal was hit,[17] and the attack on China Ocean

---

8 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.

9 Phishing is a type of cybercrime and social engineering in which cyberattackers makes use of fraudulent messages and attempts to trick or mislead innocent parties to reveal sensitive information to the attackers, whereby the attackers gain access to sensitive data such as bank credit card details and passwords.
Fruhlinger 2020 https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

10 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.

11 MAERSK is a Danish company that specializes in international container shipping, inland freight transportation and associated services, which includes supply chain management and port operation.

12 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.

13 Anon 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/.

14 The NotPetya attacks can be defined as a series of powerful cyberattacks that occurs through the use of Petya malware.
Banerjea 2018 https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html.

15 Allen 2018 *USFMLJ.*

16 On 20 September 2018 an attack was launched on the port of Barcelona and several internal servers of the organisations has been affected by this attack, and on the 25th of September 2018 an attack was launched on the port of San Diego. The attack is a threat to technology systems, and it is affecting the publics agency's ability to process park permits. Paganini 2018 https://securityaffairs.co/wordpress/76623/hacking/port-of-san-diego-attack.html#:~:text=A%20few%20days%20ago%20the,Diego%2C%20in%20the%20United%20States.

17 The Australia-based group made it official that its database management system was reeling under a cyber-attack from an unknown offender. The group of attackers behind the attack tried to sell accessed information on the dark web and tried to join hands with online terrorists. Goud date unknown https://www.cybersecurity-insiders.com/australian-defense-shipbuilder-austal-hit-by-cyber-attack/.

Company (also known as COSCO)[18] took down half of the ship owners' US network.[19] The above-mentioned indicate that cyber-security threats in the maritime sector are evolving at an alarming rate and they also have extreme financial implications. While the 4IR has led to more and more digitization, it also increases the chances of cyber-attacks as technology continues to evolve.[20]

In this dissertation the following will be discussed; firstly, the history of cybersecurity, where it comes from and what it is, followed by cybercrimes that have created problems in the maritime industry. The 4IR will be discussed after the completion of the discussion of cybercrimes and cybersecurity. The final two chapters of this dissertation will discuss firstly maritime risk management and management programmes together with formal safety assessments after which cyber risk mitigation will be analysed. Together with cybercrimes and the history of cybercrimes there will be a discussion about different domestic, foreign and international legislation and regulations that are put into place to combat cybersecurity threats. The domestic legislation includes the *Electronic Communications and Transactions Act*[21] and the *Cybercrimes Act*.[22] In these statutes the discussion will be around the relevant jurisdiction over persons committing offences in terms of the legislation and further penalties that are available for these crimes. In terms of foreign legislation, the discussion will focus on a few countries that can be classified as world powers and that are on the forefront of technology, and how their approach to cyber-activities differs and how each country handles said cyber-activities. This foreign legislation will include the following countries' approaches, the United States of America, China, Germany and the Philippines.

---

18 COSCO Shipping Lines were hit by a cyber-attack that has impacted the digital assets of the ocean water carrier's communication in the American region only. Anon 2018 https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/.

19 Arampatziz 2020 https://www.tripwire.com/state-of-security/featured/cyber-resilient-critical-maritime-industry/.

20 After the NotPetya attack in 2017 that cost Maersk more than 300 million Dollars, attacks started increasing at an alarming rate. Henriquez 2022 https://www.securitymagazine.com/articles/96972-merck-wins-14b-lawsuit-over-notpetya-.attack#:~:text=Maersk%2C%20for%20instance%2C%20ended%20up,data%20that%20the%20malware%20encrypted.

21 *Electronic Communications and Transactions Act* 25 of 2002.

22 *Cybercrimes Act* 19 of 2020.

In terms of international legislation, the discussion will be around the EU *Cybersecurity Act*,[23] as well as the *Budapest Convention on Cybercrime*[24] and the *African Union Convention on Cybersecurity and Personal Data Protection*, 2014.[25]

The question that needs to be answered surrounding legislation is whether this legislation, national, foreign and international has the capacity and ability to deal with the 4IR effectively.

1.2 Research Question

How can cybersecurity-risk in the maritime sector be managed and mitigated in the Fourth Industrial Revolution?

1.3 Research Methodology

This study aims to discuss the maritime cybersecurity threats that there are in the world; and how these attacks happen and what the effects of these cyber-attacks are on the maritime sector. This study also aims to discuss what risk management is in the maritime sector and how risks in this sector can be mitigated and reduced. In this study, previous cyber-attacks will also be evaluated to determine and discuss how to approach risk management and mitigation of risks. This study comprises of a critical review of the applicable legislation and an examination of case law where applicable, electronic sources, textbooks, and academic articles after which maritime cybersecurity risk management and mitigation of risks will be evaluated. In this study a comparative study will be done with the different laws relating to cybersecurity of countries such as China, Germany, Russia and the Philippines as well a discussion of the EU Cybersecurity Act and relevant principles relating to cybersecurity.

1.4 Research Aims and Objectives

The aim of this research project is to understand maritime cybersecurity, where it came from and how it works. The aim is to understand the impact of the 4th Industrial

---

23 *EU Cybersecurity Act* of 2019.
24 *Budapest Convention on Cybercrime*, 2001.
25 *African Union Convention on Cyber Security and Personal Data Protection*, 2014.

Revolution and its effect on maritime cybersecurity. A further aim is to determine how the risks of cyber-attacks can be managed or mitigated. Understanding the impact of the 4th Industrial Revolution might lead to a better understanding of the risks of cybersecurity in the maritime sector. The objective of this study is to firstly begin by looking at the history of maritime cybersecurity. To determine when cybersecurity became important in the maritime sector, followed by the 4th Industrial Revolution. To further determine how does the 4th Industrial Revolution affect the maritime sector and to discuss how this has changed the entire maritime sector from the way ships operate all the way to the ports safety. After having discussed the 4th Industrial Revolution and the history of maritime cybersecurity, to also discuss the risk management strategies and guidelines that was set out to protect against cyberattacks. To follow is the mitigation of risks to determine if cyberattacks cannot be prevented entirely, or how the risk of cyberattacks can be minimized.

1.5 Framework

Chapter two lays out the basis surrounding the dissertation. In this chapter the 4IR will be defined and there will also be focussed on what the technologies are in the $IR and the technologies the 4IR is based upon.

Chapter three will deal overall with cybersecurity, but in chapter three focus will be placed on the history of cybercrime as well as cybercrimes in the maritime sector. Later in the chapter focus will shift to the enforcement of cybercrimes after which the South African, Foreign and International laws for cybersecurity will be discussed.

Chapter four will be dealing with maritime cybersecurity risk management and an important aspect will be discussed namely how to build cyber resilience, as well as the central components to achieve effective cyber resilience. Chapter four will be concluded by a discussion of maritime formal safety assessment.

Chapter five will commence with the mitigation of risk and how risks in the maritime industry can be mitigated whereafter chapter six will present a summary and concluding remarks.

2 Fourth Industrial Revolution

2.1 What is the Fourth Industrial Revolution?

The founder and the executive chairman of the World Economic Forum (WEF), Klaus Schwab, has used the term Fourth Industrial Revolution to define and describe characteristics of the convergence and complementation of emerging technology fields.[26] The emerging technology domains include the following; nanotechnology, biotechnology, new materials and Advanced Digital Production (hereinafter ADP) technologies.[27] It is indeed true that the 4IR is the product of a technological advancement, but what makes it unique is the fact that it blurs the boundaries between the biological, the physical and the digital realms.[28]

The rapid and relentless rise in the 1990s gave birth to the internet, networking, and digital communications, which together constitute 'cyberspace' as we experience it today.[29] This cyberspace has produced startling changes to all the aspects of our lives.[30] This accelerated growth of cyberspace has led to a new industrial revolution which we now know as the 4IR.[31] Each sector has been affected by the 4IR, whether it was directly or indirectly. The 4IR has changed the way we live and work and it also led to the adoption use of cyber-physical systems would make cyber-attacks more likely.[32] One of the biggest changes the 4IR brings is the digital transformation in shipping as it is moving in the direction of emerging to becoming crew-less vessels that only rely on technology.[33] The 4IR has given rise to two kinds of vessels namely, remotely operated vessels and autonomous vessels, both of which are referred to as

---

26 Lavopa and Delera 2021 https://iap.unido.org/articles/what-fourth-industrial-revolution#fn-542-1.
27 Lavopa and Delera 2021 https://iap.unido.org/articles/what-fourth-industrial-revolution#fn-542-1.
28 Lavopa and Delera 2021 https://iap.unido.org/articles/what-fourth-industrial-revolution#fn-542-1.
29 Barthwal and Agarwala 2020 https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/.
30 Barthwal and Agarwala 2020 https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/.
31 Barthwal and Agarwala 2020 https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/.
32 Barthwal and Agarwala 2020 https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/.
33 Kavallieratos and Katsikas 2020 *MDPI* 1.

cyber-enabled ships (hereinafter C-ES).[34] The C-ES is a cyber-physical ecosystem which consists of the elements such as; the vessel itself, the Shore Control Centre (hereinafter SCC) that controls and handles the C-ES, the communication links between the vessel and the SCC, and other ships in the vicinity.[35]

With cyber security risks increasing rapidly, shipping companies will hire persons responsible for designing and testing security measures to prevent these attacks.[36] These are cyber security specialists. The maritime industry has a lot to gain from the 4IR as it tends to move towards the automation and connectivity of every system.[37] These gains and systems include technologies such as the internet of things,[38] artificial intelligence,[39] autonomous and unmanned technology[40] and data analytics.[41] In the midst of the 4IR, severe threats present themselves in the form of cyber-attacks and this is because of the electronic based and wireless connections that are being used in the maritime industry.[42] The digitalization and dynamics of the maritime industry will force us to rethink the capabilities of networked systems and how the Internet of

---

34 Kavallieratos and Katsikas 2020 *MDPI* 1.

35 Kavallieratos and Katsikas 2020 *MDPI* 1.

36 Anon 2018 https://safety4sea.com/cm-drivers-of-the-4th-industrial-revolution-in-maritime-industry/?__cf_chl_jschl_tk__=651b300929167e91fa1ed3cd858744d1ac23fc28-1618765679-0-Aadb3NkidxeA4wCtG49__KlN_Y3Hy_lMyWIRdWndCaddZEnXbXGF4I4ff1b6w1CT5B2Lv8jsaYRxCYHiY3UbclP8W8iQNwM7B7tqmt2NHcZ80EwCPJi2fMo_JFCUbdjWuGhvJCnQyPg9Qp3RVWQLZhopL9juy9CygvPLJjz0y2N51CVVG8CpzJ2eKMKikZmFhzLeUYwxE2gb-MgpzEMeSoCveNiWUn0-6MjhSPORzNJrmB3pljHFFAK5nTs6IxzFy8rJg08jgOZY6OAeYxcdfscqP6sAI2nQGTu8dS1-1vaSHy1ZDHKUJXNnxX28cMz4mrC67LhNyQ98lVQYDK2HmWCr7VG4m2H_Ah9u1V1e2SfpuV9wfbhnFmXLSvCMg2Y4LML4JhoGfd_r1ubYvsIAsDGgH80XA9XRKTNkl4naFzxEhpMZPB859mgnAPXY9fwS80NASVJxKI_gXIxwSOSXThY.

37 Riviera Newsletters 2019 https://www.rivieramm.com/news-content-hub/news-content-hub/how-maritime-can-make-the-most-of-industry-40-54225.

38 The Internet of Things is a definition used to define physical objects with and a system of interrelated computing devices. Furthermore, the Internet of Things can be seen as a term that encompasses all electronics that are not traditional computing devices.

39 Artificial Intelligence can shortly be defined as simulation of human intelligence processes which are now being done by computer systems. Artificial intelligence consists of three cognitive skills, including learning, reasoning and self-correction. IBM Cloud Education 2020 https://www.ibm.com/za-en/cloud/learn/what-is-artificial-intelligence.

40 Automation is about the use of technology to monitor, control and/or operate any process or function with accuracy and efficiency without human intervention. Autonomous technology has the purpose to enrich automated systems with sensors, Artificial Intelligence and analytical capabilities so that they can make decisions based on data that have been collected.

41 Riviera Newsletters 2019 https://www.rivieramm.com/news-content-hub/news-content-hub/how-maritime-can-make-the-most-of-industry-40-54225.

42 Zarzuelo 2021 https://www.sciencedirect.com/science/article/pii/S0967070X20308945.

Things can be leveraged to facilitate the next stage of the process of vessel development.[43] As technology continues to develop daily, an increasingly important aspect to the European maritime industry is Maritime 4.0 and this creates the opportunity to lead the world in the advancement of next-generation vessels.[44] The 4IR has not yet reached the whole globe, but according to the United Nations Industrial Development Organization (hereafter UNIDO) research it is suggested that the four frontrunner economies of the world, namely the United States, Germany, Japan and China, account for 77% of ADP-related patents.[45]

The globalized nature of value chains in the world means that the 4IR will sooner rather than later impact the whole world and this impact will be either directly or indirectly as well as positively or negatively.[46] Some observers of the 4IR fear that the future of this revolution will lead to unemployment as this is a result of humans being replaced by technology in nearly all parts of jobs across the world.[47] The people who are more optimistic forecasters see the revolution as an opportunity for developing countries to jump to intermediate stages of industrialization.[48]

Much advice has been given to industries and economies on how to best prepare for the effects of the 4IR.[49] The ability of industries and economies to benefit from the 4IR will depend on the availability and of course, the affordability of ADP technology, along with the level and combination of skills and industry capabilities.[50] These are

---

43 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

44 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

45 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

46 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

47 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

48 The Institution of Engineering and Technology Defining Maritime 4.0: *reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

49 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

50 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization 25*.

necessary and if developing countries are not able to fulfil these requirements they are likely to be left behind by developed countries and frontrunner economies.[51]

The purpose of this dissertation is to discuss the ways cybersecurity risks can be mitigated and managed in the 4IR, the 4IR and what it is must be discussed, how it developed and what changes it brings to the world we live in. The purpose of the discussion of the 4IR is to assist understanding how sectors, especially the maritime industry is affected by the 4IR in order to be able to discuss further on in the dissertation the ways in which cybersecurity risks can be managed and mitigated in the 4IR. In the discussion above, the technological advancements in the maritime industry are discussed and with that the cyber risks that are created when the technology advances. One of the key factors that are mentioned above is the increasing opportunity for the creation and implementation of new generation vessels that will be focused on technology and become unmanned in the future.

2.2 Technologies of the Fourth Industrial Revolution

Klaus Schwab has stated that from the publication of his book in 2016 to the Davos 2017 Summit a lot has changed about the new technologies that have started to appear across the world.[52] Some technologies that are also new and important in the 4IR include the Internet of Things and Cyber-Physical Systems.[53]

During the 1970's the Internet of Things started to adopt ideas from Computer Integrated Manufacturing (hereinafter CIM),[54] Just-in-Time (hereinafter JIT)[55] and

---

51 The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* 25.

52 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

53 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

54 Computer Integrated Manufacturing refers to a manufacturing approach whereby the entire production process is controlled by a computer. The result of Computer Integrated Manufacturing is faster production combined with less errors. Anon Date Unknown https://www.techopedia.com/definition/30965/computer-integrated-manufacturing-cim.

55 Just-In-Time is a philosophy for management, and it is not a technique. Just-In-Time has the purpose to produce goods to exactly meet the demands of the customers in time. Banton 2022 https://www.investopedia.com/terms/j/jit.asp

Theory of Constraints (hereinafter TOC).[56] The concept of Internet of Things originated with the concept of "Ubiquitous Computing" at the Palo Alto Research Centre (hereinafter PARC) by Mark Weiser during the 1990's.[57] Early in the 21st Century the fusion of these ideas of the Internet of Things enabled customers to manage assets from the factory, not only for the manufacturing or production of the goods, but also to make asset management possible from the design through to the delivery.[58] The term Internet of Things has evolved even further and by the year 2014 it has evolved so much as to include an array of sensors and devices, which can range from solar panels to thermo-electric and other devices.[59] This has led to much confusion around the term "Internet of Things".[60]

The recent classifications of the Internet of Things have been an important enabler in connecting assets, the smart wearables that have been used for the connected lifestyles and health.[61] It has also been a key enabler for the future of smart cities and the connected driverless modes of transport.[62] The purpose of understanding why the Internet of Things plays such a crucial role and how it is integrated into our connected lifestyles, is to understand that if so much technology, with so much power and capabilities can be worn on a single person's arm, consider what more can be achieved when this is implemented on cybersecurity networks either for the good of cybersecurity or the bad thereof. It helps to understand the role that the 4IR plays in the development of cybersecurity and how it deals with the management of cybersecurity risks that comes with the extreme technological advancements.

---

56 Theory of constraints is a methodology to identify limiting factors that are in the way of achieving a goal. Furthermore, the Theory of Constraints is based thereon to improve the constraint until there is no longer a limiting factor that stand in the way of manufacturing. LEANPRODUCTION Date Unknown https://www.leanproduction.com/theory-of-constraints/#:~:text=The%20Theory%20of%20Constraints%20is,referred%20to%20as%20a%20bottleneck.

57 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

58 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

59 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

60 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

61 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

62 Skilton and Hovsepian *The 4th Industrial Revolution* 11.

Cyber-Physical Systems,[63] is a concept that was created with the idea of connected systems and the role of organisations as a complete system of systems.[64] CPS embodies some key concepts that are found in the 4IR such as, digital twin model tight integration, outcome driven, automated machine to machine, total cost and operational lifecycle.[65] CPS grows rapidly in areas such as digital manufacturing and the smart factory concepts that exist within the 4IR. This all is predominantly about connected factory automation and the self-management of subsystems, and this leads to the overall automation of factories and the operations thereof.[66] The concepts around which CPS has been built now includes Human-Computing Interactions (hereinafter HCI) and the Internet of Things have encapsulated technologies of sensors and devices into a machine-to-machine automation.[67]

3 Cybersecurity

3.1 History of Cybersecurity

This chapter of the dissertation will deal with a brief history of cybersecurity, focusing on where and how it has developed. The purpose of this chapter is to obtain a better understanding of the cyber risk and threats that must be dealt with as a result of an even more developed 4IR that will be discussed later.

