COLLEGE OF LAW AND MANAGEMENT STUDIES
Unit for Maritime Law and Maritime Studies

"Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security"

A mini dissertation submitted by:

Sibusisiwe Nothando Mthembu

Student number: 212509261

In partial fulfilment of the requirements of the degree *Master of Laws in Maritime Law.*

June 2019
Word count: 26694

Supervisor: Dr. V. Surbun

TABLE OF CONTENTS

CHAPTER THREE: LEGAL FRAMEWORK REGULATING MARITIME CYBER SECURITY

DECLARATION

I, Sibusiswe Nothando Mthembu, declare that:

(i) The research reported in this dissertation, except where otherwise indicated, is my original work.

(ii) This dissertation has not been submitted for any degree or examination at any other university.

(iii) This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

  (a) their words have been re-written but the general information attributed to them has been referenced;

  (b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the References sections.

Sibusisiwe N Mthembu

DEDICATION:

Ngifisa ukuchoma iphaphu lwegwalagwala kumalume wami uMoses Fano Ngcobo ongasekho emhlabeni. Mapholoba, Fuze, Ngcobo'omkhulu mayelana nalosomqulu.

ACKNOWLEDGEMENT

Ngithanda ukudlulisa ukubonga:

- *UNkulunkulu mdali wezulu nomhlaba. Impela gikunika udumo nezibongo zikufanele ngoba uhambile name indllela yonke ungidlulisile emaghumeni nasezintabeni. Nkulunkulu wami ngikubonile ukuthi unguNkhulunkulu onothando nonakekelayo. Ngibonga angiphezi*

  "Ngiyakumbonga uJehova ngayo yonke inhliziyo yami; ngiyakulanda zonke izimangaliso zakho"

  Amahubo 9:1

- *Abazali bami, oMvelase! oMnisi wemvula, oBayeni Ndlela! nina enawela uThukela nempofana, namaFuze amahle oMapholoba! mashiya amahle nomndemi wami wonke, ngokungilekelela ngayo yonke indlela kuloluhambo lwami. Ningithwalile ngemikhuleko iziyalo namazwi akhayo. Ngibonga angiqedi futhi niyohlezi nisondele njalo enhlizweni yami.*
- *Sengifika emaphethelweni ngifisa ukudlulisa amazwi okubonga kakhulu kumphathi wazemfundo uDokotela Vishal Surbun ngegalelo lakhe elihlabasohlile ukungaluseni kulomsebenzi. Isineke kanye namaxhamo okuxhumana, kuyababazeka.*

LIST OF ABBREVIATIONS

AIS	Automatic Identification System
AU	African Union
BIMCO	Baltic and International Maritime Council
CEO	Chief Executive Officer
CFAA	Computer Fraud and Abuse Act
CFCR	Centre for Constitutional Rights
CIA	Central Intelligence Agency
CLIA	Cruise lines International Association
CMA	Computer Misuse Act 1990
COMSA	Common Market for Southern Africa
CSIS	Center for Strategic and International Studies
DDOS	Distributed denial of service
DoS	Denial of Services
DP	Dynamic Positioning
ECCC	European Convention on Cyber Crimes
Ecdis	Electronic Chart Display software
eCHARTS	Electronic Charts
ECOWAS	Economic Community of West African States

ECT	Electronic Communications and Transactions Act 2002
ERP	Enterprise resource planning
FBI	Federal Bureau of Investigation
FCIRC	Federal Computer Incident Response Center
GDP	Gross Domestic Product
GNSS	Global Navigation Satellite Systems
GNT	Positioning Navigation and timing
GPS	Global Positioning Systems
ICS	Industrial Control System
ICS	International Chamber of Shipping
ICT	Information and communications technology
INTERCARGO	International Association of Dry Cargo Ship owners
INTERTANKO	International Association of Independent Tanker Owners
IMCO	Inter-Governmental Maritime Consultative Organization
IMO	International Maritime Organisation
IRISL	Islamic Republic of Iran Shipping Lines
ISM	International Safety Management Code
ISP	Internet Service Provider
ISPS Code	International Ship and Port Facility Security Code
TEU	Twenty-Foot Equivalent Unit

IT	Information Technology
LSASS	Local Security Authority Subsystem Service
MIT	Massachusetts Institute of Technology
MSC	Maritime Security Council
NCPF	National Cybersecurity Policy Framework
NIST	National Institute of Standards and Technology
NPA	National Prosecuting Authority
NSA	National Security Agency Act 1998
OT	Operations Technology
PC	Personal computer
PLO	Palestine Liberation Organisation
Right 2 Know	R2K
RAM	Random-Access Memory
RICA	Regulation of Interception of Communication and Provision of Communication-Related Information 2002
SAAFF	South African Association of Freight Forwarders
SA COGSA	Carriage of Goods by Sea Act 1986
SADAQ	Southern Africa Development Community
SAHRC	South African Human Rights Commission
SAPS	South African Police Service

SARS	South African Revenue Services
SMB	Server Message Block
SOLAS	Safety of Life at Sea
SSO	Ship Security Officer
SUA	Suppression of Unlawful Acts against the Safety of Maritime Navigation
UNCLOS	United Nations Convention on the Law of the Sea
UK	United Kingdom
USA	United States of America
US-CERT	United States Computer Emergency Readiness Team

ABSTRACT:

Modern shipping companies are reliant on the proliferation of refined technological advancements such as Electric Chart Display and Information Systems (ECDIS), Automatic Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), Compass (Gyro, fluxgate, GPS and others), Computerised Automatic Steering Systems, Voyage Data Recorders – "Black box" (VDR), Radio Direction and Ranging or Automatic Radar Plotting Aid (Radar/ARPA). These technological advancements are vulnerable to cyber security threats. The prevalence of maritime cyber security incidents is increasing worldwide therefore it is imperative for the maritime industry to have legal regime in place that adequately regulates these cyber security threats.

This dissertation undertakes a critical analysis of the legal framework governing maritime cyber security and the adequacy in combating maritime cyber threats. The first chapter will provide an introduction and background to maritime cyber security. The second chapter focuses on the different threats and vulnerabilities to maritime cyber security. In addition to this reference will be made to the types of cybercrimes and their possible ramifications. The third chapter will analyse the International regulatory regimes in place, regional regulatory framework and South Africa's domestic laws regulating maritime cyber security. In the fourth Chapter a determination will be made as to the existence and adequacy of the law in combating maritime cyber threats and crimes. A conclusion will be derived from the findings of this dissertation, and recommendation will be submitted

The purpose of this study is to establish whether, (a) the existing law applies to maritime cyber security threats at all, and, if so, what is the extent of the existing laws applicability to maritime cyber security threats? (b) whether the domestic and international legal framework is adequate, in respect to enforcement and comprehensiveness, to address/respond to maritime cyber security threats? and (c) whether it is necessary to establish new regulations to address maritime cyber security or develop existing laws?

CHAPTER 1:

INTRODUCTION AND BACKGROUND

1.1. Introduction

Living in the 21st century, one cannot imagine a world without the modern technology that people and industries have at their disposal. Since the 1970s, which was canvassed by the arrival of microprocessors and the introduction of Personal Computers (PC),[1] technological advancements have provided businesses with numerous benefits including, but not limited to, increased efficiency to those processes that are at the core of the business and deliver value; improved information sharing between trading partners and enhanced communications between administrative personnel, manning organisations and vessel employees[2] in the maritime industry. Garcia-Perez comments that connected ships, which are vessels that use remote monitoring technology to connect the vessel to the management offices,[3] are manufactured with hundreds of electronic control units (ECUs)[4] and other built-in capabilities that allow direct access to the internet and enable them to consume, create, supplement direct and share digital information.[5] This information is then shared with other ships, port, oil platforms and semi submersibles.[6]

Often, ordinary citizens, business, and even government institutions view cyber security and cyber-attacks as invasion of personal security and data privacy violations,[7] however in reality cyber-attacks can have significant consequences for effects on businesses and can constitute a threat to national security.[8] Modern shipping companies are reliant on the proliferation of

[1] A Cosper 'History & Evolution of Computers' available at https://www.techwalla.com/articles/history-evolution-of-computers , accessed on 17 April 2019.
[2] M McNicholas *Maritime Security: An Introduction* (2012) 367.
[3] J Zhao et al 'A fleet technical condition management system for connected ships' (2013) 33 *The Italian Association of Chemical Engineering Online* at 799.
[4] The ECU is the electronic engine governor with integrated engine management. The ECU offers monitoring and diagnostic functions for the engine. Dr. S Ihmor & C Muller 'Monitoring and Remote Control for MTU Ship Propulsion Systems' available at https://www.mtu-online.com/fileadmin/fm-dam/mtu-global/technical-info/white-papers/3100701_MTU_General_WhitePaper_BlueVisionNG_2014.pdf, accessed on 20 May 2019.
[5] A Garcia-Perez et al 'Towards cyber security readiness in the Maritime industry: A knowledge –based approached' available at https://pdfs.semanticscholar.org/0bca/56d7f4c56899540d3ee9180ee6c8557a813b.pdf, accessed on 7 November 2018.
[6] *Ibid*
[7] J J Chung 'Critical Infrastructure, Cybersecurity, and Market Failure' (2018) 96 *Oregon Law review* 441.
[8] O A Hathaway… et al 'The law of cyber-attack' (2012) 100(817) *California Law Review* at 830.

refined technological advancements[9] such as Electric Chart Display and Information Systems (ECDIS), Automatic Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), Compass (Gyro, fluxgate, GPS and others), Computerised Automatic Steering Systems, Voyage Data Recorders – "Black box" (VDR), Radio Direction and Ranging or Automatic Radar Plotting Aid (Radar/ARPA).[10] In 2013 a team at the University of Texas at Austin demonstrated how a potential treat-agent could remotely take control of a vessel by manipulating the ship's GPS. [11] A yacht named "White Rose of Drax" was successfully "*spoofed*" while sailing on the Mediterranean, when the research team successfully sent false civil GPS signals to the vessel and slowly overpowered authentic GPS signals. This resulted in the ship actually turning but the chart display to the crew only showed a straight line.[12]

The above-mentioned vulnerabilities of maritime cyber security on board a ship, and other vulnerabilities in the maritime transportation system, including cargo, oil rigs and port operations, will be discussed in greater detail in chapter two of this dissertation.