There was a time in history when cyber-attacks could not have taken place as easily as they do today. This chapter comprises the discussion about the timeline and the creation of cybersecurity and antivirus programs. After the production of the first digital computer in 1943, it was for the next two decades very problematic to carry out achieve cyber-attacks .[68] Accessibility to these enormous machines were very limited with only a number of people being allowed access, and they were not networked at the time.[69] The theory of computer viruses were first made public in 1949 and this was

63 Cyber-Physical System is a system that integrates cyber components (namely sensing, computation and human users), connecting them to the internet and to each other.
64 Skilton and Hovsepian *The 4th Industrial Revolution* 11.
65 Skilton and Hovsepian *The 4th Industrial Revolution* 11.
66 Skilton and Hovsepian *The 4th Industrial Revolution* 11.
67 Skilton and Hovsepian *The 4th Industrial Revolution* 11.
68 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
69 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.

due to the fact that John Van Neumann speculated that computer programs have the ability to reproduce.[70]

In 1987 antivirus commercialized for the first time, although at times there were competing claims for who the innovator was of the first antivirus product.[71] G Data software is a software programme that was founded by two competitors, namely Andreas Lüning and Kai Figge, with a company launching an antivirus solution that was specifically aimed at the Atari ST platform in 1987.[72] During the same year John McAfee founded the programme named McAfee, that later became a well-known security company that would over time become the world's leading security vendor.[73]

The 1990s was a busy year in the development of antivirus programs, as the first polymorphic viruses were created. These codes had the purpose to mutate while keeping its original algorithm to avoid being detected by systems.[74] Early antiviruses were purely signature-based and compared binary systems with a database of what was known as virus "signatures".[75] Virus and malware numbers have grown extensively during the 1990s from only tens of thousands in the early part of the decade to almost 5 million every year by the year 2007.[76]

At the beginning of the 21st century, internet became more accessible in homes and offices, and this led to more cyber vulnerabilities for cybercriminals to exploit than ever before.[77] In the year 2000 the first open-source antivirus engine which was known as OpenAntiVirus was made available. 2001 was the year ClamAV was launched, and this was the first ever open-source antivirus engine that was commercialized, and in 2001 Avast launched its Antivirus Software, which offered fully featured security solutions

70 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
71 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
72 Popa 2020 https://news.softpedia.com/news/did-you-know-the-first-antivirus-product-was-launched-in-1987-528883.shtml.
73 Popa 2020 https://news.softpedia.com/news/did-you-know-the-first-antivirus-product-was-launched-in-1987-528883.shtml.
74 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
75 SentinelOne 2019 https://www.sentinelone.com/blog/history-of-cyber-security/.
76 SentinelOne 2019 https://www.sentinelone.com/blog/history-of-cyber-security/.
77 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.

to the masses. This initiative led to Avast growing a user base of more than 20 million people in five years.[78]

The year 2010 was the start of a new era for cybersecurity as well as antivirus, but at the same time also for cybercriminals. During this new era for cybersecurity there were many high-profile attacks and breaches that took place and this had an impact on the national security of countries and also eventually led to businesses losing millions.[79] These events include the actions in 2012 when hackers from Saudi Arabia published the details of more than 400,000 credit cards online.[80] In 2013 a former employee of the CIA (Central Intelligence Agency) had copied and leaked classified information from the National Security Agency.[81] In the year 2013-2014 malicious hackers broke into Yahoo, and comprised the accounts and personal information of 3 billion of its users. Yahoo received a fine of 35 million dollars for their failure to disclose the news about what happened.[82]

Finally in 2019 multiple Distributed Denial of Service (hereinafter DDos) attacks on the New Zealand stock market forced a complete temporary shutdown.[83] The stock market has stated that the attack had impacted the NZX network connectivity and therefore they decided to halt the trading in their cash markets.[84] The next generation of cybersecurity that was created involves a lot of different approaches to increase the detection of new threats, and it also reduces the false positives that were received.[85] This next generation of cybersecurity typically involves Multi-Factor Authentication (hereinafter MFA) and Network Behavioural Analysis (hereinafter NBA) which is able to identify malicious documents based on any behavioural deviations.[86] The new generation further involves Threat Intelligence and update automation, as well as Real-Time protection.[87] This includes on-access scanning, background guard, resident shield

78 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
79 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
80 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
81 Mazzetti and Schmidt *The New York Times.*
82 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
83 BBC News 2020 https://www.bbc.com/news/53918580.
84 BBC News 2020 https://www.bbc.com/news/53918580.
85 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
86 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.
87 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.

and auto protect.[88] Sandboxing and Web Application Firewalls (hereinafter WAF) are also included in this new generation of cybersecurity. Sandboxing is when an isolated test environment is created where suspicious files or URLs can be executed and WAF are protection against cross-site forgery, cross-site scripting, file inclusion and Structured query language injection (hereinafter).[89]

3.2 Cybercrime in the Maritime Sector

Hill Dickson describes cybercrime as:

> Criminal activity that involves the internet, a computer system or computer technology.[90]

Cybercrime in the shipping industry is a problem that is becoming worse as time continues, and the reason for this is because the digitalization of everything used in the shipping industry.[91] The digitalization includes the telecommunications and informatics, which include the terminal operating systems, electronic chart displays and information systems, electronic data interchange and finally the Global Positioning System (hereinafter GPS) systems and automatic identification systems.[92] The digitalization and the effect thereof on the shipping industry will be discussed in further detail when explicating the 4IR.

Cybercrime mainly consists of two types of attacks, namely untargeted attacks and targeted attacks.[93] Untargeted attacks are performed under an assumption that the more attacks are performed the higher the success rate will be, and these attacks are more likely very unsophisticated attacks.[94] Untargeted attacks are referred to as non-

---

88 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.

89 Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast.

90 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

91 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

92 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

93 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

94 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

targeted attacks and are also known as "attack by opportunity".[95] The success rates of these non-targeted attacks are solely based on the negligence of the potential victim.[96] Targeted attacks on the other hand are much more sophisticated and require a lot of preparation time and research into the next victim of these cybercriminals.[97] In targeted attacks there is a clear assumption that these attackers carefully select their victims and then tailor their approach according to the victim.[98] These attacks are not a once-off attack, but rather an attack that has multiple stages.[99]

Examples of cybercrimes that cause specific risks to the shipping industry and the consequences are thereof, can be data security breaches where pirates for example already know where the most valuable cargo on the ship or vessel is as container preference can be obtained prior to attacks.[100] Further examples of the risks are that these criminals use duplicate bills of lading, and this is ever increasing as there is a push towards the use of electronic bills of lading.[101] Cybercriminals can change the cargo manifests of ships remotely and are therefore able to hide substances in containers and disguise it as something else.[102] The consequences of all these examples are damage to the reputations of the shipping companies or vessels, as well as delay in delivery or shipping of goods and of course a monetary consequence.[103]

Cyber security guidelines are one way to help prevent cyber-attacks and to inform people on how to know when a cyber-attack is imminent. Leading organisations such

---

95 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

96 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

97 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

98 Ladokun *An Analytical approach to characterization of targeted and untargeted attacks in critical infrastructure honeypot* 24.

99 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

100 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

101 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

102 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

103 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

as the Baltic and International Maritime Council (hereinafter BIMCO)[104] have launched and released "The Guidelines on Cyber Security on board Ships."[105] Angus Frew, who is the Secretary General of BIMCO states that these guidelines should help companies to take a risk-based approach to cybersecurity that is specific to their business.[106] These guidelines can be categorised into four categories, namely understanding the cyber threat,[107] assessing the risk,[108] reducing the risk,[109] and finally developing contingency plans.[110]

Computer systems are used daily, whether they are used in the workplace, by academics or just for entertainment. The increase of dependence of always being online to solve problems has also led users to becoming vulnerable to cyber-attacks.[111] Because of this increase in vulnerability of attacks, there is a need for having an emergency back-up plan before attacks can occur.[112] Contingency plans are needed to increase cybersecurity.

The development of contingency plans must be in line with general as well as specific aspects of international standards, such as ISO 27001 and ISO 22301.[113] Contingency plans should be developed according to basic steps that need to be followed. The main goal of contingency plans is not solely how to react to cyber-attacks or security breaches, but more on business continuity, also known as operational resilience.[114] The strategy of operational resilience is to develop options that enable people and

---

104 BIMCO is one of the largest of the international shipping associations representing shipowners.

105 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 44.

106 Dickinson Date Unknown 'Cybercrime in the shipping industry; An overview of the risks and how they apply to you' https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf.

107 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 44.

108 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 44.

109 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 44.

110 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 44.

111 Padilla and Freire 2019 *JISEM* 1.

112 Padilla and Freire 2019 *JISEM* 1.

113 Padilla and Freire 2019 *JISEM* 2.

114 TechTarget Date Unknown https://www.techtarget.com/searchsecurity/post/Cybersecurity-contingency-planning-needs-a-face-lift.

processes to adapt to changing patterns without disrupting customers, transactions or services.[115] It can be said that the main goal, when faced with such an incident, is to execute the right protocols for the incident to continue business with minimal disruption.[116]

It should be noted that no organisation, no matter the size is entirely immune from cyber-attacks or data breaches, but large-scale organisations may have better digital infrastructure to deal with any possible data breaches or cyber-attacks.[117]

The primary stages of a contingency plan are as follows; definition, planning, realization and closure.[118] Firstly, a clear understanding must be obtained of objectives and then what is to be achieved.[119] Planning is the establishment of what type of contingency is needed to meet the defined objectives.[120] Typically, the methodology that is to be pursued should include the recovery of critical processes and avoidance of alterations.[121] Realization addresses the main part of any contingency plan, and the errors detected and the necessary adjustments thereon leads to an efficient contingency plan.[122] Finally, the last step of any contingency plan is closure, which envisage the formal acknowledgment of any contingency plan proposed, tested and then corrected by administration that is responsible in the case of eventualities.[123]

Because of the significant rise in cybercrimes, these crimes have become a problem in the world we live in. In order to control the numbers of cybercrimes that happen more and more every day there must be laws and regulations that regulate these, and in

115 TechTarget Date Unknown https://www.techtarget.com/searchsecurity/post/Cybersecurity-contingency-planning-needs-a-face-lift.
116 TechTarget Date Unknown https://www.techtarget.com/searchsecurity/post/Cybersecurity-contingency-planning-needs-a-face-lift.
117 CyberPolicy Date Unknown https://www.cyberpolicy.com/cybersecurity-education/how-to-develop-a-cybersecurity-contingency-plan-asap.
118 Padilla and Freire 2019 *JISEM* 2.
119 Padilla and Freire 2019 *JISEM* 2.
120 Padilla and Freire 2019 *JISEM* 2.
121 Padilla and Freire 2019 *JISEM* 2.
122 Padilla and Freire 2019 *JISEM* 3.
123 Padilla and Freire 2019 *JISEM* 3.

effect create laws by which guilty parties can be prosecuted, if possible. The rise in cybercrimes has led to various laws and regulations both nationally as well as internationally. National laws which have been implemented to regulate cybercrimes are firstly the *Cybercrimes Act*[124] which was implemented in 2020 and secondly the *Electronic Communications and Transactions Act*[125] which was implemented and became law on 30 August 2002. These acts will later on be discussed in more detail which will deal with the purpose of the act as well as certain provisions that deal specifically with cybercrimes. In terms of foreign law, the following countries have instituted laws to regulate cybercrimes, *Germany's IT Law*[126], in Russia it is the *Cybersecurity Doctrine*[127] and in China their *Cybersecurity Law*[128]. Further in the Philippines is the implementation of the *Cybercrime Prevention Act*[129] which is later known as the *Republic Act No.10175*[130]. These acts are the important foreign laws and regulations that will be discussed later. The implementation of legislation and regulations by different countries shows how serious the threats of cybercrimes are.

The purpose of all these acts and regulations are to minimise cybercrimes and cyber threats, therefore the rise of cybercrime has led to the development of these acts.

3.3 Enforcement for cybercrimes

One of the big questions that is being asked when it comes to cybercrimes is how the laws for these crimes will be enforced if at all. South African law recognizes cybercrimes and cyber threats and as a result thereof the *Electronics Communications and Transactions Act*[131] has been introduced. The *Electronic Communications and Transactions Act*[132] creates a lot of offences in Chapter XIII, and these include the unauthorised access or interception of data as a crime.[133] The unauthorised

124 *Cybercrimes Act* 19 of 2020.
125 *Electronic Communications and Transactions Act 25* of 2002.
126 *Germany IT Law.*
127 Russia Cybersecurity Doctrine.
128 *China Cybersecurity Law.*
129 *Cybercrime Prevention Act* 2012.
130 *Republic Act* No. 10175.
131 *Electronic Communications and Transactions Act* 25 of 2002.
132 *Electronic Communications and Transactions Act* 25 of 2002.
133 *Electronic Communications and Transactions Act* 25 of 2002.

interference with any data that causes the data to be destroyed or otherwise rendered ineffective can be rendered as a crime.[134] The crimes of computer-related extortion, fraud or forgery are also recognised in section 87 of the Act.[135] The question regarding enforceability and the investigation of these crimes was already being asked when parliament introduced his new legislation. The *Electronic Communications and Transactions Act*[136] has taken on a radical approach regarding jurisdiction that vests in South Africa if an offender commits an offence or any part thereof or the preparation thereof in South Africa,[137] or if the offence was committed by a South African citizen.[138] In South Africa, the enforcement mechanism that is proposed is to appoint Cyber Inspectors, who among other functions have the function of monitoring and reporting illegal activities.[139] South Africa has not yet appointed Cyber Inspectors, but generally Cyber Inspectors have the powers of inspecting and searching premises, information systems and data to establish if a crime has been committed.[140] Enforcement of these crimes is very difficult if it is taken into consideration that victims do not want to publicly admit to being hacked or being a target to a cyber-attack, therefore these attacks go by unnoticed by people other than the victims.[141] Furthermore, the tracking down of these criminals is extremely difficult and even if it has been achieved, it has happened in another jurisdiction.[142]

The question remains if the *Electronic Communications and Transactions Act*[143] will act as a deterrent for these crimes and prevent it from happening. The *Electronic Communications and Transactions Act*[144] states the different penalties depending on the nature of the offence. The penalties range from an unspecified fine or imprisonment for a period from one to five years.[145]

---

134 *Electronic Communications and Transactions Act* 25 of 2002.
135 Section 87 of the *Electronic Communications and Transactions Act* 25 of 2002.
136 *Electronic Communications and Transactions Act* 25 of 2002.
137 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
138 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
139 Section 80 of the *Electronic Communications Act* 25 of 2002.
140 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
141 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
142 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
143 *Electronic Communications and Transactions Act* 25 of 2002.
144 *Electronic Communications and Transactions Act* 25 of 2002.
145 Section 89 of the *Electronic Communications and Transactions Act* 25 of 2002.

Before the discussion can be held in regard to legislation, internationally and foreign as well as customary international law, there is an aspect that is important for anyone that could be a victim of cybersecurity and that is the implementation of the *Protection of Personal Information Act* (hereinafter POPIA)[146] that was introduced in South Africa in 2020. The new POPI Act is a privacy standard that is focused on business to consumer organisations, and it creates new cybersecurity obligations that every organisation now has to comply with before being able to rely on legislation to just act as a deterrent for cyber-attacks or any cyber related harm being done.[147] The POPI Act brings a new perspective with regard to cybersecurity and how to deal with cyber-attacks. They create more advanced cybersecurity tools and with the new POPI Act the days of relying purely on firewall and the antivirus systems that have been installed on computer or technology systems is long gone. The new POPI Act refocuses security that there must be an effort made at the level of a business or an organisation to protect themselves from cyber-attacks.[148] This principle of first implementing more measures of protecting yourself is something that will be discussed further on in this dissertation.

In the POPI Act there is a very specific section that is applicable to cybersecurity and the way in which businesses and organisations should react to cyber-attacks, and it is contained in section 22 of the Act.[149] In section 22(1) of the Act[150] it creates an obligation that where there is a reasonable suspicion that the personal data of a data subject[151] has been accessed or obtained by an unauthorised person the responsible party[152] now has an obligation to notify firstly the Regulator[153] and secondly the person whose personal information has been accessed unless it is not possible to identify such person.[154] Section 22(2) of the Act[155] states that the notification that is mentioned in

146 Shak Date Unknown https://saicom.io/news/popia-a-cybersecurity-perspective/.
147 Shak Date Unknown https://saicom.io/news/popia-a-cybersecurity-perspective/.
148 Shak Date Unknown https://saicom.io/news/popia-a-cybersecurity-perspective/.
149 Section 22 of the *Protection of Personal Information Act* 4 of 2013.
150 Section 22(1) of the *Protection of Personal Information Act* 4 of 2013.
151 A person to whom personal information relates.
152 A public or private body or any other person which determines the purpose of and means for processing personal information.
153 Means the information Regulator established in terms of section 39 of the Act.
154 Section 22(1) of the *Protection of Personal Information Act* 4 of 2013.
155 Section 22(2) of the Protection of Personal Information Act 4 of 2013.

subsection 1[156]must be done as soon as it may reasonably be possible after the discovery of the compromise and after taking into consideration the legitimate needs of law enforcement or the measures that are needed to determine the scope of the compromise. Furthermore, section 22(3)[157] states that the responsible party may only delay the notification of the data subject of a compromise of his/her personal information if a public body that is responsible for the prevention, detection or investigation is of the opinion that notifying will impede the investigation.

This new POPI Act[158] is very important in the prevention of cybersecurity. Its main purpose can be identified as businesses and organisations that must first before relying on legislation and other sources, do everything that is reasonable in keeping themselves safe. Subjects of cyber-attacks should first try and protect themselves before looking for other solutions and this is applicable to all aspects of cybersecurity. This is especially important with regard to South African law and cybersecurity. Before looking into and investigating South African legislation around cyber-attacks the principles set out in specifically section 22 of the POPI Act[159] should first be implemented.

With regard to what has been mentioned above enforcement remains something that is difficult to achieve, and it certainly does not come without its problems. In the following discussion, some of the difficulties of enforcing cybercrimes and cyber laws will be explicated.

There are a lot of different obstacles when it comes to enforcing cybercrimes which includes identifying cybercriminals, jurisdictional challenges, extradition process challenges, challenges regarding the nature of evidence, as well as the cost, time and efforts that are incurred in the investigation and prosecution of these criminals.[160] Out of the above-mentioned the factors that take precedence are the jurisdictional challenges and the difficulties identifying these cybercriminals. One of the most lucid

156 Section 22(1) of the *Protection of Personal Information Act* 4 of 2013.
157 Section 22(3) of the *Protection of Personal Information Act* 4 of 2013.
158 *Protection of Personal Information Act* 4 of 2013.
159 *Section 22 of the Protection of Personal Information Act 4 of 2013.*
160 Ajayi 2016 *J. Internet inf. System* 4.

and difficult reasons for the enforcement of cybercrimes is the identification of these cyber criminals, while the anonymous nature of these cybercriminals is the key behind their success.[161] The question around the pursuit of cybercriminals is how legislation can be exercised if the addresses of these criminals cannot be traced. Lord Denning in a celebrated case[162] gave the dictum "you cannot put something on nothing and expect it to stand."[163] The point of this is that because of the impossibility of identifying these criminals no law that is intended to work can be applied.[164]

A further issue to the enforceability of cybercrimes is the challenge of jurisdiction. Jurisdiction may be defined "as the power of a court or judge to entertain an action, proceeding or petition."[165] Jurisdiction forms the roots of any case and therefore, if the courts lack any jurisdiction, it then also lacks the required competence to try this case. An error in competence will result in the proceeding being null and void *ab initio*.[166] The jurisdictional challenge of enforcement comes when it has become possible to identify a cybercriminal or the identity of a cybercriminal has become clear, but he is situated in another country aside from where the victim is domiciled.[167] Then, the court has no jurisdiction to hear the matter due to the geographical differences.[168] Immediately a person would jump to extradition as the solution, but extradition comes with its own challenges and one of these challenges is the double criminality requirement.[169] What makes the extradition process even more difficult is whether or not there are extradition treaties in place.[170]

---

161 Ajayi 2016 J. *Internet inf. System* 4.
162 *Macfoy v United Africa Company Limited (West Africa),* 1962.
163 *Macfoy v United Africa Company Limited (West Africa*), 1962.
164 Ajayi 2016 J. *Internet inf. System* 4.
165 *Alade v Alemuloke* 1988.
166 Ajayi 2016 J. *Internet inf. System* 4.
167 Ajayi 2016 J. *Internet inf. System* 5.
168 Ajayi 2016 J. *Internet inf. System* 5.
169 This principle requires that the offence for which the accused is sought to be extradited must be a criminal offence at the state making the request and the state where the accused is domiciled. Blaas 2003 *DOUBLE CRIMINALITY IN INTERNATIONAL EXTRADITION LAW* 3.
170 Ajayi 2016 J. Internet inf. System 5.

3.4 South African, Foreign and International laws for cybersecurity

Maritime cybersecurity cannot be discussed without reference to South African, foreign as well as international laws thereon and the development of maritime risk management programmes and procedures. The following will be discussed in the next chapter; South African laws regulating and advancing cybersecurity and further foreign and international laws and regulations regulating and advancing cybersecurity.

3.4.1 National/South African legislation for cybersecurity

When discussing South African law with regard to the advancing of cybersecurity and cybersecurity management, the legislation that has to be discussed is firstly the *Cybercrimes Act*[171] and secondly the *Electronic Communications and Transactions Act*.[172] *The Cybercrimes Act*[173] was established with the purpose to create offences having a bearing on cybercrime and further to criminalise offences such as the disclosure of data messages which are harmful and also to regulate jurisdiction with regard to cybercrimes.[174] What will be discussed is mostly the jurisdiction of cybercrimes as well as the penalties and sentencing for cybercrimes. Section 24 of the *Cybercrimes Act*[175] states that:

> "Courts of the Republic shall try crimes under Part I or Part II of Chapter 2 If the defendant is arrested in the territory of the Republic or aboard a vessel, ship, sea installation, fixed platform, or aircraft, registered in the Republic."[176]

A court in the Republic will have the jurisdiction to hear a matter where the offence was either committed in the territory of the Republic, or on-board a vessel, ship or aircraft that is registered within the Republic at the time the offence was committed and this jurisdiction is established in terms of section 1(c) of the Act[177] at the time the

171 *Cybercrimes Act* 19 of 2020.
172 *Electronic Communications and Transactions Act* 25 of 2002.
173 *Cybercrimes Act* 19 of 2020.
174 *Cybercrimes Act* 19 of 2020.
175 Section 24 of the *Cybercrimes Act* 19 of 2020.
176 Section 1(a) of the *Cybercrimes Act* 19 of 2020.
177 Section 1(c) of the *Cybercrimes Act* 19 of 2020.

offence was committed.[178] Section 19 deals with sentencing for guilty parties, and this section states that:

> "Any person who violates section 2(1) or 2(2), 3(3) or 7(2) shall be sentenced to a fine or imprisonment for not more than five years, or a fine and imprisonment. Furthermore, any person who violates the provisions of sections 3(1) or (2), section 4(1), section 5(1), section 6(1) or section 7(1) shall be subject to a fine or shall be subject to a fine or shall be punished by imprisonment for not more than 10 years, or both a fine and imprisonment."[179]

In terms of section 19(3)[180] it deals with people who contravene section 11(1) and in this case a person contravening section 11(1) is liable upon conviction to be sentenced to either a fine or imprisonment not exceeding 15 years, or to both a fine and imprisonment.[181]

The *Electronic Communications and Transactions Act*[182] also deals with cybercrimes, penalties for these crimes as well as jurisdiction. Section 90 of the Act[183] deals with jurisdiction. This section states the following:

> "a Court in the Republic will have Jurisdiction if the crime was committed in the Republic, or the preparatory act of the crime or part of the crime was committed in the Republic,[184] or the consequences of the crime committed by a national or permanent resident or a person employed in the Republic,[185] or the offence commenced on board a vessel or aircraft registered with the Republic at the time the offence was committed."[186]

The penalties in terms of the *Electronic Communications and Transactions Act*[187] are as follows; in terms of section 89 of the Act[188] a person who is convicted of an offence referred to in subsection 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment not exceeding 12 months.[189] Any person convicted of an

---

178 Section 1(c) of the *Cybercrimes Act* 19 of 2020.
179 Section 19(2) of the *Cybercrimes Act* 19 of 2020.
180 Section 19(3) of the *Cybercrimes Act* 19 of 2020.
181 Section 19(3) of the *Cybercrimes Act* 19 of 2020.
182 *Electronic Communications and Transactions Act* 25 of 2002.
183 Section 90 of the *Electronic Communications and Transactions Act* 25 of 2002.
184 Section 90(a) of the *Electronic Communications and Transactions Act* 25 of 2002.
185 Section 90(b) of the *Electronic Communications and Transactions Act* 25 of 2002.
186 Section 90(d) of the *Electronic Communications and Transactions Act* 25 of 2002.
187 *Electronic Communications and Transactions Act* 25 of 2002.
188 Section 89 of the *Electronic Communications and Transactions Act 25* of 2002.
189 Section 89(1) of the *Electronic Communications and Transactions Act* 25 of 2002.

offence referred to in subsection 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.[190]

In addition to the abovementioned penalties set out in the Act, the following case law has affected the penalties as set out above. In the Supreme Court of Appeal case of Salzman v S[191] the appellant's special leave to appeal is dismissed and the matter is struck from the roll. The facts of the case are as follows. Cell C who is a major mobile cellular company who is one of the top four leading cellular networks in South Africa was the victim of a cyber-attack on 7 November 2004. The invasion penetrated into their systems and disconnected 80% of its systems are a result of the invasion.[192] In search for a responsible culprit, the suspicion fell upon an employee of Cell C who was employed as an IT Remote Access System Administrator, and the Appellant in this matter was charged with various contraventions of Section 86 of the *Electronic Communications and Transactions Act*.[193] On Count 1 the Appellant was charged with unlawfully accessed Cell C's computer network without having authority or permission and on count 3 the Appellant was convicted of having contravened Section 86(5) by unlawfully causing data on Cell C's system to be modified or altered or destroyed or rendered ineffective.[194] The Appellant was sentenced to a fine or 12 months imprisonment on count 1 and to three years imprisonment on count 3.[195]

Apart from the two statutes with the purpose of minimising cyber threats and cyber-attacks, an important regulation in South Africa for this purpose is the National Cybersecurity Policy Framework for South Africa (hereinafter NCPF).[196] The purpose of the NCPF is to create a safe, trustworthy cyber environment that promotes the protection of critical information structures while enhancing the understanding of

---

190 Section 89(2) of the *Electronic Communications and Transactions Act* 25 of 2002.

191 *Salzman v S(755/18) [2019] ZASCA 145; [2020] 1 ALL SA 361 (SCA); 2020(2) SACR 200(SCA)(13 November 2019).*

192 *Salzman v S (755/18) [2019] ZASCA 145; [2020] 1 ALL SA 361 (SCA); 2020(2) SACR 200(SCA) (13 November 2019).*

193 Section 86 of Electronic Communications and Transactions Act 25 of 2002.

194 *Salzman v S (755/18)[2019] ZASCA 145; [2020] 1 ALL SA 361 (SCA); 2020(2) SACR 200(SCA)(13 November 2019).*

195 *Salzman v S (755/18) [2019] ZASCA 145; [2020] 1 ALL SA 361 (SCA); 2020(2) SACR 200(SCA) (13 November 2019).*

196 *National Cybersecurity Policy Framework for South Africa.*

human values and cybersecurity to support national security.[197] The NCPF is responsible for providing measures that address national security with regard to cyberspace as well as the measures that need to be implemented to combat cyber warfare and cybercrimes, the development, review and updating of existing substantive and procedural laws.[198] In this policy it deals with the promotion of a cybersecurity culture, and it states that in order to effectively deal with cybersecurity, it is important that civil society, government and the private sector all play their part in ensuring the creation of a cybersecurity culture.[199] In order to achieve this, it is expected that businesses develop a positive culture for cybersecurity, that there is a promotion of comprehensive national awareness programmes and guidelines and that there is a development in awareness of the cyber risks together with the available solutions.[200]

In the previous chapter the difficulties of enforcing cybercrimes were mentioned and even with the legislation in place, South African legislation, as well as other foreign law instruments will be discussed later with regard to difficulties of enforcement. The difficulties or obstacles that were mentioned, include the extradition process, jurisdictional difficulties, identifying of cybercriminals, the nature of evidence, costs and time put in to prosecute these criminals.

A short discussion of Director of Public Prosecution, Western Cape, v Kouwenhoven[201] will follow as this is a case this addressed the question of extradition and jurisdiction. Mr Kouwenhoven, who is a Dutch national, was in April 2017 convicted by a Dutch Court for the illegal supply of weapons to the regime of Charles Taylor in Liberia and Guinea and he was also convicted of participating in war crimes in those countries.

197 *National Cybersecurity Policy Framework for South Africa.*
198 *National Cybersecurity Policy Framework for South Africa.*
199 *National Cybersecurity Policy Framework for South Africa.*
200 *National Cybersecurity Policy Framework for South Africa.*
201 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*

The crimes mentioned were committed in the territory of the Netherlands, but the Netherlands exercises extraterritorial jurisdiction.[202]

During the proceedings continued against him in the Netherlands, Mr Kouwenhoven was present in Cape Town and during the period of December 2017, he was arrested by a warrant issued by a magistrate in Pretoria in terms of section 5(1)(b) of the Extradition Act.[203] Mr Kouwenhoven raised three question for his defence of which only two are of relevance to this dissertation, firstly that the Director of Public Prosecutions had to prove that South Africa and the Netherlands were party to an extradition treaty and secondly that he was not liable to be extradited because the crimes he was alleged to have committed and for which he had been convicted and sentenced were not committed within the territory of the Netherlands.[204] With reference to the question of jurisdiction, South Africa in May 2003 acceded to the European Convention on Extradition (hereinafter referred to as the "Convention") and to the additional and second addition protocols thereto. The Netherlands were also signatories to the Convention.

The importance of this is the two important questions that was discussed in this case, namely the Extradition Act and the question regarding jurisdiction. In terms of article 1 of the Convention, parties undertake to surrender to each other any person who is wanted by a competent authority to carry out a sentence. Further article 7(1) states that the requested party may refuse to extradite a party for an offence which is regarded by its law as having been committed in whole or in part in its territory or in a place treated as its territory.

Article 7(2) of the Convention states the following:

> "When the offence for which extradition is requested has been committed outside the territory of the requesting Party, extradition may only be refused

---

202 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*

203 Extradition Act 62 of 1962.

204 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*

if the law of the requested Party does not allow prosecution for the same category of offence when committed outside the latter Party's territory or does not allow extradition for the offence concerned."[205]

This Convention works on the basis that the parties hereto exercise an extraterritorial jurisdiction over certain types of offences and as a result of that they recognise each other's extraterritorial jurisdiction.[206]

Turning to the second question, which is the question of extradition, in this case the focus of extradition is more around the South African Law, but it does address the question of extradition and provides valuable insight into the difficulties of extradition.

The Extradition Act[207] start with the definition of an extraditable offence and in Section 1 of the Act[208] reference is not made to incorporate an element of jurisdiction or territory. Section 3 of this Act[209] is central to the case at hand and this section has the description of 'persons liable to be extradited'. This heading is dealt with in three-fold, firstly with whom do we have extradition agreements, with whom do we not have extradition agreements and finally which are designated states as defined.[210] In terms of Section 9 of this Act[211], a person that was arrest on a extradition warrant must be brought before a magistrate and an enquiry must be held with the view of surrender the person back to the foreign state. The magistrate must hold the enquiry with the purpose to determine whether the foreign state is an 'associated state'[212] as is defined in Section 1 of the Act.[213]

---

205 Article 7(2) of the European Convention on Extradition, 1957.
206 Article 7(2) of the European Convention on Extradition, 1957.
207 *Extradition Act 67 of 1962*.
208 Section 1 of the *Extradition Act 62 of 1962*.
209 Section 3 of the *Extradition Act 62 of 1962*.
210 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*
211 Section 9 of the Extradition Act 62 of 1962.
212 Associated State is a state with limited sovereignty.
213 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*

A very important point was made in this case which is that South African law must be interpreted as far as possible to comply with international law, a principle which can be seen in the case of Glenister v President of the Republic of South Africa & others.[214] The judge in this matter was f the opinion that the broad interpretation of 'jurisdiction' that can be found in the Extradition Act is more consistent with international law, since it facilitates the extradition of persons that are charged or convicted of crimes against humanity where universal jurisdiction is consistent with international law.[215] This statement made in the above matter is important seeing that this dissertation also deals with international law aspects.

These problems that are being faced when trying to take protective measures against cybercrime or enforce the law against cybercrimes need to be taken into consideration, while a question must be addressed.

In terms of the *Cybercrimes Act*[216] that was mentioned and discussed earlier, the South African Police Service (hereinafter SAPS) is provided with authority to not only investigate cybercrimes,[217] but it also grants them the authority to co-operate with foreign states and other police forces or cybercrime enforcers to search, access and seize anything related to cybercrimes that we experience.[218] This is an important step in the right direction when anticipating the difficulties that are being experienced when trying to enforce legislation on cybercrimes. When more than one state or enforcing unit works on cybercrimes, this creates the possibility to eliminate most if not all of the difficulties that are being experienced. The reason why there is a possibility to eliminate all possible threats that are being experienced is because if there were more than one enforcing unit that is actively busy with the enforcement of cybercrimes, the area for committing these cybercrimes become closely monitored, thus minimising the chances of cybercrimes being committed. If the areas wherein cybercrimes are committed

---

214 *Glenister v President of the Republic of South Africa & others [2011] ZACC 6; 2011 (3) SA 347 (CC).*

215 *Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020).*

216 *Cybercrimes Act* 19 of 2020.

217 Section 28 of the *Cybercrimes Act* 19 of 2020.

218 Section 48 of the *Cybercrimes Act* 19 of 2020.

become closely monitored and sufficiently regulated the possibility is there to minimise risks that are being experienced. Furthermore, the National Director of Public Prosecutions has the obligation in terms of the Act, to compile reports on the numbers and the results of prosecutions related to cybercrimes for the National Prosecuting Authority.[219] The Act affords South African courts jurisdiction to adjudicate over any matter that affects a person inside South Africa even if the offence was committed outside South African territory and this is another example of handling the problem of jurisdictional difficulties.[220] It is important to note that, even though cost and time of prosecutions are a big problem and an obstacle being faced when enforcing cybercrimes, it is no comparison to the loss and damage that it causes, and this may even make it worthwhile spending all the time and money prosecuting these criminals.

These South African statutes and regulations are implemented with the purpose of minimising cyber risk threats or even cyber-attacks by punishing individuals who are involved. Should these legislations be implemented correctly, together with the risk management programmes or procedures and the cyber resiliency that can be built, they can minimise cyber risk in the maritime industry. In South Africa and with specific reference to South African legislation, in my opinion there is insufficient evidence and prosecutions to support a statement that prosecuting cybercrimes does help. Cybercrime legislation in South Africa is very young and newly enacted and therefore has not yet been afforded enough time to prove efficiency, but it is clear from this legislation that there is movement in the right direction as mention was made to the cross-jurisdiction of the South African Police Service and the National Prosecuting Authority.

3.5 Foreign and International Laws for Cybersecurity.

3.5.1 Foreign legislation for Cybersecurity

In this chapter of the dissertation, the legislation and regulations of different world powers will be discussed and how each of them deals with cyber risk management of

219 Section 56 of the *Cybercrimes Act* 19 of 2020.
220 Section 24(1)(e) of the *Cybercrimes Act* 19 of 2020.

both cyber risks and cyber-attacks. The countries that will be discussed are Germany, China, United States of America as well as the Philippines. The purpose of the discussions of these laws and regulations to follow is to establish and understand whether these countries have sufficient cybersecurity laws and how they would be implemented. The reason these countries have been chosen for the comparative study, is due to their status as first world countries or otherwise known as developed countries.

3.5.1.1 Germany

Germany has introduced the *German IT Security law 2.0*[221] which is a regulatory law with the main purpose and intention of further developing cybersecurity for the society as a whole.[222] The law focuses on the co-regulation of *Cybersecurity Act*[223] and the German IT Law in certain fields of interest.[224] This regulatory approach has new core elements which includes the protection of citizens. This means a unified IT security mark, that increases visibility for IT security for consumer products and applications.[225] It includes extensions for the German Criminal Code as well as the German Criminal Prosecution Code and also new cybersecurity duties, especially for providers.[226] Finally it includes more effective cooperation of the authorities to deal with cybercrime.[227] The due diligence of Germany's cybersecurity is relying closely on the collaboration between the public and private sectors as well as nationally and globally. Germany is well-known for its strong national data protection law and Germany is now moving towards strict cybersecurity standards.[228] Germany is becoming very active in identifying and spreading cybersecurity practices in a manner that is similar to the National Institute for Standard and Technology (hereinafter NIST) framework.

---

221 *German IT Security Law* 2.0.
222 *German IT Security Law* 2.0.
223 *EU Cybersecurity Act* of 2019.
224 *German IT Security Law* 2.0.
225 Kipker 2019 *International Regulation of Cybersecurity* file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.
226 Kipker 2019 *International Regulation of Cybersecurity* file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.
227 Kipker 2019 *International Regulation of Cybersecurity* file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.
228 Shackelford, Russel and Kuehn 2016 *CIJL*.

Furthermore, Germany is undergoing efforts in the private sector to widen discussion and the dissemination of cybersecurity best practices.[229] It is clear that Germany is taking a big step forward in the management of cyber risks in cyberspace, and these efforts can only be helpful towards the future of cybersecurity in the maritime sector.

Secondly, what will be dealt with is cybersecurity doctrines and regulations of countries that are classified as world powers. The countries that will be discussed are China and Russia.

3.5.1.2 United States of America

The USA has introduced the *Cybersecurity Information Sharing Act*[230] which is their legislation relating to cybersecurity and for the prevention of cyber risk and cyber-attacks. In terms of Section 102(1) of this act, it states that except for the provisions as provided for in this law, a non-Federal entity may for the purpose of cybersecurity and also consistent with the protection for the protection of classified information, share to another non-Federal entity or the Federal government a threat indicator or defensive measure[231], and this is to prevent cyber-attacks from happening before damage is caused. This act sets out frameworks and responses to how cyber-attacks and cyber risks can be mitigated and should be handled within the legislative framework. In terms of this Act[232] cybersecurity risk can be defined as follows:

> "Threats to and vulnerabilities of information or information systems and ay related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification or destruction of such information or information systems, including such related consequences caused by an act of terrorism"[233]

Section 205 of this Act deals with the Response Framework and in terms of this section the Secretary, in coordination with others heads of the appropriate Federal Departments and agencies that are in accordance with the National Cybersecurity Incident Response Plan, there must be regularly updated and maintained and exercise

---

229 Shackelford, Russel and Kuehn 2016 *CIJL*.
230 *Cybersecurity Information Sharing Act of 2015.*
231 Section 104(1) of the *Cybersecurity Information Sharing Act of 2015.*
232 *Cybersecurity Information Sharing Act of 2015.*
233 Section 2031(A) of the *Cybersecurity Sharing Information Act of 2015.*

the Cyber Incident Annex to the National Response Framework of the Department in order to deal sufficiently with cyber risks and cyber-attacks.[234]

The USA has effectively implemented the use of Cybersecurity plans, and this indicates that the legislation around cybersecurity in the USA has been delicately planned and implemented to ensure the mitigation of cyber risks as far as reasonably possible.