Other incidents of these cyber threat also exist. In 1998 Sri Lankan terrorists successfully attacked the servers of three embassies in the country by carrying out a denial of service attack on these servers.[13] According to the United States Computer Emergency Readiness Team (US-CERT) [14] a denial of services attack (DoS) is an attack that "occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor".[15] Though the Sri Lankan incident is generally noted as one of the first cyber terrorist events, one of the earliest incidents that brought the magnitude and seriousness of cyber security to the forefront of the world news is the Estonia cyber-attack in 2007. Following a dispute over the relocation of a Soviet era war memorial which was originally called" Monument to the Liberators of Tallinn", Estonia became the first victim of a

---

[9] J DiRenzo 'The Little –Known Challenge of Maritime Cyber Security' available at http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf accessed on 3 June 2019.
[10] *Ibid*
[11] *Ibid*
[12] *Ibid*
[13] S W Brenner & M D Goodman 'In Defence of cyber of cyber terrorism: an argument for anticipating cyber-attacks, 2002 *Journal of law, Technology and Policy,* at 30.
[14] Which is part of the United States of America's Homeland Security is the successor entity to a variety of previous organisations such as the Federal Computer Incident Response Center (FCIRC) and the National; Infrastructure Protection Center. This information security organisation has responsibility for publishing timely security information such as advisories, technical bulletins and vulnerabilities notes in addition to more general awareness and educational materials.
[15] 'Understanding denial of service attacks' United States Computer Emergency Readiness Team (US-CERT) available at https://www.us-cert.gov/ncas/tips/ST04-015 , accessed on 12 November 2018.

coordinated attack against a nation state. [16] Online servers of Estonia's banks, government bodies and media outlets were hacked at unprecedented levels. For two nights Tallinn erupted in riots and looting which left 156 people injured, 1000 people detained and one person dead.[17]

While both the above-mentioned examples illustrated the effects of cyber threats to national security, cyber threats are great cause for concern for corporate information security conduct and the international trading industry as a whole. In 2014 Sony Music lost massive amounts of sensitive company data when their systems where hacked.

> According to Elkind, "on November 24 2014 a crushing cyber-attack was launched on Sony Pictures. Employees logging on to its network were met with the sound of gunfire, scrolling threats and the menacing images of a fiery skeleton looming over the tiny '*zomibified*' heads of the studio's top two executives... It erased everything stored on the 3262 of the company's 6797 personal computers and 837 of its 1555 servers, making sure nothing could be recovered, the attackers added a special deleting algorithm that overwrote the data seven different ways, rendering the computers brain dead".[18]

According to Fortune Magazine "the hack terrified corporate America and devastated the company". [19] The above mentioned examples solidify the argument that cyber security should not be viewed strictly as a violation of personal security and data privacy violations, but rather that threats to cyber security are both a business law concern as well as a national security concern. The maritime industry should view cybersecurity as such.

The shipping industry has also suffered cyberattacks. In 2017 the *NotPetya* malware[20] infected computer network systems in companies as diverse as shipping companies to global law firms, with damage caused being estimated at $10 billion.[21] According to Reuters Shipping giant

---

[16] 'Who was behind the behind the Estonia cyber-attack?' Foreign Policy available at *https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/* accessed on 5 November 2018.
[17] 'How a cyber-attack transformed Estonia' BBC New online, 27 April 2017 available at *https://www.bbc.com/news/39655415*, accessed on 5 November 2018.
[18] P Elkind 'Inside the hack of the century' (1 July 2015) *Fortune* available at http://fortune.com/sony-hack-part-1/ accessed on 7 November 2018.
[19] T McCormack 'The Sony and OPM double whammy: International law and cyber attacks' (2015) 18 *SMU Science and Technology Law Review* at 379.
[20] The Merriam Webster online Dictionary defines malware as 'software designed to interfere with a computers normal functioning', available at *https://www.merriam-webster.com/dictionary/malware* ,accessed on 13 May 2019.
[21] A M Matwyshyn 'Cyber Harder' (2018) 24 *B.U.J SCI & Tech. L.* at 451.

A.P Moller – Maersk, which handles more than 15 per cent of global shipping[22] was affected by the *NotPetya* ransomware virus. This adapted version of the *Petya* virus was markedly more devastating in that companies could not recover their stolen data even if they paid the ransom.[23] The cyber-attack, which caused outages at its computer systems across the world in June 2017 mimicked previous malware attacks which sought financial gain, was later identified to be likely written by a nation state, which sort to cause destabilisation of another country.[24] The attack came as computer servers across Europe and India were hit by a major ransomware attack, which resulted in a breakdown that affected all business units at Maersk, including container shipping, port and tug boat operations, oil and gas production, drilling servers and oil tankers.[25] Dutch broadcaster RTV Rijnmond reported that "Maersk's port operator APM Terminals were also hit. The 17 shipping container terminals run by APM Terminals had been hacked, including two in Rotterdam and 15 in other parts of the world".[26]

The *NotPetya* malware was propelled by hackers exploiting vulnerabilities in established digital tools. A *vulnerability* in cyber security is defined as "an occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness".[27] The first vulnerability to be exploited was through the penetration of the *EternalBlue* tool. *EternalBlue* was created by the United States National Security Agency (NSA)[28] to exploit a vulnerability in Microsoft SMBv1.[29] However, earlier in 2017 there was a leak of the Agency's files to the public, by the hacking group *The Shadow Brokers*,[30] which allowed hackers to gain access to the *EternalBlue* tool. "*EternalBlue* takes advantage of this particular vulnerability in

---

[22] M Mehlman' How CFOs can mitigate the risk of ransomware' (2018) available at https://taxexecutive.org/how-cfos-can-mitigate-the-risk-of-ransomware/ accessed on 23 February 2019.
[23] *Ibid*.
[24] Matwyshyn (n 21 above) at 451.
[25] 'Maersk says global IT breakdown caused by cyber-attack' *Reuters* online, 27 June 2018 available at *https://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1NO* , accessed on 5 November 2018.
[26] *Ibid.*
[27] J Watkins 'No good deed goes unpunished: The duties held by malware researchers, penetration testers and "white hat" hackers' (2018) 19(2) *Minn J.L.SCI.& Tech at* 535.
[28] A Greenberg 'The untold story of NotPetya, the most devastating cyberattack in history' *WIRED* 22 August 2018 available at *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/* accessed on 13 May 2019.
[29] A Server Message Block (SMB) is the file protocol most commonly used by Windows. SMB Signing is a feature through which communications using SMB can digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity.
[30] A Moshirnia 'Not security through obscurity: changing circumvention law to protect our democracy against cyber attacks' (2018) 83 (4) *Brooklyn Law Review* at 1294.

machines that have not patched or fixed this vulnerability",[31] which then permits hackers to remotely run their own code on those machines.[32]

Secondly hackers used an older software called *Mimikatz*.

> "*Mimikatz* is an open-source utility that enables the viewing of credential information from the Windows LSASS(Local Security Authority Subsystem Service) through its *sekurlsa* module".[33]

Mimikatz could hack into machines by drawing passwords out of the RAM and use them to hack into other machines accessible with the same credentials.[34] On networks with multiuser computers, Mimikatz allows the hacker to access information back and forth between the networks.[35]

The combination of the *EternalBlue* tool and the *Mimikatz*, was vastly disastrous, because even though Windows had released a patch to fix the vulnerability to its system many groups had failed to either install the patch properly or had just not installed the patch.[36] The use of *Mimikatz* meant that hackers could hack computers that were not patched for the Eternal Blue vulnerability and use those computers to gain access to the password of other computers in the company.[37] The above cyber security attack, which forms the basis of this dissertation, illustrates that maritime cyber security threats are real and present a great cause of concern for the maritime sector.