Section 228 of the Act[235] deals with cybersecurity plans, and this section is two-fold. Firstly, it deals with the requirement and secondly it deal with the exception to the requirement. The requirement is that the Secretary shall in coordination with the Director of the Office Management and Budget, develop and implement an intrusion assessment with the idea of proactively detecting, identifying, and removing intruders n an agency information system on a routine basis.[236]

Onn the 1st of March 2023, the Biden-Harris administration has implemented a National Cybersecurity Strategy[237] to build on existing cybersecurity policies and also to strengthen cybersecurity in their country. There will a short discussion of the strategy. This strategy deals with different aspects, starting with the defending of the critical infrastructure.[238] On the basis of defending critical infrastructure, the strategy refers to the building of new and innovative capabilities allowing owners and operators of critical infrastructure and other parties to effectively collaborate with each other.[239] Further, the Federal Government will be able to provide better support and defense of critical infrastructure by making their own systems more defensible and efficient. In this strategy focuses is Placed thereon that the Federal Government will make use of

234 Section 205(d) of the *Cybersecurity Information Sharing Act of 2015.*
235 Section 228 of the *Cybersecurity Information Sharing Act of 2015.*
236 Section 228(1) of the *Cybersecurity Information Sharing Act of 2015.*
237 The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
238 The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
239 The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

the already existing authorities and et necessary cybersecurity requirements in sectors that it deems critical.[240]

These regulations that are to be implemented should be implemented based on performance, leveraging existing cybersecurity frameworks, voluntary consensus standards and guidance.[241] The guidance referred to includes the Cybersecurity and Infrastructure Security Agency (hereinafter CISA) and the National Institute of Standards and Technology (hereinafter NIST), which will also be discussed later on in this dissertation.[242] In the strategy the USA mentions and intends to use their national powers to disrupt and dismantle threat actors whose actions threaten the interest of the countries, and this principle is one that has not been implemented by the other countries, but is a very important aspect and also one that can have a very positive outcome.

3.5.1.3 China

The second major country that will be discussed is China and their regulations on cybersecurity. *Cybersecurity Law of the People's Republic of China*[243] has a double focus on both network security as well as data protection. These Chinese regulations follow a different approach from EU Law, which is where IT-security and data protection is separated. China follows a holistic approach in the regulation of IT.[244] Network security according to China's cybersecurity law states that networks should be in a stable and reliable state of work, which means measures can be taken against intrusions and the destruction of network resources.[245] The network security includes risk assessment, real name registration, information exchange, certification and

---

240 The White House, Washington, 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

241 The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

242 The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

243 *Cybersecurity Law of the People's Republic of China, 2017.*

244 Kipker 2019 *International Regulation of Cybersecurity* file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.

245 Kipker 2019 International Regulation of Cybersecurity file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.

education, to name only a few.[246] China's legislation on cybersecurity is formulated to ensure cybersecurity and to safeguard sovereignty and national security. In terms of article 4 of this legislation[247] the state is formulating and continuously improving cybersecurity strategies, which clarifies the fundamental requirements and the primary goals of ensuring cybersecurity in the country and further implementing cybersecurity policies.[248] Article 7 of this legislation indicates that the Republic of China is busy conducting international exchanges and actively cooperating in cyberspace governance, and also attacking cybercrime and the illegality thereof.[249] The purpose of this is to create a peaceful environment knowing sufficient legislation is in place.

Article 19 of this act is important due to the fact that one of the problems creating cyber risk can be as a result of relevant people in departments not having sufficient knowledge of how to deal with matters. Article 19 states that all levels of government and the relevant department must regularly carry out cybersecurity publicity and education and also guide the relevant units to properly carry out cybersecurity.[250] This article specifically can be carried out as a measure for cyber risk management as educating more people about the risks of cybersecurity can help prevent cyber-attacks.

3.5.1.4 Philipines

Finally follows the discussion of the *Cybercrime Prevention Act of 2012* in the Philippines[251], which is now officially recorded as the *Republic Act No. 10175*[252]*,* and in this act they set out cybercrime offences, the penalties for such offences and the law enforcement authorities. Section 4[253] states that the following acts constitute a cybercrime punishable under this act:

> "offences against the confidentiality, integrate messages (liability of computer data and systems:[254] illegal access – the access to the whole or any part of the computer

246 Cybersecurity Law of the People's Republic of China, 2017.
247 Article 4 of the Cybersecurity Law of the People's Republic of China, 2017.
248 Article 4 of the Cybersecurity Law of the People's Republic of China, 2017.
249 Article 7 of the Cybersecurity Law of the People's Republic of China, 2017.
250 Article 19 of the Cybersecurity Law of the People's Republic of China, 2017.
251 *Cybercrime Prevention Act* of 2012.
252 *Republic Act* No. 10175.
253 Section 4 of the *Republic Act* No. 10175.
254 Section 4 of the *Republic Act* no.10175.

> system without a right.[255] Illegal interception, the interception made by technical means without the right of any non-public transmission of computer data to or from or within a computer system including electromagnetic emissions.[256] Data alteration, intentional or reckless alteration, corruption, deletion or unauthorised deterioration of computer data, electronic documents, or electronic data messages(including the introduction or transmission of viruses)."[257]

Penalties for these crimes are contained in section 8 of the act and it states that any person found guilty of any punishable act in section 4(a) and 4(b) shall be punished with imprisonment of *prision mayor*[258] or a fine of at least Two Hundred Thousand Pesos up to a maximum amount commensurate to the damage incurred or both.[259]

Section 10[260] deals with the law enforcement authorities, and this section states the following:

> "The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) are responsible for efficient and effective law enforcement of the provisions of the law."[261]

As is the case with South African legislation for cybersecurity, foreign legislation for cybersecurity does not come without its own set of difficulties, and just like with South African legislation, the obstacles and difficulties enforcing cybercrimes are also applicable in this scenario.

It is widely accepted that cyberattacks by states on critical national infrastructures are increasing.[262] Cybersecurity is a treat to critical infrastructure that has been discussed by the United Nations via a parallel process on the global cyber governance in the Group of Governance experts on the responsible state behaviour in cyberspace.[263]

---

255 Section 4(a)(1) of the *Republic Act* no.10175.
256 Section 4(a)(2) of the *Republic Act* no.10175.
257 Section 4(a)(3) of the *Republic Act* no.10175.
258 The duration of the penalties of prison mayor and temporary disqualification shall be from six years and one day to twelve years.
259 Section 8 of the *Republic Act* No.10175.
260 Section 10 of the *Republic Act* No. 10175.
261 Section 10 of the *Republic Act* No.10175.
262 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.
263 Chatham House 2021

Even though cybercrime is a crime that is transnational and is not affected by borders, nationality can also coordinate with actors from other jurisdictions and help in the purview of law enforcement and the justice around cybercrimes.[264] When attacks take place on the national critical infrastructure of a state it shows that it is time to re-assess the intersections between cybersecurity and cybercrime. This persistent threat that is created by cyberattacks, undermines the overall security of countries as the core values of a country is undermined and exposed to these cybercriminals.[265] There should be a broadening of the understanding of what contributes to national security, and this is to know what protection is then needed. There is significance on the plurality of actors that uses cybercrimes in order to cause disruption and a greater recognition of the threat being posed when the focus shifts towards mitigation.[266]

Understanding and appreciating the interconnectedness of cybercrimes and cybersecurity is the first step in adopting a holistic and fluid framework to prevent, protect and mitigate disruptions from cyberattacks.[267] Removing silos between cybersecurity and cybercrime should start at national level with countries implementing national cyber coordination and this has the purpose to monitor, prevent, respond and in the end mitigate cybercrime and cybersecurity threats.[268]

---

https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

264 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

265 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

266 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

267 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

268 Chatham House 2021

When it comes to an international level and the debates about the cyber governance in the UN General Assembly together with the third committee negotiations on the *Budapest Convention on Cybercrime*[269] an approach that is more nuanced to cybercrime as a threat to national as well as international security should be established.[270] Further in this discussion there should be a greater premium placed on state and non-state actors for the assessing and analysing of attacks. Just as was the case with South African legislation, foreign legislation is newly enacted and also has not had the time to prove that it is efficient in the addressing the problems we are facing but this is once again a step in the right direction towards overcoming cybersecurity threats. In terms of litigation and with regard to the legislation set out above, there has been very little litigation in this regard. It is difficult and almost impossible, therefore, to make any assumption around the successes of litigation when very little to no litigation has taken place.

3.5.2 Customary International and Regional law for Cybersecurity

In this part of the dissertation, there will be discussion about customary international law as well as regional law. Regional law referring to certain international instruments such as the *EU Cybersecurity Act*[271] together with the *Budapest Convention on Cybercrime*[272] and the *African Union Convention on Cyber Security and Personal Data Protection*[273] will be discussed, specifically how it works and where it is applicable.

Customary international law refers to international obligations that are not formally enshrined in treaties or conventions, but that exist as part of ordinary international practice.[274] Multiple states have a sense of a legal obligation which is created through

---

https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

269 *Budapest Convention on Cybercrime*, 2001.

270 Chatham House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE.

271 *EU Cybersecurity Act* of 2019.

272 *Budapest Convention on Cybercrime*, 2001.

273 *African Union Convention on Cyber Security and Personal Data Protection,* 2014.

274 Wex 2022 https://www.law.cornell.edu/wex/customary_international_law.

general and consistent practice, and which then results in Customary International Law. Customary International law is defined under Article 38(1)(b) of the International Court of Justice (hereinafter the ICJ) as 'usual and general practice that is accepted as law'.[275] Under Article 38 of the Statute of the International Court of Justice the following are sources of Customary International Law:

> "Treaties between states, Customary International Law derived from the practice of states, general principles of law recognized by civilized nations and finally judicial decisions and writings of highly qualified publicists."[276]

Customary International Law is a two-legged approach, the first being general state practice and the second being *opinio juris*.[277] The first part of Customary International Law is that there must be general and widespread consistent state practice. The second part which reference is made to, is referred to as the opinion of the law, or in other words what has been accepted as law by states.[278]

With reference to Custom or state practice, for a rule to qualify as custom, the rule must receive general and widespread acceptance.[279] Although universal acceptance is not necessary, Rumpff CJ has suggested in the case of *Nduli v Minister of Justice*[280] that universal acceptance is necessary.[281] In the case of *S v Petane*[282] judge Conradie has made it clear that if a state persistently objects to a particular practice while the law is still in the process of being developed, it cannot be bound by any customary rule that emerges from such a practice.[283] With reference to the second part, *opinio juris,* the belief in obligation is not entirely satisfactory due to the fact that many rules are permissive, and one must realize that *opinio juris* is a belief not in obligation but a

---

275 Article 38(1)(b) of the International Court of Justice.
276 Greenwood 2008 https://legal.un.org/avl/pdf/ls/Greenwood_outline.pdf#:~:text=While%20treaties%20and%20custom%20are%20the%20most%20important,in%20a%20wide%20range%20of%20national%20legal%20systems.
277 Anon Date Unknown https://ruwanthikagunaratne.wordpress.com/2011/04/22/opinio-juris/.
278 Anon Date Unknown https://ruwanthikagunaratne.wordpress.com/2011/04/22/opinio-juris/.
279 Dugard International Law A South African Perspective 28.
280 *Nduli v Minister of Justice 1978 (1) SA 893 (A) at 906D.*
281 *Nduli v Minister of Justice 1978 (1) SA 893 (A) at 906D*.
282 *S v Petane 1988 (3) SA 51 (C) at 64A-B.*
283 *S v Petane 1988 (3) SA 51 (C) at 64A-B.*

belief in right.[284] For sufficient practice of Customary International Law, there needs to be sufficient practice together with opinio juris and only then a new rule of custom will emerge.[285]

A precedent that formed Customary International law was articulated by the International Court of Justice in the *Nicaragua v United States*[286] case. It held that those customary contractual obligations that would arise from a consistent widespread practice of States are engaging.[287] The proving of *opinio juris* is a difficult task to achieve especially when it is referred to the cyber context, and this dilemma that it creates can be solved by the suggestion that the ICJ makes. The ICJ has the preferred method of proving *opinio juris* by identifying broad principles that enjoy a widespread international agreement between states which the ICJ believe is evidenced by treaties.[288] In my opinion the success of Customary International Law is that it is capable of filling the gaps that are created by national, foreign and international law.

Customary international law as mentioned above can be describe as one of the ways forward in the maritime industry and this is with specific reference to Customary International Law and cybersecurity and how this can deal with minimising cyber risks. If states through their general and widespread action can create a legal obligation to prosecute cybercrimes, this may very well help in minimising cybersecurity risks. Legislation on the one hand is state specific, and on the other hand treaties and International Conventions are only binding on signatories thereto and if by chance we get past the obstacles of enforcing cybercrimes these legislations and international conventions and instruments can only be used on the nation states they were designed

---

284 Greenwood 2008 https://legal.un.org/avl/pdf/ls/Greenwood_outline.pdf#:~:text=While%20treaties%20and%20custom%20are%20the%20most%20important,in%20a%20wide%20range%20of%20national%20legal%20systems.

285 Greenwood 2008 https://legal.un.org/avl/pdf/ls/Greenwood_outline.pdf#:~:text=While%20treaties%20and%20custom%20are%20the%20most%20important,in%20a%20wide%20range%20of%20national%20legal%20systems.

286 *Nicaragua vs United States of America* 1986 I.C.J. 14.

287 *Opinio juris sive necessesitatis* or simply known as opinion juris is the belief that an action was carried out as a legal obligation. Gunaratne 2011 https://ruwanthikagunaratne.wordpress.com/2011/04/22/opinio-juris/.

288 Shackelford, Russel and Kuehn 2016 *CIJL 27.*

for or the signatories to the conventions, but it can be difficult to be efficient if there are what is known as persistent objectors to the creation of customary international law. As it is clear, customary international law is complex, but it also has several limitations thereto, which is that it cannot be made in coordinated manners in advance to certain events and also it cannot be made with sufficient and all the necessary details.[289] Customary international law principles are not made with the heterogenous reciprocity that is needed and it is also not specifically designed for organisational support.[290]

With reference to cybercrime, international agreements such as the *Budapest Convention*[291] and the *African Union Convention on Cyber Security and Data Protection*[292] could serve as *opinio juris* that states are obligated to enact and enforce cybercrime laws in their jurisdictions and cooperate in the prosecution and extradition of cybercriminals.[293] But even these international agreements and conventions lack binding language, but nonetheless there is growing international consensus that is the establishment of domestic cybercrime laws is an international obligation.[294]

With the exceptions of the EU Cybersecurity Act[295], the *Budapest Convention on Cybercrime*[296] and the *African Union Convention on Cyber Security and Personal Data Protection*[297] of which the African Union Convention[298] is not yet in force, there is no international law that has tailor-made rules for regulating cyberspace. There is national and foreign legislation and regulations that are country specific, but no law regulating cyberspace internationally. Today, most states and several international organisations that include the UN General Assembly, the First Committee on Disarmament and International Security, the G20 and the European Union have affirmed that existing

289 Trachtman *The Obsolescence of Customary International* Law 1.
290 Trachtman The Obsolescence of Customary International Law 1.
291 Shackelford, Russel and Kuehn 2016 *CIJL* 27.
292 Shackelford, Russel and Kuehn 2016 *CIJL* 30.
293 Shackelford, Russel and Kuehn 2016 *CIJL* 29.
294 Shackelford, Russel and Kuehn 2016 *CIJL* 30.
295 *EU Cybersecurity Act* of 2019.
296 *Budapest Convention on Cybercrime*, 2001.
297 *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
298 *African Union Convention on Cyber Security and Personal Data Protection,* 2014.

international law applies to the use of information and communication technologies (hereinafter ICTs) by states.[299]

International issues are generally regulated and governed by international agreements and international law. The governance of cyberspace does not originate with states, but it originates from academic institutions and private actors. [300] Because international law is primarily a legal order for states, international law does not have a monopoly for the regulation of cyberspace. The regulating and governance of cyberspace can now be found in multistakeholder governance[301] which has become the main governance of the internet's architecture.[302] To follow is a discussion of some international laws and regulations and how they may be useful in dealing with cybersecurity and cybersecurity problems.