1.2. Definitions

Definitions play an important role in any legal framework. It is therefore important to distinguish what functions those definitions have. In law, there are descriptive and statutory

---

[31] Watkins (n 27 above) at 537.
[32] Greenberg (n 28 above).
[33] B Cannols & A Ghafarian 'Hacking experiment by using USB rubber ducky scripting' *Systemics, Cybernetics And Informatic*s (2017) 15 (2) at 68, available at http://www.iiisci.org/journal/CV$/sci/pdfs/ZA340MX17.pdf , accessed on 12 February 2019.
[34] Greenberg (n 28 above).
[35] *Ibid.*
[36] N Perlroth…*et a*l 'Cyberattack hits Ukraine and then spreads internationally' *The New York Times Online* 27 June 2017 at 2 , available at http://www.vis-am.ch/uploads/allegati/Cyberattack_Hits_Ukraine_Then_Spreads_Internationally_-_The_New_York_Times.pdf ,accessed on 15 February 2019.
[37] Greenberg (n 28 above)

definitions.[38] Descriptive definition are “used to explain the meaning of ambiguous words”[39] whereas statutory definitions “commit those that are subject to law to a particular definition of a word.[40]

Cyber space has been defined as “the interdependent network of information technology infrastructure. It includes the internet, telecommunications networks, and computer processing systems and embedded industrial processors and controllers”.[41] These cyber networks are characterised by physical infrastructure as well as an electromagnetic spectrum that stores and transmits information and data.[42] Protecting cyber networks against penetration by either malicious or innocuous actors requires maintaining the integrity, confidentiality and availability of information as well as effective deterrence mechanisms and efficient incident responses.[43]

The term *cyber attack* can be defined as “any type of offensive manoeuvre that targets Information technology (IT)[44] and Operational Technology (OT)[45] systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data”,[46] Cyber attacks in this body of work refers to “an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.”[47] The definition of *maritime cyber security* often centre on a particular actor or a certain system instead of a more holistic approach. These definitions are problematic as they do not give a holistic approach to the term. A broad definition of *maritime cyber security* is understood as: “the protection of electronic systems, communication networks, control

---

[38] Dr. M Gercke ‘Understanding cybercrime: phenomena, challenges and legal response’ *The ITU Publication*, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf , accessed on 28 May 2019 at 169.
[39] *Ibid.*
[40] *Ibid.*
[41] S Tully ‘Protecting Australian cyberspace: Are our international lawyers ready?’ (2012) 19 *Australian International Law Journal* 50.
[42] N Shactman ’26 Years after Gibson , Pentagon defines ‘cyberspace’ *WIRED* available at https://www.wired.com/2008/05/pentagon-define/ accessed on 22 May 2019.
[43] Tully (n 41 above) at 5.1
[44] Information technology is “the application of computers to process, transmit and store data, typically in a business or enterprise environment.” Available at https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf, accessed on 30 May 2018.
[45] Operational Technology is “hardware and software systems that monitor and control physical equipment and processes, often found in industries that manage critical infrastructure.” Available at https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf , accessed on 30 May 2018.
[46] Guidelines on Cyber Security on Board Ships, published by BIMCO (Version 1.1- February 2016).
[47] ‘Cyber-attack’ Merriam Webster, available *at* https://www.merriam-webster.com/dictionary/cyberattack, accessed on 11 November 2018.

algorithms, software[48], users and underlying data within the maritime infrastructure from malicious attacks, damage unauthorised access, or manipulation".[49] Another more comprehensive definition, put forward by Maskun, defines *cyber security* as:

1. "A set of activities and other measures intended to protect - from attacks, disruption or other threats - computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software data, as well as the other elements of cyberspace. The activities can include security audit, patch management, authentication procedures, access management, and so forth. They can involve for example, examining and evaluating the strength of vulnerabilities of the hardware and software used in the country's political and economic electronic infrastructure. They also involve detection and reaction to security events, mitigation of impacts and recovery of affected components. Other measures can include thing like software and hardware firewalls, physical security such as hardening facilities and personnel training and responsibilities;"[50]
2. "The state or quality of being protected from such threats";[51]
3. "The broad field of endeavour, including research and analysis, aimed at implementing and improving those activities and quality." [52]

Cyber security on board a ship protects "the operational technology against the unintended consequences of a cyber-incident; information and communications systems and the information contained therein from damage, unauthorised use or modification, or exploitation; and/or against interception of information when communicating and using the internet".[53]

A "cyber incident" is "an occurrence, which actually or potentially results in adverse consequences to an on-board system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences".[54]

---

[48] The *Merriam Webster online Dictionary* defines software as "the entire set of programs, procedures, and related documentation associated with a mechanical or electronic system and especially a computer system" available at https://www.merriam-webster.com/dictionary/software, accessed on 13 May 2019.
[49] Garcia-Perez (n 5 above).
[50] Maskun, 'Cyber security: rule of use internet safely' (2013) 15 *Journal of Law, Policy and Globalization* at 20.
[51] *Ibid.*
[52] *Ibid.*
[53] The BIMCO guidelines (n 46 above).
[54] *Ibid.*

It should be noted that definitions at to what cyber security threats and attacks are, are not universally agreed upon which makes regulations of these types of attacks increasingly difficult.

1.3. Research Problem

The prevalence of maritime cyber security incidents is increasing worldwide. Reports suggest that cybercrime amounts to more than $400 billion in annual costs to the global economy.[55] According to the Cisco Annual Security Report South Africa is one of the most targeted counties for cyber-crime, this is due in part to outdated organisational structures and practices. It has been reported that "South Africa lost approximately ZAR50 billion in 2014 due to cyber –incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015",[56] with these number expected to rise in the coming years. With the launch of the Smart Port Initiative, the port of Durban has an Integrated Port Management System,

> which is a holistic, web-based, end-to-end system that integrates Marine Operations, Systems and Reporting, on a single platform. This system provides users with access to a wide range of near real-time operational information- that is accessed centrally 24/7.[57]

With a goal of turning Durban port into a successful smart port, it will be in the government's best interest to ensure a proper cyber security platform is implemented as part of the foundation of the port.[58] In South Africa cybercrime accounts for 0.14% as a percentage of GDP.[59]

There are a number of inherent complexities and challenges to maritime cyber security. First, there are different categories of vessels (bulk carriers, break-bulk carriers, container ships, auto carriers, tankers, passenger ships etc.), all of which operate on different computer systems and are built to last a long time. Crew members often work with systems that they are unfamiliar with. According to Jensen, the maritime industry has a unique set of characteristics that make

---

[55] 'Cyber-Security Threats to the Maritime Industry' available at http://www.mile.org.za/QuickLinks/News/1st%20Annual%20Maritime%20Summit%20Presentations/Day%201.6-Carl%20Uys-Cyber%20Security%20Threats.pdf , accessed on 5 November 2018.

[56] B Van Niekerk ; An analysis of cyber incidents in South Africa' (2017) 20 *The African Journal of Information and Communication* at 114.

[57] "Port of Durban: The Busiest container port in sub-Saharan Africa' *Transnet* available at https://www.transnetnationalportsauthority.net/OurPorts/Durban/Documents/(TNPA)%20Durban%20Brochure.pdf , accessed on 29 April 2019 at 6.

[58] *Ibid.*

[59] 'Net losses: estimating the global cost of cybercrime. economic impact of cybercrime II' Center *for Strategic and International Studies* available at https://collabra.email/wp-content/uploads/2015/04/rp-economic-impact-cybercrime-2014.pdf , accessed on 6 November 2018 on page 20.

cyber defence difficult.[60] In generic shipping line operations, IT departments are often land based systems, whereas the IT systems on board a vessel are within the control and scope of the marine technical department on board that particular ship, who often have a limited understanding of the backend systems used or the technological infrastructure on board that ship.[61] Chartering of ships add to this challenge as the shipping line may not have full control of the crew on board the ship.[62] The fluctuating nature of the users of the IT systems on board a ship and the dynamic schedule that ships operate under often results in crew members being unfamiliar with the technology.[63] For example many ships do not change their passwords and default usernames, and because of this hackers can take advantage of this and remotely reconfigure a ship's Electronic Chart Display software (ECDIS),[64] which would allow hackers to change the receiver's GPS location, which could lead to a collision.[65]

Second, differing views and approaches existing to address the challenge and threats to maritime cyber security.[66] Currently regulators follow one of three approaches when considering cybersecurity. These approaches include the Technical Approach which "sees a problem as a technical challenge to be overcome… by developing new devices and or methods to respond quickly"[67] to cyber challenges. The Criminal Approach which consists of "formal legal regimes and strong widely understood domestic and international norms for reducing crime"[68]. The Warfare Approach "seeks to develop and apply military doctrine for threat deterrence and response".[69]

Lastly, the different conventions contain generic terms which are vague and do not give a clear indication as to how vessels are to be protected from cyber threats and how to protect the lives of the passengers and crew on board a vessel should a cyber-attack occur while the vessel is at sea. For example, in 1948 a Convention formally establishing the International Maritime

---

[60] L Jensen 'Challenges in maritime cyber-resilience' 2015 *Technology Innovation Management Review*, available at *https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=35* , accessed on 28 May 2019.
[61] *Ibid.*
[62] *Ibid.*
[63] K Martin and R Hopcraft 'Why 50,000 ships are so vulnerable to cyber attacks' *The Conversation* 14 June 2018, available at *https://phys.org/news/2018-06-ships-vulnerable-cyberattacks.html* , accessed on 28 May 2019.
[64] A computer –powered navigation system.
[65] L Kelion ' Ships hack 'risk chaos in English Channel' '*BBC News Online* 7 June 2018, available at https://www.bbc.com/news/technology-44397872 ,accessed on 19 February 2019.
[66] J Healey & H Pitts 'Applying international environmental legal norms to cyber statecraft' (2012) 8(2) *ISJLP* at 359.
[67] *Ibid* at 357.
[68] *Ibid* at 358.
[69] *Ibid* at 358.