The final international instruments and regulations that will be discussed with regard to cybersecurity is firstly the EU *Cybersecurity Act*.[303] The *EU Cybersecurity Act*[304] is a response to recent cybersecurity incidents, and the Act is meant to strengthen cybersecurity preparedness in Member States and to increase awareness of citizens on cybersecurity issues.[305] Furthermore, it must increase the overall transparency of cybersecurity assurance and avoid fragmentation of certification schemes in the EU.[306] The Act has different certification levels, which go from high to low. A high certification level is a defence against the ultra-modern cyber-attacks that take place, or which happen with extensive sources and state of the art security functions.[307] A medium certification level is the minimization of a known cyber risk by an actor with only limited

---

299 Carnegie *Endownment for International Peace A Brief Primer on International Law and Cyberspace.*
300 Carnegie *Endownment for International Peace A Brief Primer on International Law and Cyberspace.*
301 Multistakeholder governance is a practice of governance that employs bringing multiple stakeholders together to participate in dialogue, decision making, and implementation of responses to jointly perceived problems.
302 Carnegie Endownment for International Peace A Brief Primer on International Law and Cyberspace.
303 *EU Cybersecurity Act* of 2019.
304 *EU Cybersecurity Act* of 2019.
305 *EU Cybersecurity Act* of 2019.
306 *EU Cybersecurity Act* of 2019.
307 Kipker 2019 International Regulation of Cybersecurity file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.

resources and now public known vulnerabilities.[308] Finally a low certification level is the minimization of basic risks, and a review of technical documentation.[309]

Secondly, the *African Union Convention on Cyber Security and Personal Data Protection* in article 24[310] deals with the national cyber security framework, and it states that it is working with stakeholders to develop a National Cybersecurity Policy that recognizes the importance of the Critical Information Infrastructure (CII) to identify the risk that are being faced.[311] Article 25 of the Convention[312] deals with legislation against cybercrime and in this article it states that:

> "Each party state shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affects the confidentiality, integrity, availability and survival of information."[313]

Article 27 of this Convention[314] deals with the national cyber security monitoring structures and it is stated that each party state shall adopt the measures that are necessary to ensure an appropriate institutional mechanism responsible for cyber security governance.[315] In this article it also deals with the establishment of clear accountability in all matters of cyber security and this can be achieved by defining the roles and responsibilities in precise terms to the people responsible.[316] It is further mentioned that cyber security governance should be established within national frameworks that are capable of dealing and responding to perceived challenges of cyber risks or any issues relating to cyber security at a national level.[317]

Finally, the *Budapest Convention on Cybercrime*[318] will be discussed, and in this Convention the articles that apply to this dissertation will be discussed, which will

---

308 Kipker 2019 International Regulation of Cybersecurity file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.
309 Kipker 2019 International Regulation of Cybersecurity file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf.
310 Article 24 of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
311 Article 24(1) of the *African Union Convention on Cyber Security and Personal Data Protection,* 2014.
312 Article 25 of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
313 Article 25 of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
314 Article 27 of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
315 Article 27(1)(a) of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
316 Article 27(b) of the *African Union Convention on Cyber Security and Personal Data Protection,* 2014.
317 Article 27(c) of the *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
318 *Budapest Convention on Cybercrime*, 2001.

include jurisdiction, and measures to be taken against certain cybercrimes. In this Convention article 2 and 3 deal with illegal access and illegal interception. With reference to illegal access it states that each party shall enact such legislative measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally.[319] Illegal interception in article 3 states that each party state shall adopt such legislative and other means as and when appropriate to establish criminal offences when these acts for the interception of data without a right, made by technical means and of non-public transmissions of computer data to, from or within a computer system. Are committed intentionally[320]

Article 22 of this Convention deals with jurisdiction and each State Party shall have jurisdiction over offenses under articles 2 to 11 of this Convention, if committed on its territory. It stipulates that necessary legislative and other measures shall be taken to establish jurisdiction, if the offence is committed, in its territory,[321] on board a ship flying the flag of that party,[322] on board an aircraft registered under the laws of that party,[323] and if the offence was committed by one of its nationals, if the offence was punishable under criminal law where it was committed.[324] Finally in this article the provision relating to international co-operation is discussed, and this is contained in article 23 of the Convention.[325] In this article it is set out that the parties to this Convention shall co-operate with each other and in conformity with the provisions of this chapter and through the applicable international instruments on international co-operation on criminal matters.[326]

The purpose of these instruments is to show and understand that cybersecurity is a threat worldwide, but more than enough legislation and regulations are available to

319 Article 2 of the *Budapest Convention on Cybercrime*, 2001.
320 Article 3 of the *Budapest Convention on Cybercrime,* 2001.
321 Article 22(1)(a) of the *Budapest Convention on Cybercrime*, 2001.
322 Article 22(1)(b) of the *Budapest Convention on Cybercrime*, 2001.
323 Article 22(1)(c) of the *Budapest Convention on Cybercrime*, 2001.
324 Article 22(1)(d) of the *Budapest Convention on Cybercrime*, 2001.
325 Article 23 of the *Budapest Convention on Cybercrime*, 2001.
326 Article 23 of the *Budapest Convention on Cybercrime,* 2001.

deal with cyber risks, and more importantly to play a supporting role in implementing a risk management programme.

3.5.2.1 Application of International law to cyberspace

In the discussion of application of international law to cyberspace, especially after the discussion in the previous chapter regarding different international laws and regulations, there are aspects that will be discussed. The first of these are the two principles, namely sovereignty and non-interference, and the second is the intersection between international humanitarian and human rights law that will now be referred to in the discussion.

When the principle of sovereignty is discussed in the cyber context, a group of experts who were involved in the *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* were considering the possibility to determine the criteria for infringements of the target State's territorial integrity where the cyber intrusions or cyber-attacks that take place will only reach a certain level of violation of sovereignty as compared to the level of harmful effects the cyber intrusion causes.[327] An agreement was reached that a cyber operation that causes physical damage to any cyber infrastructure would then qualify as a violation of sovereignty.[328] In time to come, State practice and the practice of *opinio juris* may give rise to an understanding of cyber-specific intrusion of the principle of sovereignty, just as state practice has done in other forms of international law.[329]

Second is the discussion about non-intervention, and this principle is derived from the principle of sovereignty that was discussed above. The main objective of this principle is that states are prohibited from intervening with the business of another State's

---

327 Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

328 Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

329 Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

sovereign power.[330] An example of this can be seen in the Nicaragua v United States of America case where the principle of non-intervention and state sovereignty was recognized.[331] When the focus shifts from the two principles as individuals to mentioning them as overlapping, it has been mentioned that state sovereignty can be violated when the cyber activity of a state results in the usurpation of the targeted state's government functions.[332]

The second discussion in this chapter is about dealing with the intersection between international humanitarian law and International human rights law. When discussing International Humanitarian Law and International Human Rights Law the question of what human rights is affected needs to be discussed. When human rights are discussed in cybersecurity, reference dis mostly made to the human rights that are contained and guaranteed under the United Nations' Universal Declaration of Human Rights (hereinafter the UDHR) and the International Covenant on Civil and Political Rights (hereinafter the ICCPR) and these include the following rights, freedom of expression, freedom of speech, the right to privacy, freedom of opinion and the freedom of association.[333] In 2011 the UN Special Rapporteur on Freedom of Opinion and Expression and other free expression rapporteurs from Europe, America and Africa have signed a declaration which confirms that the human right 'freedom of expression applies to the internet'.[334] A year later in 2012 it was confirmed by the UN Human Rights Council that the same rights that people enjoy offline should also be protected online.[335]

In order to ascertain what combination of international humanitarian law and international human rights law should apply to cyber-attacks, the intersections between them need to be investigated. Human rights conventions are generally

---

330 Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

331 *Nicaragua v United States of America* 1986 I.C.J 14.

332 Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

333 Rossini and Green *GCCS* 2015.

334 Rossini and Green GCCS 2015.

335 Rossini and Green GCCS 2015.

responsible for implementing obligations on states and do not focus on the individual, but in turn where there are treaties in places or *erga omnes* customary law obligations that have been established then states have an obligation to protect these international legal obligations imposed on them.[336] International Humanitarian law on the other hand is created with the objective of protecting members of specific groups during types of armed conflict.[337] The purpose of international humanitarian law is to lay down the obligations which States are bound to respect. The international humanitarian law and the international human Rights law were designed originally with the objective to apply in different circumstances and therefore the two bodies of law may cross-fertilize as they both apply to cyber-attacks.[338] International human rights law applies in the aspect that it creates obligations for States to protect relevant human rights as was previously discussed.

International humanitarian law and International human rights law is not a solution to cyber-attacks or cyber threats that we may experience, but these conventions and treaties that are in place can always act as guidelines in assisting the combat against cyber-attacks or threats.

3.6 The way forward for the maritime industry

The maritime transportation industry is now accountable for almost 90% of all international cargoes and therefore it plays a very important role in the functioning of the global economy.[339] The fact that maritime transportation is responsible for such a large number of economic activities makes it vulnerable to the risks and cyber threats that may occur. The struggles that the maritime industry endures are conjunctural problems and these problems range from macroeconomic changes to political changes.[340] There is no direct or absolute way to prevent this from happening, but what can be done is to implement risk management and risk assessment programmes that are designed to deal with problems like these and that can be implemented in a

336 *Cyber-attacks in International Law: From Atomic war to computer war* 15.
337 *Cyber-attacks in International Law: From Atomic war to computer war* 15.
338 *Cyber-attacks in International Law: From Atomic war to computer war* 15.
339 Balkan 2020 *AID 2020*.
340 Balkan 2020 *AID 2020*.

multi stakeholder initiative which would include all the relevant parties, including business, civil society and other stakeholder such as the government.[341]

Cyber risk management programmes will react differently to different situations, and these cyber risk management programmes need to have the capacity to be built according to a strategic management plan.[342] The risk management and risk assessment plans need to reshape the organisation as it deems necessary and this shaping covers the following areas.[343] Critical personnel need to be competent and trained to know how to respond to different situations that may occur.[344] The fields of activity in the organisation needs to be diversified such as enabling the collection storge and use of large and diverse amounts of data. This means that the activities of the organisation should not be narrow, but widespread to enable digitalisation in the organisation.[345] Risk management and risk assessment programmes will be discussed in more detail in chapter 4 of this dissertation.

The 4IR has introduced new technologies to the shipping and maritime industry and while most of these technologies have been deployed and accepted some technologies are yet to be introduced to the shipping industry.[346] Among these new technologies that are introduced to the shipping and maritime shipping, are the emerging technologies of autonomous or unmanned vessels.[347] While some ships already have a form of unmanned or autonomous systems the shipping industry is coming into alignment with Industry 4.0, with the emergence of unmanned or autonomous vessels which are operated remotely by machinery and systems that make the decisions on the vessels.[348] In June 2017, the first remotely operated commercial vessel was tested

341 Balkan 2020 *AID 2020.*
342 Balkan 2020 *AID 2020.*
343 Balkan 2020 *AID 2020.*
344 Balkan 2020 *AID 2020.*
345 Balkan 2020 *AID 2020.*
346 Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* 16.
347 Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* 16.
348 Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* 16.

and demonstrated in the Copenhagen harbour in Denmark,[349] however, it is estimated that fully autonomous and unmanned ocean-going vessels will only be launched in 2035 as understandably, some work still needs to be done.[350] Cyber risk management is mentioned and the purpose is to show and understand that a cyber risk management plan is not a plan fit for every organization, it needs to be customised according to each organization's needs, allowing it to cover all the necessary areas, from personnel training to responding to different situations. The goal of discussing the way forward in the maritime industry is to show that the maritime industry is moving forward with technology. This was discussed in showing that shipping is becoming partly unmanned and it is expected to be completely unmanned and autonomous in the near future, ruling out human error that can create cyber risks on board these vessels. Human error is not the sole cause of cyber-attacks that occur, but it is part of the problem, there has however also been unmanned vessels that have been subject to cyber-attacks which makes it clear that the problem is more than just human error. Human error is not the only problem, but it sure is part of the problem.

The colonial pipeline incident is a ransomware attack that took place in May 2021. The colonial pipeline consists of more than 8 850 kilometer of pipeline that originates in Houston, Texas o the coast of the Gulf of Mexico and it terminates at the port of New York and New Jersey. The attack that happened infected the systems of this pipeline systems causing it to shut down for several days.[351] The effect of this incident was widespread as it affected consumers and airlines along the East Coast. Due to the fact that this pipeline moves oil from refineries to industry markets, has caused it to be deemed a national security threat. [352] The Pipeline is responsible for the moving of refined oil for gasoline, jet fuel and home heating oil. The attackers named DarkSide had accessed the network through an exposed VPN pass and stole 100 gigabytes worth

---

349 Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* 17.

350 Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* 17.

351 Kerner 2022 https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

352 Kerner 2022 https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

of data in a very short period of time and following the theft they infected the colonial pipeline IT network with ransomware. [353] The hackers gained access to the colonial pipeline network system wherethrough the started to steal the data and threatening to expose the stole data.

The above-mentioned deals with how the future for the maritime industry looks like, and it seems to be growing at an astonishing pace. Therefore, the legislation that is in place must be capable of changing extremely fast in order to keep up with the trends that the 4IR brings. Some legislation like the *Cybercrimes Act*[354] which has only been introduced in 2020 is the newest of the legislation and regulations that have been mentioned earlier. Therefore, legislation like this act may very well still be able to deal with cybersecurity for some time to come, what is meant by this is that at the moment this legislation may be adequate as it was developed in light of the current circumstances and the current need we have for cybersecurity but as the area cybersecurity is evolving at an enormous pace, this may need to be amended in time to come. The legislation that is referred to can be adequate for time to come due to the fact that it was introduced recently and in light of the present circumstances relating to cyberrisks in the maritime sector. Legislation in general needs to either be updated or amended on a regular basis to keep up with the trend. Alternatively, when these laws and regulations are amended, they must be so amended that the scope of application is broad enough to deal with cybersecurity and the fast-changing pace of the world we live in so that it need not be amended every year or even every few months. This can be done by implementing better, stronger and clearer guidelines relating to cybercrimes and cybersecurity. Furthermore, the introduction of better legislation and better training in relation to the above-mentioned.

From the above paragraph dealing with legislation, it is also clear there is effective law, but as a fast-changing subject this legislation will need to be updated and amended frequently to keep up with the fast-changing pace of cybersecurity. Through

---

353 Kerner 2022 https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

354 *Cybercrimes Act* 19 of 2020.

the action that states take in order to prevent cyberattacks and deal with cybersecurity, there is a development of cyber law through Custom.[355]

Therefore, if states can prosecute cybercriminals and people responsible for cybercrimes through international laws and conventions then through the actions of these states that have started to prosecute cybercriminals, prosecution of cybercrime can become state practice which would lead to a binding obligation which would be known as Customary International Law, which would be able to act as a way forward in the fight against cybercrime, cyber-attacks and cybercriminals. The binding obligation is when States accord immunity because of the believe that there is a legal duty to do something. Therefore, the binding obligation referred to in customary international law only takes effect one there is belief of an existing obligation. If states prosecute criminals in terms of their own national legislation, then this would not contribute to what is known as customary international law.

Because the internet and the way it respawned into an entirely new domain of operations referred to as 'cyberspace' has existed for only a very short time, there is no robust body of law governing state conduct in cyberspace.[356] Most states have laws relating to cybersecurity and how to deal with it and there is international law that can be seen as a way to deal with cybersecurity and cyber-attacks but there is no body of law that governs cybersecurity.[357] But as times goes on the development of cyber law will be through the actions that state actors take in managing cyber-attacks and dealing with cybersecurity. Furthermore, the framework will remain through the way that states have made public on the way that international law applies in the cyberspace. This means that international law exists for the regulation of states' cyber activities, and over time the creation of customary international law may very well become a part of the solution to cyber risks that we experience.

Customary international law is mentioned in this part of the dissertation as a way forward in the maritime industry and this is with specific reference to Customary

355 Brown and Poellet 2012 JSTOR 129.
356 Brown and Poellet 2012 JSTOR 129.
357 Brown and Poellet 2012 JSTOR 129.

International Law and cybersecurity and how this can deal with minimising cyber risks. If through their general and widespread action states can create a legal obligation to prosecute cybercrimes, this may very well help in minimising cybersecurity risks. Legislation on the one hand is state specific and on the other hand there are treaties and International Conventions that are only binding on signatories thereto. If by chance, we get past the obstacles of enforcing cybercrimes these legislations and international conventions and instruments can only be used on the nation states they were designed for or the signatories to the conventions and therefore these are not very efficient. With specific reference to what opinion juris is and why customary international law can be the way forward for maritime cybersecurity and cybersecurity risks in the maritime sector, focus needs to be placed on the requirements for customary international law, what it is and what obligations are being placed on states if customary international law is well established.

The requirement for the identification of customary international law is two-sided, one side is a general practice, and the other side is the acceptance of such practice.[358]

As can be seen in the previous chapters of this dissertation there are many instances of legislation and regulations around maritime cybersecurity, but the main problem is that these legislations and regulations are not entirely effective due to the fact that these laws and regulations are country specific. The International Conventions on Cybercrime and the protection against Cyberattacks are only binding on signatories to these conventions. This is exactly where customary international law comes in and has the ability to play a very big role in the prevention and managing of cybercrimes and perhaps minimization of these cybercrimes. Customary international law will provide and create a legal obligation to which all states are bound because all states are bound by customary international law. The legal obligation created can push states towards a position of prosecuting cybercrimes and thereby also create further obligations. Customary international law is important because of the legal obligation that is created through custom and general use by states. If states begin to prosecute cybercrimes or

[358] Dugard *International Law A South African Perspective* 26.

cyber-attacks the obligation can be placed on states that are not signatories to conventions regarding cybercrime or any other convention.

4 Maritime Cybersecurity Risk Management

In this chapter of the dissertation maritime cybersecurity risk management will be discussed and later how it can be introduced to minimise maritime cyber risks or to mitigate these risks. Cybersecurity risk management can be defined as follows:

> "Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation's cyber security threats. The first part of any cyber risk management programme is a cyber risk assessment. This will give you a snapshot of the threats that might compromise your organisation's cyber security and how severe they are. Based on your organisation's risk appetite, your cyber risk management programme determines how to prioritise and respond to those risks."[359]

As was discussed earlier in the dissertation, the world is becoming very dependent on digitalisation, connectivity and automation to become more efficient and improve its reliability by eliminating the human factor that can cause human errors.[360] Cyber-attacks on board ships have been increasing in recent times, and like this, several incidents occurred that were a result of interference that took place with the navigation equipment that these ships use.[361] As a result of these interferences that took place, the damage can range from substantial disruption to as much as financial damage or damage to the company's reputation.[362] Cyber risk management programmes that will be implemented are required to align with existing requirements, requirements that are contained in Resolution A.741(18) International Safety Management Code (hereinafter ISM) that was adopted in 1993, which has the purpose of providing a safe management and operation for ships.[363] The ISM code after first being adopted in 1993, was made mandatory with the entry thereof into force on the 1st of July 1998.[364] In adopting this code it is important to realize that there are no shipping companies that are the same neither are there shipowners who are the same and it should be

359 Anon Date Unknown https://www.itgovernance.co.uk/cyber-security-risk-management.
360 Standard Club Maritime Cyber Risk Management Guidelines 2.
361 Standard Club Maritime Cyber Risk Management Guidelines 2.
362 Standard Club Maritime Cyber Risk Management Guidelines 2.
363 Resolution A.741(18) International Safety Management Code, 1993.
364 Resolution A.741(18) International Safety Management Code, 1993.

understood that ships operate under different conditions. As a result of this the code is designed and based on general principles and objectives.[365] The International ship and port facility security code (hereinafter ISPS) came into force on the 1st of July 2004. The purpose of this code is a framework that was developed which allows ships and port facilities to co-operate to deter and deter acts which pose a threat to maritime security.[366] The procedures that relate and will deal with the cyber risk management part of cyber-attacks must reflect in the Safety Management System (hereinafter SMS) and the aspects of physical security must be addressed in the Ship Security Plan (hereinafter SSP).[367]

When having regard to the urgency that there was to raise awareness around cyber vulnerabilities and the threats in the shipping industry, the International Maritime Organisation (hereinafter IMO) and the Maritime Safety committee approved what is known as the "Interim Guidelines on Maritime Cyber Risk Management".[368] The purpose of these guidelines were to provide guidance for high level recommendations for maritime cyber risk management.[369]

IMO Instruments may not always be binding, they are sometime mandatory and sometimes they are merely a recommendation. The IMO is the sources for approximately 60 legal instruments that have the purpose of improving safety at sea and also to protect the maritime environment.[370] The top layer of instruments consists of IMO instruments, whereas the second layer codes consist of the, such as the ISM code that was mentioned above. Layer three consist of technical resolutions and circulars which give interpretation and layer four is standalone resolutions and circulars. In identifying the legal status of these legal instruments is not always s

---

365 Resolution A.741(18) International Safety Management Code, 1993.

366 The ISPS is an essential security measure put in place as a result of the 9/11 terrorist attacks. The main purpose of ISPS is to regulate and control the security and safety of the crew, ships, ports and cargo as they travel through international waters.
Anish 2020 https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/.

367 Standard Club Maritime Cyber Risk Management Guidelines 2.

368 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.

369 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.