Organisation[70] was adopted in and international conference in Geneva.[71] A key purpose of the IMO is…

> Article 1 (a) To provide machinery for co-operation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade, and to encourage the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships; and to deal with administrative and legal matters related to the purposes set out in this Article.[72]

In order to improve maritime cyber security and safety, the IMO is required to develop International treaties and foster mechanism for co-operation among governments in the development of their regulatory framework, so as to realise the purpose of its function. Technological advancements and computing technology is changing at an exponential rate,[73] the threats to cyber security will inevitably try to keep up with these advancements, the true challenges to maritime security will thus be whether regulations focused on cyber security change at the same pace. While the IMO has accepted that it has to play a fundamental role in "combating the growing menace that terrorism and other unlawful acts posed for the safety of international shipping,"[74] there has been no mention of the proposed way of combating the unlawful acts and in turn the enforcement strategies to be applied.

Both domestic law and international legal regimes have fallen short of regulating maritime cyber security. For example the "United Nations Convention on the Law of the Sea"[75] (herein after referred to as UNCLOS), does not explicitly provide for cyber security. This then means that nations that are signatories to this convention, would have to interpret other sections of the Convention that could apply to maritime cyber security, leaving room for misinterpretation or narrow approaches being followed to the detriment of one party. For example, Article 19 of

---

[70] The original name was the Inter-Governmental Maritime Consultative Organization, or IMCO, but the name was changed in 1982 to IMO.Resolution A.358 (ix), Adopted on 14 November 1975 available at *https://treaties.un.org/doc/source/docs/A_358_IX-E.pdf* accessed 22 May 2019.
[71] 'Brief history on the IMO' *http://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx* accessed on 4 November 2018.
[72] Convention on the International Maritime Organization, art. 1, *Mar. 6, 1948, 9 U.S.T. 621, 289 U.N.T.S. 48*. The Convention on the Inter-Governmental Maritime Consultative Organization Adopted by the United Nations Maritime Conference in Geneva on 6 March 1948.
[73] L Sturdevant, 'Cyber warfare and maritime security: A call for international regulation' in J DiRenzoIII… et al Issues in *Maritime Cyber Security* Washing DC: Westphalia Press, (2017) at 123.
[74] R Balkin 'The International Maritime Organisation and Maritime Security' (2006) 30(1&2) *Tulane Maritime Law Journal* 3.
[75]United Nations Convention on the Law of the Sea (10 December 1982) available at *https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf* accessed on 20 May 2019.

UNCLOS deals with the safe passage of vessels and Article 109 (a) of UNCLOS which deals with the suppression of unauthorised broadcasting from the high seas. Both these articles are wide enough to encompass unauthorised digital penetration of vessels at sea as well as attacks by hackers to a vessel at sea. “The International Ship and Port Facility Security Code”[76], further makes it mandatory for its signatories to take appropriate preventative measures against security threats. The Code falls short in that it does not set out what these steps are or even a minimum set of guideline to be followed. In South Africa, cyber security and maritime cyber security are largely unregulated. In order to prosecute a cyber-transgression one would have to rely on the “Electronic Communications and Transactions Act”[77] or the “Regulation of Interception of Communication and Provision of Communication-Related Information Act”.[78] Both of these do not have stringent prosecutorial remedies. No mention of specific technological requirements or capabilities or which entities are charged with reaction responsibilities are found in the Acts and conventions mentioned above. The Cybercrimes and Cyber Security Bill of 2002 sought to rectify this however the bill has not been enacted in the country. These conventions and South Africa’s domestic laws will be discussed in more detail in Chapter Three of this dissertation.

1.4. Research question

The questions to be answered in this dissertation are whether:

(i) the existing law applies to maritime cyber security threats, and, if so, what is the extent of the existing laws’ applicability to maritime cyber security threats?

(ii) the domestic and international legal framework is adequate, in respect to enforcement and comprehensiveness, in addressing/responding to maritime cyber security threats? and

(iii) it is necessary to establish new regulations to address maritime cyber security or develop existing laws?

---

[76] Code International Ship and Port Security Code, Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended.

[77] Electronic Communications and Transactions Act 25 of 2002.

[78] Regulation of Interception of Communication and Provision of Communication-Related Information Act 70 of 2002.

1.5. Key points from existing literature:

A M Matsyshyn, who has written extensively about cyber security and who challenges existing assumptions of the emerging legal area of cyber security, argues that the two main focuses of cybersecurity, namely information-sharing and deterrence,[79] which fail to acknowledge that national security concerns and corporate sharing cannot be separated. This problem is called "reciprocal security vulnerability".[80] The issue of reciprocal security vulnerability means that the security threats and vulnerabilities impacting the public sector impacts the private sector and likewise vulnerabilities in the private sector impact the public sector, the two are inextricably interwoven.[81] Therefore, "in practice our current legal paradigms channel us in suboptimal directions".[82] Matsyshyn emphasises three flaws that cause legal and policy dialogues on cyber security to be misframed. First, "questions of privacy are often conflated with questions of security". These questions according to Matsyshyn require different enquires. Legal scholars and policy makers often frame cyber security in the lens and as indistinguishably reliant on privacy law. Legal scholars who argue on this point, like Bambauer, put forward that "security merely implements privacy choices"[83] and that the prevention of cyber security breaches is futile and should rather be replaced with mitigating the effect of cyber threats after the ccurrence.[84] Secondly Matsyshyn argues, that technical barriers between policy makers and computer scientist, due to a deficiency in language, means that often the two parties misunderstand each other to the detriment of policy changes in a nation.[85] Lastly cyber security is not just cyber in its nature, often physical and digital security considerations have to be made.[86]

Foote advocates for a cyber a culture of cyber risk awareness and contends that it is "critical for all maritime partners to implement a culture of cyber risk awareness…that must be pervasive, reaching from the highest level of management to the workers at the most junior position".[87] Additionally governments should "work with industry to share information

[79] A M Matsyshyn 'CYBER' 2010 *BYU L. REV* at 1109.
[80] *Ibid* at 1121.
[81] *Ibid* at 1109.
[82] *Ibid* at 1109.
[83] D E Bambauer 'Ghost in the Network' (2014) 162 *U. PA. L. REV.*at 1012.
[84] *Ibid* at 1135-44.
[85] *Ibid* at 1146.
[86] *Ibid* at 1154.
[87] Foote, R 'Cybersecurity in the marine transportation sector: Protecting intellectual property to keep our ports, facilities and vessels safe from cyber threats' (2017) 8 Cybris Intell. Prop. L. Rev. at 264.

leverage current regulations to their full extent and create new regulations that specifically focus on cyber security”.[88]

The deep existing problems brought by cyber security threats lie in the complex nature of regulating the cyber threats as jurisdiction is difficult to establish and the outcomes of the cyber threats are global in nature with transnational repercussions. According to Cassim, the challenge facing cybercrime regulation lies in the fact that cybercrimes “can be easily committed, it requires few resources, and it can be committed in a specific jurisdiction without the offenders being physically present there”.[89] Cassim further provides that “domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world”.[90]

Sturdevant, puts forward that Academic papers such as the Tallinn Manual[91] on “International Law Applicable to Cyber Warfare”[92] are insufficient for regulation of cyber security, mainly because the international community might not be adequately equipped or even prepared to create international treaties regulate cyber security because the use of the internet is linked to privacy rights or the right to freedom of speech. [93]

Stahl importantly puts forward that cyber transgressions pose an unprecedented challenge to cyber security, thus “without an international agreement that defines the spectrum of cyber aggression, provides for some form of universal jurisdiction over perpetrators and establishes and international organization focused on cyber security policy, the threat to international security posed by cyber transgressions will continue to grow”.[94]

It is common cause the legal framework regulating maritime cyber security and maritime cybercrimes is not where it should be internationally, regionally and of importance to this body of work domestically.

---

[88] *Ibid.*
[89] F Cassim ‘Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role player” available at https://core.ac.uk/download/pdf/79170924.pdf accessed on 30 May 2019.
[90] F Cassim ‘Formulating specialized legislation to address the growing spectre of cyber-crime: A comparative study’ (2009) 12(4) PER at 66.
[91] Tallinn Manual on the International Law Applicable To Cyber Warfare, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence(2009).
[92] Sturdevant (n 73 above) at 119.
[93] *Ibid*.
[94] W M Stahl ‘The uncharted waters of cyber space: Applying the principles of the international maritime law to the problem of cyber ‘(2011) 40 (247) GA. J.INT’L & COMP.L. at 273.

1.6. Delimitations

It is necessary to set the parameters of this dissertation. The dissertation will not consider the measures and framework used by naval intelligence during times of war. The term cyber-attack is used here in a purely technical sense in a peace time scenario and not in the meaning of armed conflict.

1.7. Research methodology

This dissertation will be based on a doctrinal analysis of international and domestic legal principles, legislation and policies

This dissertation will be based on a desktop/black letter review of the relevant legal materials. This analysis will be performed through utilising documentary sources such as media articles, reports, practice and policy guides, reviews, journal articles and statistical data.