370 Nam 2021 J Korean Soc. Mar. 421.

straight forward as it seems.[371] Top layer instruments, which is IMO Conventions will always be mandatory in nature and second layer legal instruments such as IMO codes have exceptions and are not always mandatory and can sometimes be recommendatory.[372] But beside the exceptions of certain IMO codes, they are mostly mandatory of nature.[373]

The IMO has released guidelines on maritime cyber risk management such Resolution MSC-FAL.1/Circ3 Guidelines on Maritime Cyber Risk Management[374], the FSA and the previously mentioned Resolution A741.(18) International Safety Management Code[375], to mention but a few, but the approaches that are accepted by the IMO have to do a comprehensive assessment and comparison between the shipping company's current cyber risk management posture and plan and the desired cyber risk management posture, to reveal the gaps in the system and to establish what needs to be addressed to achieve a successful risk management process.[376]

When building a cybersecurity risk management system, there are three main guidelines or directions that must be implemented to be successful. Firstly, there should be recognition of the cybersecurity risk and the development of a company-wide policy against the risk.[377] Examples of actions that can be taken include first, developing a security policy that takes cybersecurity into consideration at the same time while it is aligning the company's management policy in such a manner that management can announce the organisation wide policy inside and outside the company.[378] The company implementing this security policy should post it where it is accessible to employees and further management should ensure that employees are familiar with and educated on the policy implemented.[379] Secondly, the building of a

371 Nam 2021 J Korean Soc. Mar. 421.
372 Nam 2021 J Korean Soc. Mar. 422.
373 Nam 2021 J Korean Soc. Mar. 422.
374 Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management 5 July 2017.
375 Resolution A.741(18) International Safety Management Code, 1993.
376 Standard Club Maritime Cyber Risk Management Guidelines 2.
377 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.
378 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.
379 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

management system for cybersecurity risk, and the recommended actions that need to be taken are that the Chief Information Security Officer (CISO) establishes a cybersecurity management structure and defines the scope thereof.[380] The CISO should partake in the corporate risk management committee, and finally the directors of the company should audit the management structure and check if it is properly working according to the problem.[381] The third direction or guideline, is having secure resources for the cybersecurity measures. This guideline includes the following, identifying the necessary measures and the budgets that are needed for implementing these measures.[382] The final guidelines include providing a secure budget that is there to provide constant training for employees in accordance with their roles, considering the internal human resources for cybersecurity, and this typically includes the hiring of external resources and designing a career path for them that forms part of the organization's IT strategy.[383] When it is too difficult to train human resources for cybersecurity within the organization, using the security training that is provided by external organizations,[384] should be considered.

The National Institute of Standards and Technology (hereinafter NIST) develops technical standards and guidelines for the securing of non-national security of federal information systems, and it works together with other agencies to define security requirements for federally held information.[385] The NIST has implemented the "Framework for Improving Critical Infrastructure Cybersecurity, 2018"[386] to the principles of a risk management approach, where the steps are emphasized namely,

---

380 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

381 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

382 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

383 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

384 Anon Date Unknown https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

385 Anon 2017 https://www.commerce.gov/sites/default/files/2018 06/International%20Cybersecurity%20Priorities%20Report.pdf.

386 National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, 2018.

identify, protect, detect, respond and recover.[387] The Framework for Improving Critical Infrastructure Cybersecurity was a project launched by the convening private and public sectors in 2013 and was published in 2014.[388] During 2017 and 2018 the revisions of this framework was revised and there was relied upon different public workshops and thousands of interactions with stakeholders across the USA along with many other sectors across the world.[389] The main purpose of the NIST's framework is to provide tools for organisations to improve their cyber security resilience against future attack or cyber risks regardless of how sophisticated they are or what the size of the attack or risk may be.[390]

The principles that the NIST has implemented through the framework that should be considered as part of a risk management process's discussion will follow.

Identification is the basis of understanding the systems, the data and capabilities and also understanding that when they are disrupted may be a risk to operations. The Identification process defines the roles and responsibilities of personnel for cyber risk management, and it identifies systems, assets, data and capabilities that pose a risk to ship operations when it is disrupted by cyber threats.[391]

Protection is the second functional element, and this is the element that implements the elements of risk control processes and measures as well as contingency plans to protect against any cyber-event and furthermore ensure the continuity of the shipping operations.[392] Detection is the development and implementation activities that are necessary to detect cyber-events in a timely manner before they cause disruption.[393] If detection and advanced analytical techniques are used right a cyber-attack can be anticipated before it has even taken place.[394] Response is responsible for the

---

387 Erstad, Ostnes and Lund 2021 *Transnav* 31.
388 Framework for Improving Critical Infrastructure Cybersecurity, 2018.
389 Framework for Improving Critical Infrastructure Cybersecurity, 2018.
390 Erstad, Ostnes and Lund 2021 *Transnav* 32.
391 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.
392 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.
393 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.
394 Standard Club Maritime Cyber Risk Management Guidelines 2.

progression and implementing of activities and plans to provide resilience and to restore the systems necessary for shipping operations or any other services that were impaired due to a cyber-event.[395] The last functional element needed to sustain a culture of risk awareness is recovery. Recovery is the identification measures to back-up and be able to restore cyber systems that are necessary for any shipping operations that are impacted by a cyber-event.[396]

There are other considerations that come into the construction of a cyber risk management plan and these include national and international regulations, commercial aspects as well as insurance complications.[397] Rightship's inspection and assessment report and the OMCIF Tanker Management Self-Assessment (TMSA-3) has placed a requirement on shipowners and the operators to incorporate these policies on cyber risks, and the cyber risk procedures within the shipping company and the vessels operating system.[398] These requirements mentioned are usually more stringent than the guidelines that have been laid down by the IMO, and the reason behind these more stringent requirements are that operators need to incorporate software and system configuration management procedures and after doing this they have to demonstrate their involvement in the testing as well as the implementation of the up-to-date security programmes.[399] Furthermore with relation to the requirements being more stringent than the guidelines, is because there is a choice whether or not to incorporate these guidelines into an organisation.

The Baltic and International Maritime Council (hereinafter BIMCO) has released a cyber security clause in 2019 which reads as follows:

(a) "Each party shall

(i) implement appropriate cyber security measures and systems and otherwise use reasonable endeavours to maintain its cyber security

---

395 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security* 43.

396 Mthembu *Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security 43*.

397 Standard Club Maritime Cyber Risk Management Guidelines 6.

398 Standard Club Maritime Cyber Risk Management Guidelines 6.

399 Standard Club Maritime Cyber Risk Management Guidelines 6.

(ii) have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a cyber security incident
(iii) regularly review its cyber security arrangements to verify its application in practice and maintain and keep records evidencing the same.

(b) Each party shall use reasonable endeavours to ensure that any third-party providing services on its behalf in connection with this contract complies with the terms of subclause (a)(i)-(iii).

(c) If a party becomes aware of a cyber security incident which affects or is likely to affect either party's cyber security, it shall promptly notify the other party.

(i) if the cyber security incident is within the digital environment of one of the parties, that party shall:
- promptly take all steps reasonably necessary to mitigate and/or resolve the cyber security incident
- as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other party with details of how it may be contacted and any information it may have which may assist the other party in mitigating and/or preventing any effects of the cyber security incident."[400]

The Cyber Security Clause of BIMCO[401] fulfils three important functions, to firstly raise awareness of the risk encountered, to provide a mechanism to ensure that parties have procedures in place and to minimise the risks f cyber incidents and finally to ensure that parties mitigate and resolve the effects of an incident when it occurs.[402]

4.1 Building cyber security resilience

Cyber security resilience is a system's ability to prepare for, respond to and to recover from cyber-attacks.[403] This has emerged over the last couple of years when the traditional cyber security measures that were put into place no longer seemed to be effective and were not enough to protect organisation against the persistent cyber-attacks.[404] The question that is being asked in the cyber security world is not 'if' someone will suffer from a cyber-attack but rather 'when' such an attack will take

400 BIMCO Cyber Security Clause 2019.
401 BIMCO Cyber Security Clause 2019.
402 BIMCO Cyber Security Clause 2019.
403 Anon Date Unknown https://www.itgovernance.co.uk/cyber-resilience.
404 Anon Date Unknown https://www.itgovernance.co.uk/cyber-resilience.

place. The IMO has from the above-mentioned decided that there is a demand for cyber security resilience in the maritime industry.[405] The IMO recognizes these cyber security resilience measures in the resolution adopted on 16 June 2017"[406] The concept of cyber security resilience can be seen in the maritime sector as a very important improvement in the aspect of maritime cybersecurity. According to the IMO the importance of implementing a cyber risk management approach is meant to be more resilient towards future cyber risks.[407] The main goal of a risk management programme is to be in a state where you are 'free from danger or threat' while the meaning of resilience in this context can mean the management focuses on a system's recovery.[408]

A way to differently define this is to say that a resilience management process acknowledges that being in a state that is 'free from danger or threat' is impossible. In shipping and on-board vessels, the critical infrastructure of the vessel is made from the navigational equipment because this is responsible for the safe movement from point A to point B.[409] The IMO has been urging maritime industries to begin incorporating more resilience principles when implementing their maritime cyber risk management programmes. With reference to IMO guideline Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management this Resolution also recognizes the urgent needs to raise awareness of cyber risk and the threats and the vulnerabilities, which in turn is an important aspect for the building of resilience to cyber risks.[410] This framework can be used by an organisation as a key part of its systematic processes, but it does not have the purpose to replace an organisations systems, but rather to work in cooperation with the organisations systems.[411] The framework was specifically designed to complement existing business and cybersecurity operations.[412]

---

405 Erstad, Ostnes and Lund 2021 *Transnav* 29.
406 MSC.428(98) Maritime Cyber Risk Management in the Safety Management Systems, 2017.
407 Erstad, Ostnes and Lund 2021 *Transnav* 30.
408 Erstad, Ostnes and Lund 2021 *Transnav* 30.
409 Erstad, Ostnes and Lund 2021 *Transnav* 30.
410 Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management 5 July 2017.
411 Framework for Improving Critical Infrastructue Cybersecurity, 2018.
412 Framework for Improving Critical Infrastructue Cybersecurity,2018.

The MITRE Cyber Resilience Engineering Framework' defines cyber resiliency as:[413]

> "The ability of a nation, organisation or mission or business process to anticipate, withstand, recover from and evolve to improve capabilities in the face of, adverse conditions, stresses or attacks on the supporting cyber resources it needs to function[414]
>
> In understanding cyber resilience, it must be understood that there is one vital difference between humans and computers, and that is that a computer only needs to learn something once and never again. While it cannot perform a function that it has not yet learned, humans can.[415] A vessel can be seen as a 'working machine' but consists of different types of seafarers, which includes sailors, engineers and navigators.[416] The cyber risk management in shipping should place focus on the security and resilience of the integration, automation and network-based systems both ashore as well as those systems that are on board the vessels."[417]

Before focus can shift to discussing what are the components for building effective cyber resilience are, there must first be understood what cyber resilience is and therefore the above quoted definition of cyber resilience by the MITRE cyber resilience engineering framework is important and draws out the relevance this quote has to the topic of cyber resilience.

4.1.1 Central Components for Effective Cyber Resilience

People, Process and Technology in that specific order are the mainstays for building an effective cyber resilience or otherwise necessary for establishing a more robust framework for managing risks.[418] The three mainstays on which effective cyber resilience is built will be discussed.

4.1.1.1 People

People are one of the vulnerabilities when it comes to maritime cyber-attacks and cyber risks. Perhaps one of the biggest reasons why cyber threats and the risks

---

413 Erstad, Ostnes and Lund 2021 *Transnav* 32.
414 Mitre *Cyber resiliency engineering framework* 6.
415 Erstad, Ostnes and Lund 2021 *Transnav* 34.
416 Erstad, Ostnes and Lund 2021 *Transnav* 34.
417 Standard Club Maritime Cyber Risk Management Guidelines 6.
418 Nasdaq 2019 https://www.nasdaq.com/articles/people-process-technology-three-pronged-approach-cyber-risk-governance-2019-04-23.

associated with them can spread so quickly is because of the awareness gap.[419] People believe that cyber security is a matter for the company's IT department, although that is not entirely true. IT departments play a pivotal role in the implementing of mitigation measures which include firewalls, anti-virus software and intrusion detection systems.[420] People are a big risk to cyber threats and associated risks, and it is well-known that the competency of the crew or the staff on board vessels as well as the staff ashore play a vital role and are the primary defence against cyber risks.[421] With reference back to the Cybersecurity Law of the People's Republic of China[422] and specifically article 19 of the Act where reference was made that all levels of the government and the relevant departments must organize and carry out regular cybersecurity publicity and education and guide an stimulate relevant units in properly carrying out cybersecurity and education.[423] This is an important aspect to ensure that there is sufficient knowledge on cybersecurity and the risk related thereto. The implementation of a provisions of this nature can help with the building of cyber resilience.

Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management[424] is the IMO guideline for Maritime Cyber Risk Management and according to this guideline that are set out by the IMO it has been made clear that adequate cyber security risk management should begin at senior level management and then be further worked down through the system to be embedded as an organisational culture at all levels.[425]

Regulation (EU) 2019/881 of the European Parliament and of the Council[426] states that cybersecurity is not only an issue that is related to technology but is also one where the behaviour of each individual human is important.[427] It states that "cyber-hygiene", which is a simple routine measure that minimises their exposure to cyber risks, creates

419 Standard Club Maritime Cyber Risk Management Guidelines 6.
420 Standard Club Maritime Cyber Risk Management Guidelines 6.
421 Standard Club Maritime Cyber Risk Management Guidelines 6.
422 Cybersecurity Law of the People's Republic of China, 2017
423 Article 19 of Cybersecurity Law of the People's Republic of China, 2017.
424 Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management 5 July 2017.
425 Standard Club Maritime Cyber Risk Management Guidelines 6.
426 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019.
427 Regulation (EU) 2019/881 of the European Parliament and of the Council.

cyber resilience when it is implemented and carried out regularly by citizens, organisations and businesses.[428]

Cyber Inspectors is another key aspect for the increase of cyber resilience and the building of better cyber resilience. Cyber inspectors are dealt with in section 80 of the *Electronic Communications and Transactions Act*[429] and it states that the Director-General has the authority to appoint an employee of the Department as a Cyber Inspector and who is then empowered to perform the functions given to them by the chapter in the act. Section 81[430] deals with the powers and in short, the powers of these inspectors are to monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authorities.[431]

The guidelines being implemented is a measure to ensure that there is an appropriate level of awareness at any level and all levels of an organisation, and further it should be noted that the level of awareness should be in proportion to the roles and responsibilities in the cyber risk management system.[432] Although in terms of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)[433] there is not a mandatory training requirement for cyber security, but in terms of the ISM Code there is a requirement that staff should be qualified for their tasks and this serves as protection as well as a measure of control that form part of every cyber risk management programme.[434]

4.1.1.2 Process

Process in building cyber resilience comprises of rules, regulations and oversight, and it consists of a board that has the responsibility to help ensure that any enterprise

---

428 Regulation (EU) 2019/881 of the European Parliament and of the Council.
429 Section 80 of the *Electronic Communications and Transactions Act* 25 of 2002.
430 Section 81 of the *Electronic Communications and Transactions Act* 25 of 2002.
431 Section 81 of the *Electronic Communications and Transactions Act* 25 of 2002.
432 Standard Club Maritime Cyber Risk Management Guidelines 6.
433 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978.
434 Resolution MSC-MEPC.7/Circ.8 Revised Guidelines for the Operational Implementation of the International Safety Management (ISM) Coode by Companies, 2013.

focuses on appropriate risks.[435] The reason for this is that it is not feasible to invest an unlimited amount of money and resources on every possible threat.[436]

The assessment requirement and the management of risks are essential to the ISM Code as they are defined in paragraph 1.2 of the ISM Code objectives, and it is a key element of the risk analysis process to determine the likelihood and impact of cyber-attacks.[437] The likelihood of future cyber-attacks or any cyber security incident is not dependent on the frequency of past occurrences, but is dependent on the following factors, namely discoverability, exploitability and reproducibility.[438]

Regulation (EC) No 460/2004 of the European Parliament and of the Council has established ENISA[439] with the purpose, amongst others, to ensure that there is a high level of network and information security within the Union.[440] The purpose is to develop a culture of network and information security that is of the benefit to consumers, enterprises and public administration.[441]

A further process for the development and building of cyber resilience, is the establishment of a designated point of contact[442] which is dealt with in section 52 of the *Cybercrimes Act*.[443] In this act it states the following:

> "that the National Commissioner must establish or designate an office within the existing structures of the South African Police Service which will be known as the

---

435 Nasdaq 2019 https://www.nasdaq.com/articles/people-process-technology-three-pronged-approach-cyber-risk-governance-2019-04-23.

436 Nasdaq 2019 https://www.nasdaq.com/articles/people-process-technology-three-pronged-approach-cyber-risk-governance-2019-04-23.

437 Standard Club Maritime Cyber Risk Management Guidelines 7.

438 Standard Club Maritime Cyber Risk Management Guidelines 7.

439 ENISA is the European Union Agency for Cybersecurity which is dedicated to achieving a high common level of cybersecurity across Europe.
Anon Date Unknown https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vh6tfw7n7epz.

440 Regulation (EU) 2019/881 of the European Parliament and of the Council.

441 Regulation (EU) 2019/881 of the European Parliament and of the Council.

442 A point of contact can be defined as a person or department that can be approached for information or assistance on a specific topic.

443 Section 52 of the *Cybercrimes Act* 19 of 2020.

designated point of contact for the republic,[444] and the National Commissioner must also equip, operate and maintain the designated point of contact."[445]

The establishment of the point of contact can be helpful in building cyber resilience as this is a department or a specific person that can help to deal with certain cybersecurity risks or threats.

4.1.1.3 Technology

Each organisation may have a different solution for their problems. To assess risks, it is essential for each company and organisation to evaluate the capabilities of information technology (hereinafter IT) and operational technology (hereinafter OT) systems. Information technology includes a wide range of technologies such as information processing, e-mail systems, planned maintenance systems and procurement systems.[446] Operational Technology on the other hand consists of the hardware and software of a system that monitors and manages physical equipment and processes. These processes include bridge navigation systems, cargo handling as well as propulsion and machinery management systems.[447] Historically, OT (Operational Technology) and IT (Information Technology) have been used separately, but with the internet these are becoming increasingly integrated with one another. The result of these becoming integrated is that any cyber risk or cyber-attack can have an immediate and widespread impact.[448] When disruption of the operational technology systems takes place, the effect can lead to impeding of the ship's operation or it can cause risk to safety of life, property and the environment.[449] When the informational technology system is being disrupted, the result can range from reputational damage to sometimes legal disputes or financial losses.[450] The IMO recommends a holistic approach to maritime cyber security risk management or assessment and in this approach OT and IT should not be used separately but both

444 Section 52(1)(a) of the *Cybercrimes Act* 19 of 2020.
445 Section 52(1)(b) of the *Cybercrimes Act* 19 of 2020.
446 Standard Club Maritime Cyber Risk Management Guidelines 7.
447 Standard Club Maritime Cyber Risk Management Guidelines 7.
448 Standard Club Maritime Cyber Risk Management Guidelines 7.
449 Standard Club Maritime Cyber Risk Management Guidelines 7.
450 Standard Club Maritime Cyber Risk Management Guidelines 7.

must be used together in a cyber risk management plan and appropriate defence measures should be established against any future cyber-attacks.[451]

4.1.2 Maritime Formal Safety Assessment

The Maritime formal Safety Assessment was developed over a disaster that happened at the North Sea oil production platform Piper Alpha in 1988. The result of this disaster that had taken placed led to the IMO implementing binding guidance to evaluate safety in the maritime industry. As a result of the disaster 167 crewmen lost their lives and this can now ben seen as the worst ever oil production disaster in terms of how many human lives have been lost.[452] The FSA is used and applied to achieve a balance between technical and operational issues, which is human elements, which one is one can also be a cyber risk, marine environment protection and marine safety.[453] At the end of this chapter, an important aspect of FSA will be discussed namely As Low As Reasonably Possible (hereinafter referred to as ALARP). The FSA is not a guideline on its own, but it is an internal rule-making process that is applied by the IMO.