1.8. Structure of the dissertation

This dissertation undertakes a critical analysis of the legal framework governing maritime cyber security and the effectiveness in combating maritime cyber threats. Having provided an introduction and background to maritime cyber security in this chapter, the second chapter focuses on the different threats and vulnerabilities to maritime cyber security. In addition to this reference will be made to the types of cybercrimes and their possible ramifications. The third chapter will analyse the international regulatory regimes in place, regional regulatory framework and South Africa’s domestic laws regulating maritime cyber security. In the fourth Chapter a determination will be made as to the existence and adequacy of the law in combating maritime cyber threats and crimes. A conclusion will be derived from the findings of this dissertation, and recommendation will be submitted.

CHAPTER 2:

VULNERABILITIES AND THREATS TO MARITIME CYBER SECURITY

2.1. Maritime cybersecurity threats:

The increase in connectivity in the maritime industry had dramatically changed the way that business in the maritime industry is conducted. It is clear that it is in the best interest of the maritime community to develop a comprehensive and multilateral cyber security legal framework, as the widespread use of the internet in every aspect of daily life has created an almost “irreversible dependence” on technology.[95] It is therefore essential to identify these threats. Threats in the shipping industry can vary. They can either be intentional or unintentional (accidental) and also “targeted at a specific company, ship or fleet or untargeted (shotgun approach)”.[96] A number of maritime cyber security threats are discussed in the following paragraphs.

2.1.1. Malware

Malware, is the abbreviated form for “malicious software” and is a term that comprehensively covers a variety of malicious forms of computer software.[97] This includes computer viruses, Trojan horses and worms or any type of malicious code.[98] Malware often infects the computer to and emails or websites that have been modified to carry out functions that they were not originally intended for.[99] Malware is intended to “steal data from a computer an exploit any known deficiencies and problems of the network”.[100] Characterisation of software as malware is based on the intention of the person creating the software than the features the software contains.

[95]*Ibid* at 249.
[96] S Langouvardou ‘Maritime *Cyber Security: Concepts, Problems and Models’* (Master’s Thesis, Technical University of Denmark, 2018).
[97] McNicholas (n 2 above) at 377.
[98] McNicholas (n 2 above) at 377.
[99] D Weissbrodt ‘Cyber Conflict, Cyber Crime and Cyber Espionage’ (2013) 22 (2*) Minnesota Journal of International Law* at 355.
[100] Langouvardou (note 96 above).

In 2010 cybercriminals were becoming more organised and began utilising more sophisticated coders and programmers to hide their malware.[101] Because this gave the cybercriminals more time to conduct their illegal activities, the frequency and extent of these types of attacks grew and cybercriminals were becoming bolder in their attacks.[102]

2.1.1.1. Virus

A virus is similar to a biological virus. A virus is a "program that modifies other computer programs, causing them to perform the task for which the virus was intended."[103] A computer virus can be spread though sharing files or data via email, over the internet using company networks (intranet) or by disk.[104]

2.1.1.2. Trojan Horse

Trojan horses are programs that have a legitimate function, but simultaneously contain a hidden malicious code, which tricks a user into installing or running a seemingly harmless programme.[105] Once this is done the perpetrator releases and activates the hidden code, which activates a virus or enables a person to get unauthorised access into a particular system. [106]

2.1.1.3. Logic bombs

Logic bombs are instructions coded onto a program "which trigger a function at some later stage pursuant to which disruption or harm can be caused to the computer or its data."[107]

2.1.1.4. Worms

A worm is a program that uses the computer networks or the internet to create copies of itself.[108] Whereas viruses need human action to replicate and spread between different computer, worms

---

[101] A Minnaar 'Organised crime and the 'new more sophisticated 'criminals within the cybercrime environment: How 'organised ' are they in the traditional sense?' (2016) 29 (2) *Acta Criminologica: Southern African Journal of Criminology* at 130.

[102] *Ibid.*

[103] J L McCurdy 'Computer crimes' (2010) 47 (287) *African Criminal Law Review* at 291.

[104] *Ibid.*

[105] P J Denning 'Computer Viruses' (21 March 1988) Research Institute for Advanced Computer Science available at *https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890017050.pdf* accessed on 29 April 2019.

[106] *Ibid.*

[107] D M Reimer 'Judicial and legislative responses to computer crimes' 1LAN986 *Insurance Counsel Journal* 408.

[108] McCurdy (n 103 above) at 291..

can "modify and delete files and even eject additional malware into the computer"[109] on their own.

2.1.2. Ransomware

Ransomware is a type of malware where by a computer is infected or functions of a computer are specifically disabled with the intention of leveraging the attack on the computer, for payment of a ransom. [110]

2.1.3. Spyware

Spyware is a form of malware that, once installed a computer monitors the user's activities. This is usually done without the user's knowledge.[111] Spyware can gather a variety of information including emailing information, user names and passwords and even track every keystroke of the web activity of the user.[112]

2.1.4. Social Engineering

In modern day businesses including in the maritime environment, "people interact extensively with computer systems, whether that be the ship's navigation system a drilling rig or a ballistic missile system".[113] Good information technology security is never solely based on protecting a company or government institution from the theft of the physical machine. Human vulnerability through manipulation and threat are always key aspects of cyber and information security.[114] Social engineering is the tem used when cyber attackers exploit the fragilities of human behaviour to gain access to and organisation's systems or the virtual premises of that organisation.[115] In this way the social engineers manipulate insider individuals to become a conduit between the attacker (cyber attacker) and the computer system they want to attack.[116] This type of attack on maritime platforms and maritime infrastructure is normally conducted

[109] Langouvardou (note 96 above).
[110] P R DeMuro 'Keeping internet pirates at bay: Ransomware negotiation on the health industry (2017) 14 *Nova Law Review* at 352.
[111] D B Garrie; A F Blakley; M J Armstrong 'Legal status of Spyware' (2006) 59 *Federal Communications Law Journal* at 160.
[112] *Ibid* at 161.
[113] O Fitton…et al 'The future of maritime cyber Security' (2015) available at *http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf* , accessed on 2 November 2018.
[114] Matsyshyn (n 79 above) at 1156.
[115] J Parms '10 Common social engineering tactics used by attackers' 22 February 2015 available at https://www.business.com/articles/10-common-social-engineering-tactics-used-by-attackers/ ,accessed on 11 November 2018.
[116] Langouvardou (note 96 above).

when the attack manipulate employs and former employees, who usually have a sophisticated understanding of the company's computer systems, into uploading malicious software on the computers. Social engineering is usually the first point of accesses in launching cyber malicious software on an organisation.[117] Through social engineering hackers often gain access to their targets credentials or access to the physical machine to launch malware such as viruses or worms.[118] Employees of companies and former employees have managed to successfully launch malicious software, and employ in extortionate acts on the company or steal the company's trade secret among other crimes.[119]

2.1.5. Phishing

In the past decade online cyber attacks have increased in severity and regularity, partly due to the difficulty in identifying cybercriminals and perpetrators, making cybercrime one of the fastest growing crimes in the world.[120] Phishing refers to "the act of sending an e-mail to a user falsely claiming a legitimate bank, organisation or company with the intention to coax the user into surrendering private information about him or her or his or her company".[121] Thus phishing schemes "utilise pretext emails…where the phishers pose as a trusted entity such as a financial institution, an Internet Service Provider (ISP) or a government agency".[122] Phishing is usually directed at a group of people in the hopes that one or some of them will fall prey to the trap. Although phishing emails are widely used, they can only pose a threat if they are opened.[123]

2.1.5.1. Spear phishing

Spear phishing is a method, whereby hacker or cyber criminals target a specific user who has access privileges in a particular company or organisation.[124] The targeted nature of spear phishing means that perpetrators must have prior knowledge of the target user or victim.

---

[117] *Ibid.*
[118] L Ablon 'Social engineering explained: The human element in cyber attacks' 20 October 2015 available at *https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html*, accessed on 11 November 2018.
[119] D W Yang and B M Hoffstadt 'Countering the cyber-crime threat' (2006) 43 (201) *American Criminal Law Review* 205.
[120] F Cassim 'Addressing the spectre of phishing: Are adequate measures in place to protect victims from fishing' (2014) 41 *Comparative and International Journal of South Africa* 406.
[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] I Kilovaty 'World Wide Web of exploitations- The case of peacetime cyber espionage operations under international law: Towards a contextual approach' (2016) 18 *The Columbia Science and Technology Law Review* 50.