Formal safety assessment is a structured and systematic methodology that was introduced by the IMO, and it has the aim of enhancing maritime safety which includes but is not limited to the protection of life, health, marine environment and property.[454] This has been described as:

> "A rational and systematic process for assessing the risks associated with shipping activity and for evaluating the costs and benefits of the IMO's options for reducing these risks."[455]

It can be used as a tool to help evaluate new regulations or to compare proposed changes with existing standards.[456] Furthermore, this assessment can be used in measuring or comparing old regulations with the new ones that are being

---

451 Standard Club Maritime Cyber Risk Management Guidelines 7.
452 Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.
453 Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.
454 International Maritime Organisation *Formal Safety Assessment*.
455 Montekwa, Goerlandt and Kujala 2014 *RESS* 77 / FAS bron gedownload.
456 International Maritime Organisation *Formal Safety Assessment.*

introduced.[457] As was discussed earlier, the NIST has set out five domains that are important for a risk management process, and the five steps that the FSA (Formal Safety Equipment) consists of are similar to that of the NIST. The FSA's five steps are as follows: firstly, the identification of the hazard,[458] assessment of risks,[459] risk control options,[460] cost benefit assessment,[461] and finally the recommendations for decision-making.[462]

In other articles about the formal safety assessment, dilemmas are discussed. One such example is that according to FSA's guidelines, the use of an FSA Formal Safety Assessment should be 'consistent with, and should provide support to, the IMO's decision making process.'[463]. As was mentioned earlier, the FSA consists of five steps for a risk management process, namely identification, assessment, risk control options, cost benefit assessment and finally decision making. The FSA also has a framework, and this framework has four challenges to which any modern maritime safety regulation must respond.[464] This framework or the objectives of this framework can be achieved by implementing the five steps for a risk management process as was discussed earlier. Firstly, the framework must be proactive, this means to anticipate hazards rather than waiting for incidents to occur which would then lead to monetary loss and have an effect on the safety of members on board vessels.[465] The framework has to be systematic in using a formal and structured process.[466] It has to be transparent to be clear and justifiable of the safety level that has been achieved and

457 International Maritime Organisation *Formal Safety Assessment.*
458 International Maritime Organisation *Formal Safety Assessment.*
459 International Maritime Organisation *Formal Safety Assessment.*
460 International Maritime Organisation *Formal Safety Assessment.*
461 International Maritime Organisation *Formal Safety Assessment.*
462 International Maritime Organisation *Formal Safety Assessment.*
463 School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* 3.
464 School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* 3.
465 School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* 4.
466 School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* 4.

finally it has to be cost-effective, meaning it has to find a balance between safety and the price that is paid for that safety by stakeholders. [467]

The above-mentioned that have been discussed are very good processes and programmes to ensure cybersecurity from cyber-attacks and cyber risks which can be implemented by ship owners or ship operators as a method of trying to minimise and mitigate cyber risks and cyber-attacks on board vessels. With reference back to chapter 2[468] of this dissertation and specific reference to the POPIA Act[469] that states that companies, individuals and anyone that is targeted by cyber-attacks or has cyber risks. The POPI Act creates obligations that an individual affected should first have to comply with the provisions before being able to rely on legislation and international legal instruments to protect from cyber-attacks. The main purpose of the Act is to ensure that everything in the power of the individual or the companies or organisations are done before relying on legislation, or otherwise defined that there are proactive measures in place, rather to only reactively rely on States to locate and prosecute cybercriminals. This places the obligation to act proactively instead of reactively and with the implementation of cyber security risk management programmes this is a good start to protect without first relying on legislation and legal instruments. Further this new act creates the obligation that if there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired the responsible party is under the obligation to report what is happening or what has happened to the Regulator as set out in the act, and also to the person whose personal information has been accessed. Wen the discussion starts flowing regarding data protection and privacy one can in South Africa turn to the POPIA, but in terms of the rest of the world the focus is on the European Union's General Data Protection Regulation (hereinafter GDPR) which came into force on the 25th of May 2018.[470] The GDPR is the protective legislation for data protection and it has the aim and purpose to standardise data

---

467 School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* 4.

468 See para 3.3 above.

469 *Protection of Personal Information Act* 4 of 2013.

470 Novation Consulting Date Unknown https://novcon.co.za/wp-content/uploads/2018/01/IPD-white-paper.pdf.

protection and one can see that as is the same with POPIA as the underlying purpose is proactively protecting data and preventing cyber risks and attacks from happening rather than reacting thereto.[471]

Chapter 2 of the dissertation fits in perfectly with this discussion as well as the discussion about FSA, especially because the POPIA Act places the first obligation on people who are being targeted to take preventative measures first to protect themselves from cyber risks and/or attacks.

As can be seen in the discussion above, a risk management process or programme is one that is not easy to establish. It takes a lot of work and change to systems that people are familiar with, but in order to create such a risk management programme and to try and prevent cyber risks from happening in the future these changes are necessary. It is clear that the five-step process that has been set out by the NIST and the FSA are the best ways to prevent these attacks in the future as the 4IR continues to change the world that we live in.

At the beginning of this chapter, the background of an FSA was discussed and what led to the development of the FSA. An important aspect of an FSA is the ALARP. The basic principles of ALARP are weighing up risk control option to the cost implications to a system.[472] In essence this means what is the cost of risk control option going to be in order to achieve the least level of risks in a system and furthermore, at what stage does it become unprofitable to control the risk.[473] The ALARP compares two aspects namely the domain of risk and the level of risk and then only can it be determined which viable and comparative model suits the system the best. Therefore, it is comparing different aspects of risk to determine a system which is best suitable.[474]

---

471 Novation Consulting Date Unknown https://novcon.co.za/wp-content/uploads/2018/01/IPD-white-paper.pdf.

472 Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.

473 Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.

474 Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.

The comparative risk study that is done, is completed on the basis of cost benefit assessment.

It should be noted that everything that has been mentioned in this chapter of the dissertation should be read together with chapter 2.3 of this dissertation, with specific reference to the new POPIA act. Risk management programmes and cyber resilience implemented together with the provisions of this act are the first steps in protection against cybersecurity threats and cyber-attacks before an individual can rely on legislation and this is because legislation does not yet have the effect that it should have. Therefore, it is very important for companies, organisations and individuals to do all they can to protect themselves first and then proceed with litigation of cybersecurity matters.

5 Mitigation of Risks

The 4IR has created many difficulties for the maritime industry with regard to maritime cybersecurity and safety measures to prevent these attacks from happening. The previous chapter of this dissertation discussed risk management and risk management processes to ensure better safety on board these vessels. This chapter of the dissertation has the purpose of establishing risk mitigation factors that have a positive effect on the maritime industry. The main purpose of this chapter is to determine what risk mitigation is and how it can be used together with risk management to improve maritime cybersecurity and reduce cyber threats.

Maritime transportation plays a major role in global logistics,[475] and this is accompanied by an increasing number of cyber-attacks on these vessels year after year.[476] It has come to the realisation of people that it is critical to establish a defence mechanism on these maritime transportation networks, otherwise these attacks would leave the

[475] Maritime transport is the backbone of international trade and the global economy. Around 80 per cent of global trade by volume and over 70 per cent of global trade by value are carried by sea and handled by ports worldwide.
Matekenya 2022 https://jshippingandtrade.springeropen.com/articles/10.1186/s41072-022-00106 9#:~:text=According%20to%20Rodrigue%20(2020)%20over,measurable%20social%20and%20 economic%20gains.

[476] University of Houston *Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation.*

entire network paralysed.[477] If hackers are successful in entering a network, they can redirect vessels to different locations or they can obtain valuable information on board these vessels, including valuable cargo that is being transported by these vessels. Any of these scenarios will have a negative impact on the transportation business as lots of money can be lost due to stolen goods when these vessels are misled and eventually this will have a negative impact on international trade as people no longer have faith in security measures.[478]

There are a few questions that need to be answered before discussing cyber risk mitigation and these are first, what are the potential risk mitigation strategies in shipping operations and second, which strategies are the most important. The reason for these questions is that in the maritime industry sometimes only a limited number of resources are available and it is therefore crucial to know how to prioritise risk mitigation strategies in order of importance to reduce maritime cyber risks.[479] Risk mitigation strategies that can be effective in reducing cyber risks or threats, is the use of more advanced infrastructure which includes hardware and software upgrades.[480] It has been suggested that using advanced infrastructure could reduce the impact of such risks on the maritime sector. This sector covers the use of advanced information communication technology (ICT).[481] A further effective risk mitigation strategy is the execution of more regular employee training. Until the introduction of unmanned or autonomous vessels humans still play a vital role on ships and are also a vulnerability for any vessels exposed to cyber-attackers.[482] An important strategy to deal with all the human-caused risks and errors is to implement employee training. Regular employee training can reduce any human-caused risks, especially when operating in

---

477 University of Houston *Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation.*

478 University of Houston *Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation.*

479 Maritime Business *review Selection of effective risk mitigation strategies in container shipping operations* 414.

480 Maritime Business review *Selection of effective risk mitigation strategies in container shipping operations* 414.

481 Maritime Business review *Selection of effective risk mitigation strategies in container shipping operations* 416.

482 Maritime Business review *Selection of effective risk mitigation strategies in container shipping operations* 416.

dangerous environments or where employees must work with a high complexity IT system.[483]

In the previous chapter risk management, the importance thereof and how it can increase security against cyber-attacks or cyber threats was discussed. It is important to take notice that risk management planning is not a once off idea, it needs to be an ongoing effort and cannot stop after a qualitative risk assessment has been completed.[484] Risk mitigation strategies or plans should include the following; characterising the root causes of the risk that are identified, evaluating the risk interactions, identifying alternative mitigation strategies, methods and tools for every major risk that can occur.[485] These plans should assess and prioritize the mitigation alternatives as well as select and commit available resources that are required for the mitigation of specific risks.[486] Risk response and mitigation tools are the measures to readily eliminate when a risk is identified.

Because certain risks can be difficult to mitigate, risk mitigation should be a long-term project. A third effective risk mitigation strategy is the transfer of risks. This is the general idea that owners should allocate risks to parties that are best equipped to deal with them and to effectively deal with mitigation.[487] The transfer of risk is the basic technique whereby risk is transferred to a third party. In this sense the third arty mentioned assume the liabilities of another party. A further effective risk mitigation strategy that is mentioned is risk control and this refers to assuming a risk but taking the necessary steps to reduce, mitigate and otherwise manage its impact or likelihood.[488] Risk control can take on many forms, of these include the installing of data-gathering or early warning systems that provide information that would enable a person to more accurately assess the impact and likelihood of cyber risks.[489]

---

483 Maritime Business review *Selection of effective risk mitigation strategies in container shipping operations* 416.
484 *National Research Council "Risk Mitigation"* 41.
485 *National Research Council "Risk Mitigation"* 41.
486 *National Research Council "Risk Mitigation"* 41.
487 *National Research Council "Risk Mitigation"* 43.
488 *National Research Council "Risk Mitigation"* 45.
489 *National Research Council "Risk Mitigation"* 45.

The International Convention for the Safety of Life at Sea, 1974,[490] was amended and after the amendment became known as the SOLAS 1974. The focus of SOLAS is to protect human life during shipping activities.[491]

The management of risks associated with shipping is known as a very effective way to ensure life and safety at sea as this is the main objective of the SOLAS 1974.[492] Around the 1990s the IMO started a transition from being reactive to being proactive when it comes to marine disasters, and with this transition began the utilisation of methodologies to anticipate and prevent these accidents.[493] These risk mitigation strategies and the transition of the IMO to become more proactive, link in with each other due to the fact that both can now be seen as being proactive rather than reactive, and being proactive is better than repairing after cyber-attacks have already taken place. The methodologies that were used is the introduction of an FSA, which was discussed in the previous chapter, and this was a proactive move that was made by the IMO to ensure analytical and methodical techniques in managing risks.[494]

As it has become clear out of the argumentation thus far in the dissertation, risk management cannot function on its own to minimise the risk of cyber threats. It is also clear that risk mitigation on its own cannot minimise cyber risk or threats. Risk management and risk mitigation are two factors that need to be implemented together to be efficient. It is important to understand that cyber risks cannot be mitigated wholly, but they can be mitigated and managed to minimise damage. Risk management and risk mitigation are aspect of fighting against cybersecurity, but a was mentioned with the IMO guidelines and ISM Codes and all other legal instruments these have to be implemented together in order to be efficient against cybersecurity and cyber risks.

490 *International Convention for the safety of life at sea, 1974*.
491 Joseph and Dalaklis 2021 *J. int. marit.saf.environ.aff.shipp* 3.
492 Joseph and Dalaklis 2021 *J. int. marit.saf.environ.aff.shipp* 3.
493 Joseph and Dalaklis 2021 *J. int. marit.saf.environ.aff.shipp* 4.
494 Joseph and Dalaklis 2021 *J. int. marit.saf.environ.aff.shipp* 4.

6 Conclusion

In this dissertation we clarified that with the introduction and development of the 4IR came a fair amount of cybersecurity risks and threats in the maritime industry. The cyber risks or threats that have appeared due to the 4IR can have different effects on the maritime industry, as these risks can lead to reputational damage or even monetary damage. However, as was discussed throughout this dissertation there are ways and strategies to prevent these cybersecurity risks and threats. In this dissertation the numerous South African, foreign and international legislation and regulations have been discussed which shows that cybersecurity is a problem in the world we live in but there is developing and ever evolving legislation that can possibly address any cyber security risks that may occur in the future. When legislation was discussed, national foreign and international law including the creation of laws through custom, one principle has stood out, namely that the cybersecurity problems that we are experiencing now cannot fully be managed and solved by states and the laws and regulations of states alone but that there are many role players in effectively fighting against cybersecurity problems and attacks such as educational institutions, private actors and States and by all of these functioning together may help reaching a solution against cybersecurity problems.

These laws and regulations need to be implemented together with cyber risk management programmes and the risk mitigation strategies to be effective. The risk management programmes, and risk mitigation strategies are two very important factors for minimizing cyber risk or threats in the maritime industry. As was mentioned the one cannot be fully effective without the other, therefore risk mitigation and risk management need to be introduced and applied *in tandem*.

This dissertation has clearly indicated that risks in the maritime industry can be managed and mitigated by introducing risk management programmes, together with risk mitigation strategies, and these need to be implemented together with the national, foreign and international legislation and regulations to deal with cybersecurity risks. The legislation and regulations that are discussed throughout the dissertation certainly have a positive impact on cybersecurity and cyber-attacks, but they are not

yet fully capable to deal with the threats that the 4IR poses. Although the introduction of the legislation, law and regulations dealing with cybersecurity is a step in the right direction, we are still years away from a cyber security system that is flawless as there is still work that needs to be done with regard to this ever evolving and rapidly changing area of law.

Although legislation, law and regulations are in place, these laws are only applicable to their own states, and one cannot prosecute an individual on the laws of another country. Similarly, conventions that take place with regard to cybercrime and minimising cybersecurity risks are only binding on the signatories to such conventions, or any other States who are not persistent objectors. If a State is not a persistent objector to the laws for the creation of custom, then these States will be bound by customary international law. States therefore have no hold or leverage over other states. In the course of the discussion in this dissertation it has become clear that the way to start with prosecuting while simultaneously minimising cybersecurity risk, is through the development of customary international law whereby every state has a belief that it is bound and obligated to prosecute cyber risks and cyber-attacks through laws and regulations that have been established through consistent state practice and once again, only if the State is not a persistent objector to the development of customary international law.

Reference List

Literature

Ajayi E.F. G 2016 "Challenges to enforcement of cyber-crimes laws and policy" 2016 J. Internet Inf. System

Balkan D "Maritime 4.0 and expectation in the maritime sector" 2020 *AID* 133-170

Blaas FC *DOUBLE CRIMINALITY IN INTERNATIONAL EXTRADITION LAW* (LLM-Dissertation University of Stellenbosch 2003)

Brown G and Poellet K "The Customary International Law of Cyberspace" 2012 JSTOR 126-145

Carnegie Endownment for International Peace A Brief Primer on International Law and Cyberspace available at https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 accessed 28 February 2022

Dugard J *International Law A South African Perspective* 4th ed (Juta Cape Town 2017)

Erstad E, Ostnes R and Lund M,S "An Operational Approach to Maritime Cyber Resilience" 2021 *Transnav* 27-34

Eswara, Arun Kishore, Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines, 2013.