2.1.6. Water holing

The name of this type of cyber attack was inspired by the wild, whereby predators would lurk around the water hole waiting for unsuspecting prey. Water holing refers to an attack "in which the attacker seeks to compromise a specific group of end users by infecting websites that member of the group are known to visit". [125] Water holing attacks are often untargeted and intentional. [126] Cybercriminals often infect a popular site with malware that is automatically loaded when an individual visit that site.[127]

2.1.7. Distributed Denial of Services

Regulating the cyber world in the legal sense is very difficult, mainly because cyber-attacks such as Distributed denial of service (DDOS) are carried out in a manner that makes it very difficult to identify the perpetrator. This makes these types of cybercrimes, extremely attractive for cyber criminals, as liability is difficult to prove. Denial of services refers to "an attack that seeks to disable the target so that it no longer is able to offer the services it normally provides".[128] According to the United States Computer Emergency Readiness Team (US-CERT) [129] a denial of services attack (DoS) "attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor".[130] The server is generally "sent a large volume of communications traffic that overwhelms it and causes it to crash".[131] On the other hand Distributed denial of service (DDoS) "occurs when multiple machines are operating together to attack one target"[132] The services that may be affected include websites, online accounts, email or other services that rely on the server network or the computer. The attack makes use of many other computer that have been previously infected by malware referred to as

[125] 'Watering hole attack' available at https://searchsecurity.techtarget.com/definition/watering-hole-attack, accessed on 11 November 2018.
[126]Langouvardou (note 96 above).
[127] *Ibid.*
[128] *Ibid.*
[129] Which is part of the United States of America's Homeland Security is the successor entity to a variety of previous organisations such as the Federal Computer Incident Response Center (FCIRC) and the National; Infrastructure Protection Center. This information security organisation has responsibility for publishing timely security information such as advisories, technical bulletins and vulnerabilities notes in addition to more general awareness and educational materials.
[130] 'Understanding Denial of Service Attacks' United States Computer Emergency Readiness Team (US-CERT) available at *https://www.us-cert.gov/ncas/tips/ST04-015* , accessed on 12 November 2018.
[131] J A Chandler 'Security in cyberspace: Combating distributed denial of services attacks' 2003-2004 *University of Ottawa law and Technology Journal* 236.
[132] US-CERT (n 130 above).

"zombies".[133] A distributed denial of services involves remotely instructing large networks of these "zombie" machines to attack a targeted site simultaneously,[134] these Zombie PC networks are called bonnets. Because many of these zombie PCs seek access on to a particular server at the same time, it becomes very difficult to distinguish malicious access by a zombie PC and a legitimate one.[135]

2.1.8. Port Scanning

A computer uses some of its 65 536 Transmission Control Protocol ports for internet and email purposes.[136] These ports are means by which information passes to and from a computer, thus a port is a communication channel.[137] The use of port scanning techniques enables a person to:

1. Examine (also called probing) the services a computer us running. Port scanning can indicate particular characteristics of the target computer such as (a) what type of operating system the computer is using, and (b) what type of security software (known as firewalls) it is using; and to
2. Reveal exploitable weaknesses in a computer's security without exploiting theses weaknesses.[138]

Perpetrators of cybercrime can use port scanning software to scan for vulnerabilities in the computer network, to determine which malware or other cyber threat will work in gaining entry into the network, or damage the network. Port scanning is often used as a precursor to other forms of cyber-attacks.

2.1.9. Website defacement

This form of cyber attack is often used by hacktivist, who seek to get a message or their point of view through. Cyber defacement is conducted through a hack of an organisations or an individual's website, whereby an unauthorised post in the form of a text message or graphic is uploaded on the site. The most used form of defacement is through SQL[139]injections used to

---

133 *Ibid.*

134 L Edwards 'Dawn of the death of distributed denial of services: How to kill zombies' (2006) 24 (23) *Cardozo Arts and Entertainment Law Journal* at 23.

135M Tsuchiya 'Japan's response to cyber threats in the surveillance age' (2015-2016) 7 *Section Hall Journal of Diplomacy and international Relations* 9.

136 E J Ebersohn 'Internet law: Port scanning and ping flooding- a legal perspective' (2003) 66 Journal for Contemporary Roman Dutch law THTHR 563

137 *Ibid.*

138 *Ibid.*

139 SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for streaming processing in a relational data stream management system.

log on to an administrators accounts.[140] The message is one that criticises the site, a particular individual or an organisation.[141] The extent to what a website defacement can occur varies. The hacker could attack one site, or potentially hundreds or thousands of sites. It is worth noting that while website defacement can vary as to the number of sites attacked/hacked, the defacement of websites does not necessarily damage the targeted site, but hijacks the site to convey their message, text or graphic.[142] This, while not causing substantial harm, often provides the attacker with some symbolic fulfilment.

2.1.10. Subverting the supply chain

Due to the real time connectivity facilitated by a technology based maritime industry, this type of attack is tremendously popular in the maritime sector. An ICT supply chain compromise is defined as

> An occurrence within the ICT supply chain whereby an adversary jeopardises the confidentiality, integrity or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the production or service.[143]

Subverting the supply chain consists of attacking a company or ship, whereby software, equipment or supporting services being delivered to the ship or company are compromised.[144]

[140] 'Website defacement' Cybercrime.org.za available at http://cybercrime.org.za/website-defacement accessed on 15 November 2018.
[141] G O'Malley 'Hacktivism: Cyber activism or cybercrime' (2013) 16 *Trinity College Law Review* at 143.
[142] N C N Hampson 'Hactivism: A new breed of protest in a networked world' (2012) 35(2) Boston *College International and Comparative law Review* at 519.
[143] J Boyens… et al 'Supply chain risk management practices for federal information systems and organisations' (2015) NIST Special Publication available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 161.pdf accessed on 20 November 2018 800-161.
[144] Langouvardou (note 96 above).

2.2. Incidents of maritime cyber attacks

Incidents of maritime cyber attacks have become very prevalent in recent years.

2.2.1. Deleting carrier information as to the location of cargo

Cargo is undoubtedly one of the most valuable components in the shipping industry supply chain and enables goods, such as food, clothing and machinery, to be transported from one area to another.[145] The smuggling of cargo consists of bringing prohibited goods into a country or stealing merchandise for which duty has not been paid.[146] The cargo supply chain is thus susceptible to illegal and unauthorised access by criminals and terrorist groups. Because of the key role that cargo plays in international trade we will now examine the cyber threats to cargo shipping.[147]

In August 2011 the state owned Islamic Republic of Iran Shipping Lines (hereafter referred to as IRISL) was the target of a malicious cyber attack.[148] The IRISL lost all data relating to their rates, loading, and cargo number date and place and eliminated the company's internal communication network, leading to cargo simply disappearing, while other cargo was sent to the wrong destination. This had devastating financial consequences for the shipping liner.[149]

2.2.2. Barcode scanners used as hacking devices

This type of cyber attack consists of an attack hidden within a piece of hardware.[150] The cyber threat was malware that was preloaded in a newly manufactured scanner, which compromised at least eight logistics and shipping companies. "When the scanners were plugged into the company's network it launched a series of automated attacks searching the company network for the ERP financial server".[151] Once this process had been completed the company's network would be compromised, opening the network to a remote connection by the attackers, who would then have access into the financial system and the ability to modify the shipping database

---

145 D Gliha 'Maritime cyber crime-21st Century piracy' (2017) 20 Annals Fac. L.U. Zenica at 231.
146 *Ibid.*
147 McNicholas (n 2 above) at 131.
148 Y Torbati and J Saul 'Iran's top cargo shipping line says sanctions damage mounting' *Reuters* (22 October 2012) available at *https://www.reuters.com/article/us-iran-sanctions-shipping/irans-top-cargo-shipping-line-says-sanctions-damage-mounting-idUSBRE89L10X20121022* , accessed on 16 November 2018.
149 Gliha (n above 145) at 230.
150 CyberKeel, 'Maritime cyber security: Virtual Pirates at large on the cyber seas' (2014),available at *https://docplayer.net/19421672-Maritime-cyber-risks-virtual-pirates-at-large-on-the-cyber-seas-10-15-2014.htm,l* accessed on 17 November 2018.
151 *Ibid.*

and thereby tapering with the location of packages.[152] The accesses provided to the attackers by the weaponised malware meant that the attackers could circumvent most of the company's security measures and have near complete control of the enterprise perimeter.[153] This form of hardware attack has been termed 'Zombie Zero'. TrapX labs discovered this form of attack in 2014. According to a TrapX report, the attacks appeared to originate from a location near Lanxiang University in China, however tracing the source of the attack is very difficult as sophisticated methods are being used to remove the coders "signature" and hide the true origin of the attack.[154]

2.2.3. "*Icefog*"|

In 2013, information pertaining to a form of attacked dubbed "*Icefog*", was released by security company Kaspersky.[155] The aim of the attack was to provide the cyber perpetrator with backdoor access into a targeted company or organisations, in order to extract data, documents, email accounts and passwords as well as gain access to the resources within the company's or organisation's network.[156] The attacks were mainly aimed at Korean and Japanese targets, covering a range of business sectors, including the shipbuilding and maritime sector.[157] "*Icefog*" attacks utilise spear-fishing attacks to attempt to trick a victim into opening malicious emails or websites. There after the cyber perpetrator has access to the victim's data and can initiate lateral movement tolls to steal or modify data.[158] According to Kaspersky, "the attackers masked their backdoor entry using Fucobha:"[159]

> The "*Icefog*" backdoor set (also known as Fucobha) is an interactive espionage tool that is directly controlled by the attackers. There are versions for both Microsoft Word and Mac iOS X.

Unlike many forms of cyber-attacks were the aim is to maintain access into a network over extended period of time, *"Icefog*" attacks are focused and the malware often expires in a short

---

152 *Ibid.*
153 Gliha (n above 145) at 231.
154 'Anonymity of a of an attack: Zombie zero' *TrapX Research Labs* (1 March 2017) , available at *http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf* ,accessed on 17 November 2018.
155 The '*icefog*' Apt :A tale of cloak and three daggers' Kaspersky Lab Global Research and Analysis Team 2013 available at https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf accessed on 17 November 2018.
156 CyberKeel (n 150 above).
157 *Ibid.*
158 *Ibid.*
159 *Ibid.*

period of time. "*Icefog*" does not infiltrate data; the operators perform actions directly on the victims live system instead.[160]

2.2.4. Ghost shipping

In 2011 an organised crime group, consisting of drug smugglers enlisted the assistance of Belgian hackers, infiltrated the computerised tracking systems in the port of Antwerp, to gain access to container location and security details.[161] The Belgian hackers were able to gain access to management systems within two piers in the port.[162]The group was able to identify which containers had a consignment of drugs hidden in them and were later able drive away from the port, retrieve the consignment of drugs by producing false bills of lading then taking custody of the container, all while being undetected. This happened for a period of two years.[163] Once the breach in the ports management systems had been identified, the port installed firewalls. However, the hackers physically penetrated the port and installed "wireless bridges on the operating computers, which allowed them direct access to the operating system".[164] Ghost shipping is therefore the term coined to describe thus type of cyber invasion of the cargo management systems. When the authorities were alerted, a raid on the groups hide-out uncovered hacking devices, drugs, €1.3 million in cash, and firearms.[165]

A similar attack was discovered in Australia in 2012. The cargo system controlled by the Australian Customs and Border Protection Service Agency was compromised by a group of hackers who worked for a criminal syndicate. The penetration of the cargo systems "allowed criminals to check whether the shipping containers were regarded as suspicious by police or customs authorities"[166]. As a result of having access to this information the criminals would either abandoned the shipping container containing contraband items, if they felt that the authorities were suspicious of it, or retrieve the containers that were not deemed suspicious. [167]

---

[160] *Ibid.*
[161] Gliha (n above 145) at 232.
[162] *Ibid.*
[163] 'The risk of cyber-attack to the maritime sector' *Marsh and McLennan Companies(* July 2014), available at https://www.ahcusa.org/uploads/2/1/9/8/21985670/the_risk_of_cyber-attack_to_the_maritime_sector-07-2014.pdf , accessed on 17 November 2018 at 2.
[164] Gliha (n above 145) at 233.
[165] C R Hayes *Maritime Cyber Security: The future of National Security* (Master's thesis, Naval Postgraduate School, 2016) 16
[166] CyberKeel (n 150 above) at 8.
[167] *Ibid.*

2.3. Defining maritime cyber security threat perpetrators

While it is important to consider the security measure and legal framework that is in place in combating maritime cyber security, a holistic review of the security measures in place would not be complete without identifying the perpetrators of maritime cybercrimes and the key traits which must be considered when exploring the threat role that these perpetrators play in the malicious use of computer systems. It is thus prudent to identify these actors and what their roles are.

Malicious actors can cause disruptions to shipping vessels, as well to the timely functioning of ports. In the past the key players in cybercrimes has been limited to individuals who have an in depth knowledge of computer systems and "mastery of computer languages, computer programming, or network architect".[168] The reality in the status quo is very different. The growing number of people with access to knowledge of how computer systems work, through integration of information technology in their personal and business lives, has increased the number of potential cybercrime perpetrators.[169] The access to this information is also widely available on the internet which also increases the number of potential cyber criminals or perpetrators. Social engineering attacks have been used by criminal and political organisations for their personal gain or to put through a certain view.[170] Although cybercrime perpetrators take many different forms "they seek to exploit vulnerabilities created by the design to implementation of hardware, software, protocols and networks to achieve a wide range of political or economic effects".[171]

2.3.1. Individuals

2.3.1.1. Insiders (Employees and ex-employees)

Individuals within a company are often familiar with the company's computer networks and the intellectual property assets stores within a company. This makes it easier for them to act in a malicious manner when they are disgruntled. [172] An insider threat can be defined as "a current or former employee, contractor or business partner who: has or had authorised access to an organisation's network, system or data can bypass existing physical and electronic security

---

[168] Yang and Hoffstadt (n 119 above) at 204.
[169] *Ibid.*
[170] Fitton (n 113 above).
[171] 'National Strategy to secure cyberspace' (2013) Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program, available at *https://www-heinonline-org.ukzn.idm.oclc.org/HOL/Page?public=true&handle=hein.beal/nastsecyb0001&div=10&start_page=27&collection=beal&set_as_cursor=31&men_tab=srchresults* ,accessed on 18 November 2018.
[172] Yang and Hoffstadt (n 119 above) at 205.

measures through legitimate measures".[173] There are many reason that could potentially motivate insiders to carry out a cyber attack on a company or organisation, these include "greed, financial gain, and anger at employer or dissatisfaction at work, blackmail, and ideology or split loyalty". [174]

One of the most famous, or infamous depending on which side of the coin one falls under, insiders to highlight the threat of insiders in cyber security is Edward Snowden. In 2012 and 2013 Edward Snowden leaked classified documents, relating the National Security Agency's spying program, to journalist from the Guardian and the Washington Post. Intelligence sources reported that Snowden did not use any sophisticated software or device, but rather used thumb drives to explicit vulnerabilities in the NSA's outdated security system that gave him access to the NSA's sever and remove approximately 20 000 documents without ever being detected. [175] Snowden developed his skill and talent in computer and technology through online forums and friends, on his own accord.[176] He was hired by the CIA as a computer systems administrator and was given top secret clearance. [177]

2.3.1.2. Criminals

Criminal networks often do not possess any technical knowledge, and are typically looking for financial gains to support their illicit criminal activities.[178] These individuals or groups are usually already active in the maritime sector through various means including vessel high jacking, theft in cargo, drug smuggling etc.[179] Cyber criminals is possession of technical can choose to work on their own or to work for other crime syndicates.

2.3.1.3. Non-malicious individuals

People seeking no harm or material gains may also compromise the computer network systems of a company or port. This happens when tech savvy individuals or experimenters gain access

---

[173] C R Hayes Maritime Cyber Security: The future of National Security (Master's thesis, Naval Postgraduate School, 2016).

[174] 'Consequences to seaport operations from malicious cyber activity' *Home Land Security National Protection and Programs Directorate* (3 March 2016), available at *https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf* , accessed on 17 November 2018.

[175] 'Who is Edward Snowden, the man who spilled the NSA's secrets?' NBC New online 31 May 2014 available at *https://www.nbcnews.com/feature/edward-snowden-interview/who-edward-snowden-man-who-spilled-nsas-secrets-n114861* , accessed on 18 November 2018.

[176] *Ibid*.

[177] *Ibid*.

[178] Gliha (n above 145) at 230.

[179] CyberKeel, 'Maritime cyber security: Virtual Pirates at large on the cyber seas' (2014), available at https://docplayer.net/19421672-Maritime-cyber-risks-virtual-pirates-at-large-on-the-cyber-seas-10-15- 20

to a network system without the permission or knowledge of the owner which may cause accidental damage.[180] Human error, caused by negligence or lack of knowledge of certain technical upgrades, by outsourced individuals on a ship could also lead to a breach in computer network systems.[181]

2.3.2. Terrorists

Though not the focus of this dissertation, cyber terrorism is well worth discussing in greater degree. The threat of cyber terrorism is certainly a major concern to all nations, this largely due to the fact that it offers the attacker a degree of anonymity, unlike any other form of terrorist threat in the world.[182] The ever changing nature of ICT systems in the maritime field also makes maritime cyber security very difficult to legally regulate, even though cyber terrorist attacks have been occurring for decades.[183] From the inception of the United Nations, safety and security has always been at the forefront, with Article One stating that the purpose and principle of the United Nations is[184]:

> To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and international disputes or situations which might lead to a breach of the peace.

Considering the above, all states should have regulatory measures in place to regulate maritime cyber terrorism as this would be an integral part of maintaining international peace and security.

There is no universally accepted definition of cyber terrorism, and current definitions range from narrow definitions to broader definitions.[185]Although cyber terrorism is often referred to as a terrorist attack conducted in the cyberspace dominion, a formal definition by the Center for Strategic and International Studies (CSIS), defines “Cyber terrorism as the use of computer

---

180 *Ibid.*
181 *Ibid.*
182 *Ibid.*
183 *Ibid.*
184 Charter of the United Nations and Statute of the International Court of Justice (1945) available at https://treaties.un.org/doc/publication/ctc/uncharter.pdf, accessed on 12 November 2018.
185 J Brickey ‘Defining cyberterrorisim: capturing a broad range of activities in cyber space’ *Center for Security Studies* 2 October 2018, available on http://www.css.ethz.ch/en/services/digital-library/articles/article.html/153108/pdf , accessed on 20 November 2018.

network tools to shut down critical national infrastructures (e.g. energy, transportation, government operations) or to coerce or intimidate a government or civilian population".[186] According to Tafoya, cyber terrorism is "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information".[187] Cyber terrorist are therefore non-state actors who directly participate on hostilities in support of terrorist groups such al-Qaeda, ISIS and the Taliban, by using cyber network assets or carrying out their attack in the cyber domain.[188] The definition put forward by the Federal Bureau of Investigation (FBI): "cyber terrorism is the premeditated, publically motivated attack against information, information systems computer programmes and data, resulting in violence against non-combatant targets by sub-national groups or clandestine agents".[189]