Hayes C *Maritime Cybersecurity: The Future of National Security* (Thesis Naval Postgraduate School Monterey, California 2016)

Integrating requirements of Industry 4.0 into maritime education and training: case study of Vietnam *World Maritime University* (2018) available at https://commons.wmu.se/cgi/viewcontent.cgi?article=1651&context=all_dissertations Accessed 24 October 2021

Jones K *Factors Affecting Cyber Risk in Maritime* (2019) available at https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/14474/CyberSecurity2019%20Factors%20Affecting%20Cyber%20Risk%20in%20Maritime.pdf?sequence=1&isAllowed=y Accessed 1 June 2021

Joseph A and Dalaklis D " The international convention for the safety of life at sea: highlighting interrelations of measures towards effective risk mitigation" (2021) *J. int. marit.saf.environ.aff.shipp*

Kavallieratos G and Katsikas S "Managing Cyber Security Risks of the Cyber-Enabled Ship" 2020 JMSE 1-19

Ladokun BA *An Analytical Approach to Characterization of targeted and untargeted attacks in critical infrastructure honeypot* (Tallin University of Technology, 2017)

Maritime Business review *Selection of effective risk mitigation strategies in container shipping operations* (2019) available at https://www.emerald.com/insight/content/doi/10.1108/MABR-04-2019-0013/full/pdf?title=selection-of-effective-risk-mitigation-strategies-in-container-shipping-operations Accessed 9 August 2021

Mitre *Cyber resiliency engineering framework* (2011) available at https://www.mitre.org/sites/default/files/pdf/11_4436.pdf Accessed 20 June 2021

Mrakovic I and Vojinovic R "Maritime Cyber Security Analysis – How to Reduce Threats?" 2019 TOMS 132-139

Mthembu SN Navigating the complex maritime cyber regime: A review of the international and domestic framework on maritime cyber security (LLM Dissertation University of KwaZulu Natal, 2019)

Nam D "Identification and Analysis of the Legal Status of International Maritime

Organization Instruments" 2021 *J. Korean Soc. Mar* 421-428

Padilla VS and Freire FF "A Contingency Plan Framework for Cyber-Attacks" 2019 *JISEM* 1-6

Rossini C and Green N "CYBERSECURITY AND HUMAN RIGHTS" 2015 *GCCS* 09-16

School of Naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* (2006) available at file:///C:/Users/thero/Downloads/Formal_Safety_Assessment_A_Critical_Review_and_Way.pdf Accessed 4 August 2021

Shackleford SJ, Russel S and Kuehn A "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors" 2016 *CIJL* 1-51

School of naval Architecture and Marine Engineering *Formal Safety Assessment: a critical review and ways to strengthen it and make it more transparent* (2006) available at file:///C:/Users/thero/Downloads/Formal_Safety_Assessment_A_Critical_Review_and_Way.pdf Accessed 4 August 2021

Skilton M and Hovsepian F *The 4th Industrial Revolution* 1st ed (Palgrave Macmillan London 2018)

Standard Club *Maritime Cyber Risk Management Guidelines* available at https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/loss-prevention-industry-expertise-handouts/3365323-sc_ie_cyber_risks_20201117_final.pdf Accessed 5 June 2021

Sullivan B, Nava E, Desai S, Sole J, Rossi M, Ramundo L and Terzi S "Defining Maritime 4.0: Reconciling principles, elements and characteristics to support vessel digitalization" 2020 IET 23-36

The Institution of Engineering and Technology *Defining Maritime 4.0: reconciling principles, elements, and characteristics to support maritime vessel digitalization* (2021) available at *https://www.researchgate.net/publication/349501163_Defining_Maritime_40_Reconciling_principles_elements_and_characteristics_to_support_maritime_vessel_digitalisation* Accessed 1 October 2021

Trachtman, Joel P. *The Obsolescence of Customary International Law* (October 21, 2014). Available at SSRN: https://ssrn.com/abstract=2512757

University of Houston *Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation* (2017) available at file:///C:/Users/thero/Downloads/ReviewonCybersecurityRiskAssessmentandEvaluationandTheirApproachesonMaritimeTransportation.pdf Accessed 5 August 2021

Case Law

Alade v Alemuloke 1988

Director of Public Prosecutions, Western Cape v Kouwenhoven; Kouwenhoven v Director of Public Prosecutions, Western Cape and Others (A181/2020) [2020] ZAWCHC 185; [2021] 1 All SA 843 (WCC); 2021 (1) SACR 579 (WCC) (23 December 2020)

Glenister v President of the Republic of South Africa & others [2011] ZACC 6; 2011 (3) SA 347 (CC)

Macfoy v United Africa Company Limited (West Africa), 1962

Nduli v Minister of Justice 1978 (1) SA 893 (A) at 906D

Nicaragua vs United States of America 1986 I.C.J. 14

S v Petane 1988 (3) SA 51 (C) at 64A-B

Salzman v S (755/18) [2019] ZASCA 145; [2020] 1 ALL SA 361 (SCA); 2020(2) SACR 200(SCA) (13 November 2019)

Legislation

China

Cybersecurity Law of the People's Republic of China, 2017

Germany

German IT Security Law 2.0

Philippines

Republic Act no.10175 of 2012

South Africa

Cybercrimes Act 19 of 2020

Electronic Communications Act 25 of 2002

Protection of Personal Information Act 4 of 2013

United States of America

Cybersecurity Information Sharing Act of 2015

International Instruments

African Union Convention on Cyber Security and Personal Data Protection (2014)

Budapest Convention on Cybercrime (2001)

European Convention on Extradition, 1957

International Convention for the safety of life at sea, 1974

International Convention on Standards of Training, Certification and Watchkeeping

for Seafarers, 1978

Resolution A.741(18) International Safety Management Code, 4 November 1993

Regulation (EU) 2019/881 of the European Parliament and of the Council, 17 April 2019

Resolution MSC.428(98) Maritime Cyber Risk Management in the Safety Management Systems, 16 June 2017

Resolution MSC-FAL.1/Circ.3 Guideline on Maritime Cyber Risk Management 5 July 2017

Internet Sources

Anonymous 2018 https://safety4sea.com/cm-drivers-of-the-4th-industrial-revolution-in-maritime-industry/?__cf_chl_jschl_tk__=536f9f8b37425f1f080e9578f49b207766307408-1619688328-0-Af8v7Zi5aFDhAkTAKecJdjwUlWAtEYYAhCygt8LXPVN6WZH0bzJ7tZuRNwjRNnoWWj4mzct0l27chi4qNdZ_oOC3wsD707F2-TJzYyHbNpCKgpg8T3YCqYOl1NOb6kapAKbWYfLMXWkxcvY-8UR6e-c8pK88zO5U_BpxEeXP9cgLvQLRUiQatxHOQFxdi5a9tbudqk2ydSdM2psY50hvqz3V3eIlHLJ44mIGoou4TBr_hXmS5xpORtQhDWZWXzys3fEqwAV-q6zKhqb-fjkCLJX7Zkq77YK60N0i3nY8426EV3vcpN_BxOL1hyNoHGubt3EfzQ5H7kUbfdenjBKF4zGw7M5aohTGBYW-CU9iPp4vtjhWIOGPcIaMd4eQwoK-VGmdWNzvW75y4rQiXuPJk79BHkMghIn2aUVGn-u2UOPvYeRIgQSGXDGHR8Vqt7fPS6noYfo_EJV1ftZQS8I7_52fiFHVkYPhhdR_1NicVawe

Anonymous 2018 *Drivers of the 4th Industrial Revolution in maritime industry* https://safety4sea.com/cm-drivers-of-the-4th-industrial-revolution-in-maritime-

industry/?__cf_chl_jschl_tk__=536f9f8b37425f1f080e9578f49b207766307408-1619688328-0-Af8v7Zi5aFDhAkTAKecJdjwUlWAtEYYAhCygt8LXPVN6WZH0bzJ7tZuRNwjRNnoWWj4mzct0l27chi4qNdZ_oOC3wsD707F2-TJzYyHbNpCKgpg8T3YCqYOl1NOb6kapAKbWYfLMXWkxcvY-8UR6e-c8pK88zO5U_BpxEeXP9cgLvQLRUiQatxHOQFxdi5a9tbudqk2ydSdM2psY50hvqz3V3eIlHLJ44mIGoou4TBr_hXmS5xpORtQhDWZWXzys3fEqwAV-q6zKhqb-fjkCLJX7Zkq77YK60N0i3nY8426EV3vcpN_BxOL1hyNoHGubt3EfzQ5H7kUbfdenjBKF4zGw7M5aohTGBYW-CU9iPp4vtjhWIOGPcIaMd4eQwoK-VGmdWNzvW75y4rQiXuPJk79BHkMghIn2aUVGn-u2UOPvYeRIgQSGXDGHR8Vqt7fPS6noYfo_EJV1ftZQS8I7_52fiFHVkYPhhdR_1NicVawe Accessed 17 April 2021

Anonymous 2020 https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/

Anonymous 2020 *Cyber-attacks on the rise in the maritime industry* https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/ Accessed 10 April 2021

Anonymous 2017 https://www.commerce.gov/sites/default/files/2018 06/International%20Cybersecurity%20Priorities%20Report.pdf

Anonymous Date Unknown https://www.oracle.com/za/internet-of-things/what-is-iot/

Anonymous Date Unknown *What is IoT* https://www.oracle.com/za/internet-of-things/what-is-iot/ Accessed 19 August 2021

Anonymous Date Unknown https://www.itgovernance.co.uk/cyber-security-risk-management

Anonymous Date Unknown *Cyber Risk Management Service* https://www.itgovernance.co.uk/cyber-security-risk-management Accessed 19 June 2021

Anonymous Date Unknown
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf

Anonymous Date Unknown *Cybersecurity Management Guidelines Ver. 2.0* https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf Accessed 4 August 2021

Anonymous Date Unknown https://ruwanthikagunaratne.wordpress.com

/2011/04/22/opinio-juris/

Anonymous Date Unknown *Opinio Juris* https://ruwanthikagunaratne.wordpress.com/2011/04/22/opinio-juris/ Accessed 3 September 2022

Anonymous Date Unknown https://www.techopedia.com/definition/30965/computer-integrated-manufacturing-cim

Anonymous Date Unknown *Computer-Integrated Manufacturing (CIM)*

https://www.techopedia.com/definition/30965/computer-integrated-manufacturing-cim Accessed 28 November 2022

Arampatzis 2020 https://www.tripwire.com/state-of-security/security-data-protection/biggest-challenges-best-practices-mitigate-risks-maritime-cybersecurity/

Arampatzis A 2020 *The Biggest Challenges and Best Practices to Mitigate Risks in Maritime Cybersecurity* https://www.tripwire.com/state-of-security/security-data-protection/biggest-challenges-best-practices-mitigate-risks-maritime-cybersecurity/ Accessed 20 April 2021

Banton 2021 https://www.investopedia.com/terms/j/jit.asp

Banton C 2021 Just in Time (JIT) https://www.investopedia.com/terms/j/jit.asp Accessed 19 September 2021

Barthwal and Agarwala 2020 https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/

Barthwal N and Agarwala N 2020 *INDUSTRY 4.0 IN THE SHIPPING INDUSTRY: CHALLENGES AND PREPAREDNESS – THE PREVAILING SCENARIO* https://maritimeindia.org/industry-4-0-in-the-shipping-industry-challenges-and-preparedness-the-prevailing-scenario/ Accessed 22 August 2021

BBC News 2020 https://www.bbc.com/news/53918580

BBC News 2020 *New Zealand stock exchange halted by cyber-attack* https://www.bbc.com/news/53918580 Accessed 29 May 2021

Chadd 2020 https://blog.avast.com/history-of-cybersecurity-avast

Chadd 2020 *The history of cybersecurity* https://blog.avast.com/history-of-cybersecurity-avast Accessed 10 August 2021

CyberPolicy Date Unknown https://www.cyberpolicy.com/cybersecurity-education/how-to-develop-a-cybersecurity-contingency-plan-asap

CyberPolicy Date Unknown *How to Develop a Cybersecurity Contingency Plan ASAP* https://www.cyberpolicy.com/cybersecurity-education/how-to-develop-a-cybersecurity-contingency-plan-asap Accessed 17 June 2021

Chantam House 2021 https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE

Chatham House 2021 *Closing the space between cybercrime and cybersecurity* https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-

cybersecurity?gclid=CjwKCAjw5NqVBhAjEiwAeCa97RJ4HHpfiAfma3dYHEBpRAYXouEf5KufPoqIuLlM5xPuNAP351fbvxoCX8wQAvD_BwE Accessed 17 August 2022

Fruhlinger 2020 https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Fruhlinger J 2020 What is phishing? How this cyber-attack works and how to prevent it https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html Accessed 20 April 2021

Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667

Giles J 2009 *Cybercrime law in South Africa explained* https://www.michalsons.com/blog/cyber-crime-explained/2667 Accessed 27 November 2021.

Greenwood 2008

https://legal.un.org/avl/pdf/ls/Greenwood_outline.pdf#:~:text=While%20treaties%
0and%20custom%20are%20the%20most%20important,in%20a%20wide%20range%20of%20national%20legal%20systems.

Greenwood C 2008 Sources of International Law: An Introduction https://legal.un.org/avl/pdf/ls/Greenwood_outline.pdf#:~:text=While%20treaties%20and%20custom%20are%20the%20most%20important,in%20a%20wide%20range%20of%20national%20legal%20systems Accessed 4 April 2023

IBM Cloud Education 2020 https://www.ibm.com/za-en/cloud/learn/what-is-artificial-intelligence

IBM Cloud Education 2020 *Artificial Intelligence* https://www.ibm.com/za-en/cloud/learn/what-is-artificial-intelligence Accessed 19 August 2021

Kipker 2019
file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf

Kipker DK 2019 *International Regulation of Cybersecurity* file:///C:/Users/thero/Downloads/InternationalRegulationofCybersecurity.pdf Accessed 17 September 2021

Lavopa and Delera 2021 https://iap.unido.org/articles/what-fourth-industrial-revolution#fn-542-1

Lavopa A and Delera M 2021 *What is the Fourth Industrial Revolution?* https://iap.unido.org/articles/what-fourth-industrial-revolution#fn-542-1 Accessed 19 June 2021

LEANPRODUCTION Date Unknown https://www.leanproduction.com/theory-of-constraints/

LEANPRODUCTION Date Unknown Theory of Constraints (TOC) https://www.leanproduction.com/theory-of-constraints/ Accessed 19 September 2021

Mavrias 2019 https://www.standard-club.com/knowledge-news/web-alert-new-cyber-security-clause-from-bimco-now-available-1108/

Mavrias N 2019 *Web Alert: New cyber security clause from BIMCO now available* https://www.standard-club.com/knowledge-news/web-alert-new-cyber-security-clause-from-bimco-now-available-1108/ Accessed 10 September 2021

Moynihan 2019 https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/

Moynihan H 2019 *The Application of International Law to Cyberspace: Sovereignty and Non-intervention https://www.justsecurity.org/67723/the-*

application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/ Accessed 1 March 2022

Nasdaq 2019 https://www.nasdaq.com/articles/people-process-technology-three-pronged-approach-cyber-risk-governance-2019-04-23

Nasdaq 2019 *People, Process, Technology: A Three-Pronged Approach to Cyber Risk Governance* https://www.nasdaq.com/articles/people-process-technology-three-pronged-approach-cyber-risk-governance-2019-04-23 Accessed 19 September 2021

Novation Consulting Date Unknown https://novcon.co.za/wpcontent/uploads/2018/01/IPD-white-paper.pdf.

Novation Consulting Date Unknown *The EU General Data Protection Regulation: Should South African Organisations Care?* https://novcon.co.za/wp-content/uploads/2018/01/IPD-white-paper.pdf Accessed 11 April 2023

Popa 2020 https://news.softpedia.com/news/did-you-know-the-first-antivirus-product-was-launched-in-1987-528883.shtml

Popa B 2020 *Did you know: The First Antivirus was launched in 1987* Did You Know: The First Antivirus Product Was Launched in 1987 (softpedia.com) Accessed 17 April 2021

Ravikumar Date Unknown https://www.infosys.com/insights/ai-automation/autonomous-technologies.html

Ravikumar G Date Unknown *Autonomous Technologies to Power Tomorrow's Enterprises* https://www.infosys.com/insights/ai-automation/autonomous-technologies.html Accessed 19 August 2021

Reva 2021 https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports

Reva D 2021 *Cyber-attacks expose the vulnerability of South Africa's ports* https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports Accessed 19 August 2021

Redaction Africanews Date Unknown https://www.africanews.com/2021/07/27/south-africa-ports-paralyzed-by-cyber-attack-struggle-to-recover//

Redaction Africanews Date Unknown *South Africa ports paralyzed by cyber-attack struggle to recover* https://www.africanews.com/2021/07/27/south-africa-ports-paralyzed-by-cyber-attack-struggle-to-recover// Accessed 19 August 2021

Riviera Newsletter 2019 https://www.rivieramm.com/news-content-hub/news-content-hub/how-maritime-can-make-the-most-of-industry-40-54225

Riviera Newsletters 2019 *How maritime can make the most of Industry 4.0* https://www.rivieramm.com/news-content-hub/news-content-hub/how-maritime-can-make-the-most-of-industry-40-54225 Accessed 17 April 2021

Sakar, Koseoglu, Buber and Toz Date Unknown https://d1wqtxts1xzle7.cloudfront.net/59963076/GMC-Cyber_security20190708-52225-1l8n1x.pdf?1562652470=&response-content-disposition=inline%3B+filename%3DAre_The_Ships_Fully_Secured_Against_The.pdf&Expires=1622707476&Signature=LudolyesWXWEWLpUUYPa~WBazi~Qz69LQozTHuc87Eil75y3qSWYrvQT5rgV5VG6DwsSjKXFQHjosskBeajoYxE9sE9fFyPhIqTlmrhPLGQ7k-MSnRBBIk~4kT51ZP4rlwEMRxeDzMHt0O1rkS9h5Q52dobN-fA6lB41XgHK7P20pi~YYfCgY4S0~3hjvtijkEkPWn5WPvLEVji8uehDVia--zOCJ5baBcY10f~yTtqN2OAzGmTsqtVgSCNAgzzaBmH~wwSNhTbXmtCujR0Nh9eOYnNdISxYmQm2IHqRiaqghpvpKakznBMmd3V8NY2UeVV5pjxtQM1hX9GV9DQjZw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Sakar C, Koseoglu B, Buber M, Toz A Date Unknown *Are The Ships Fully Secured Against The Cyber-Attacks?* https://d1wqtxts1xzle7.cloudfront.net/59963076/GMC-Cyber_security20190708-52225-1l8n1x.pdf?1562652470=&response-content-disposition=inline%3B+filename%3DAre_The_Ships_Fully_Secured_Against_The.pdf&Expires=1622707476&Signature=LudolyesWXWEWLpUUYPa~WBazi~Qz69LQozTHuc87Eil75y3qSWYrvQT5rgV5VG6DwsSjKXFQHjosskBeajoYxE9sE9fFyPhIqTlmrhPLGQ7k-MSnRBBIk~4kT51ZP4rlwEMRxeDzMHt0O1rkS9h5Q52dobN-fA6lB41XgHK7P20pi~YYfCgY4S0~3hjvtijkEkPWn5WPvLEVji8uehDVia--zOCJ5baBcY10f~yTtqN2OAzGmTsqtVgSCNAgzzaBmH~wwSNhTbXmtCujR0Nh9eOYnNdISxYmQm2IHqRiaqghpvpKakznBMmd3V8NY2UeVV5pjxtQM1hX9GV9DQjZw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA Accessed 1 June 2021

SentinelOne 2019 https://www.sentinelone.com/blog/history-of-cyber-security/

SentinelOne 2019 *The History of Cyber security – Everything you ever wanted to know* https://www.sentinelone.com/blog/history-of-cyber-security/ Accessed 7 April 2021

Shak Date Unknown https://saicom.io/news/popia-a-cybersecurity-perspective/

Shak I Date Unknown *POPIA – A cybersecurity perspective* https://saicom.io/news/popia-a-cybersecurity-perspective/ Accessed 25 August 2022

TechTarget Date Unknown https://www.techtarget.com/searchsecurity/post/Cybersecurity-contingency-planning-needs-a-face-lift

TechTarget Date Unknown *Cybersecurity contingency planning needs a face-lift* https://www.techtarget.com/searchsecurity/post/Cybersecurity-contingency-planning-needs-a-face-lift Accessed 10 April 2021

Techopedia Date Unknown https://www.techopedia.com/definition/30965/computer-integrated-manufacturing-cim

Techopedia Date Unknown Computer-Integrated Manufacturing (CIM) https://www.techopedia.com/definition/30965/computer-integrated-manufacturing-cim Accessed 19 September 2021

The White House, Washington 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House, Washington 2023 *National Cybersecurity Strategy* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf Accessed 5 April 2023

Zarzuelo 2021
https://www.sciencedirect.com/science/article/pii/S0967070X20308945

Zarzuelo I 2021 Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue https://www.sciencedirect.com/science/article/pii/S0967070X20308945 Accessed 27 April 2021