All economic domains are controlled to a high degree by electronic networks, these include, the banking and financial sector, air traffic control, Geographic Positioning Systems (GPS) in the transportation industry etc., the objective of cyber terrorism is thus to alter or destroy information of strategic value through these terrorist attacks.[190] It is clear from the above definitions that while there is no universally accepted definition of cyber terrorism, for an attack to qualify as cyber terrorism it has to be a deliberate attack, which leads to violence against property of persons, or generate fear, with the perpetrators have some form of terror group allegiance.[191]

One of the biggest areas of vulnerabilities in maritime security, and especially to port security, is containerised shipments.[192] World seaborne trade amounted to 10.3 billion tons in 2016.[193] According to Transnet Port Terminals[194] 2018 Report the expected number of containers entering South African Port is set to be 4.5 million TEUs.[195] Richard Mallabone of the South

---

[186] A V Schmidt 'Cyberterrorism: Combating the aviation Industry's vulnerability to cyber-attack' (2016) 39(1) *Suffolk Transnational Law Review* at 172.
[187] W L Tafoya 'Cyber Terror' (2011) 1 *FBI Law Enforcement Bulletin* at 2.
[188] A C Goode 'Cyberterorists : The identification and classification of non-state actors who engage in cyber hostilities' 2015 (223) *Military Law Review* at 160.
[189] D Besliu 'Cyber Terrorism- A growing threat in the field of cyber security' (2017) 6(2) *International Journal of Information Security and Cybercrime* at 37.
[190] *Ibid.*
[191] *Ibid.*
[192] *Ibid.*
[193] UNCTAD Handbook of Statistics 2017- Maritime transport, available at *https://unctad.org/en/PublicationChapters/tdstat42_FS13_en.pdf*, accessed on 20 November 2018.
[194] The National Ports Act, No 12 of 2005 (Ports Act) is the enabling legislation for Transnet Port Terminals and promulgates the parameters within which terminals operate in South Africa
[195] Transnet Port terminals Report 2018, available at *https://www.transnet.net/InvestorRelations/AR2018/TPT.pdf*, accessed on 21 November 2018.

African Association of Freight Forwarders (Saaff) reported that South Africa has never been able to report to the government on reliable container inspection in South Africa, as there has never been a database containing those statistics.[196] Mallabone stated that currently manual manifests were used to manage the inspection of containers, which includes the South African Police Service (SAPS) stopping container at random or stopping containers based on the description that is provided on the container. These obstacles are heightened by the fact the South African Revenue Services (SARS) has a technology database in place containing valuable information about shipping containers, but will not share this information with SAPS.[197] This inability to efficiently and effectively inspect the goods that are potentially being transported into the country leaves South Africa particularly vulnerable to terrorist using shipping containers transport weapons of mass destruction or use cyber vulnerabilities in the computer networks to conceal the shipment of weapons or to conceal terrorist themselves as stowaways.[198] In October 2001 a suspected al-Qaeda terrorist was found in a container, on board a commercial container vessel, which was destined for Halifax in Canada from Gioia Tauro, a southern Italian port.[199] The container was fitted with a toilet, bed and food. The suspected Egyptian al-Qaeda terrorist, had in his possession a cellular phone, laptop computer and a satellite telephone as well as forged identity documentation.[200] This illustrates that the porous nature of container shipments to maritime cyber terrorism should be an area of great concern to legal minds and legislators of all states and more so for a country like South Africa which has the two biggest ports in Africa.[201]

---

[196] 'Saaff develops container inspection database' *Freight &Trading Weekly* (7 July 2017) (no.2253), available at *http://storage.news.nowmedia.co.za/medialibrary/Feature/6319/FTW-7-July-2017.pdf*, accessed on 21 November 2018.
[197] *Ibid.*
[198] A stowaway is a person who hides abroad a ship, airplane, etc to get free passage, evade port officials. Webster's *New World College Dictionary*, 4th Edition 2010 by Houghton Mifflin Harcourt.
[199] 'When trade and security clash' *The Economist (*4 April 2002), available at *https://www.economist.com/special-report/2002/04/04/when-trade-and-security-clash*, accessed on 22 November 2018.
[200] McNicholas (n 2 above) at 252.
[201] The Durban port (also known as Durban Harbour) has 59 beths making it one of the largest cargo ports in Southern Africa. According to statistics from Transnet National Ports Authority Cargo, a South African government organisation, in 2017 the port catered for 9,821 vessels and processed 22,785,7619 metric tons of cargo. It is rated number one in PwC's hub attractiveness list for the continent. The port of Richards Bay, which is located approximately 60 kms away from Durban is the main coal export terminal internationally, managing approximately 1.3 billion tonnes of coal up to date . Available *on* *https://www.ship-technology.com/features/emerging-ports-africa/* , accessed on 22 November 2018.

2.3.3. Hacktivist

Hacktivism is a worldwide phenomenon that is increasingly becoming a "popular form of protest".[202] Social activism[203] has been utilised by different groups and people for many years, with the increased reliance on technology and the world as a whole become more interconnected, it is therefore not surprising that this form of social activism is being used more often. The right to freedom of expression[204] is the legal structure offered in many jurisdiction including South Africa[205], that supports civil disobedience and legitimate protect action. Hacktivism has been defined as "the nonviolent use of 'illegal or legally ambiguous digital tools' like website defacement, information theft, website parodies, DoS attacks, virtual sit-ins and virtual sabotage, motivated not by personal or individual gains but by larger social, moral or political agenda."[206] Hacktivist are individuals engaging in similar forms of disruptive activities, to "highlight a political or social case".[207] Hacktivist believe that information should not be restricted and that it is the right of all individuals to have access to that information.[208] One of the most well-known hacktivist group is "Anonymous". The group has made many mainstream media headlines, their most prominent one, being the campaign in January 2008 against the Church of Scientology. The Church of Scientology had attempted to suppress the publication of information regarding the church by internet media outlets.[209] The magnitude of the campaign saw more than 6000 participants of Anonymous's operation dubbed "Project Chanology" protest in 90 city streets all over the world wearing the group's signature Guy Fawke's masks.[210]

---

[202] Social activism is defined as an intentional action with the goal of bringing about social change. Amherst College , at https://www.amherst.edu/campuslife/careers/amherst-careers-in/government-nonprofit/picareers/careers/social_activism, accessed on 25 November 2018

[203] *Ibid.*

[204] The right to freedom of expression is entrenched Article 19 of the International Convention on Civil and Political Rights (1976), which is ratified by South Africa and is also protected in the Universal Declaration of Human Rights (1948) in Article 19.

[205] The Constitution of the Republic of South Africa, 1996 Section 16 (1) states:

(1) "Everyone has the right to freedom of expression, which includes:
   (a) freedom of press and other media;
   (b) freedom to receive or impart information or ideas;
   (c) freedom of artistic creativity; and
   (d) academic freedom and freedom of scientific research."

[206] Hampson (n 142 above) at 514.

[207] O'Malley (n 141 above) at 140.

[208] A T Illig 'Computer age protesting: Why hacktivism is a viable option for modern social activists' (2015) 119(4) *Penn State Law Review* at 1036.

[209] B B Kelly 'Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cyber reform (2012) 92 (1663) *Boston University Law Review* 1678.

[210] *Ibid* at 1679.

The most contentious issue surrounding hacktivism, the discussion of which is important for completeness of any discussion pertaining to hacktivism, is the matter of whether cyber hacktivism should be classified as a legitimate, legal form of socio-political public protest or a cybercrime necessitating harsh legal action?

In recent years, especially in the United States of America, there has been a move to characterise hacktivist as people to be feared rather than socio-political activist.[211] The dawn of a new technology era means activism will not only be limited to real life, physical demonstrations, but that cyber activism or hacktivism will also play a role protest action and civil disobedience.[212] The "United States of America's Computer Fraud and Abuse Act (CFAA)"[213] was codified by Congress to regulate a variety of computer crimes in 1984. Amongst other things the CFAA criminalised the intentional accessing of a computer without authorisation.[214] The indictment of Aaron Hillel Swartz brought the focus of the wide cast net of the acts criminalised by the CFAA. Swartz was an American computer programmer, whose work focused on civic awareness and activism.[215] Swartz was arrested in 2011 after he connected a computer to the "Massachusetts Institute of Technology (MIT)" network, in and undisclosed closet, and systematically downloaded approximately 4.8 million academic journals form JSTOR.[216] Swartz was charged with 11 felony charges carrying a maximum of 1 million dollar fine and 35 years in prison.[217] At the time of his arrest, Swartz had not distributed any of the downloaded files. The act has since been amended in 1989, 1994, and 1996 and in 2001 by the USA Patriot Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act, which have expanded the list of acts that fell within the ambit of actions that could be prosecuted. These amendments have received some opposition as ordinary

---

[211] *Ibid* at 1679.
[212] O'Malley (n 141 above) at 138.
[213] Which was codified at Title 18 of the United States Code in section 1986.
[214] The current Act, 18 USC § 1030 (2006)
(a)Whoever-
> (2) intentionally accesses a computer without authorization or exceeds authorised access, and thereby obtains-
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> (B) information from any department or agency of the United States; or
> (C) information from any protected computer;

[215] B Seidman 'Internet activist charged with hacking into MIT network' *The daily Need* 22 July 2011, available at *https://www.pbs.org/wnet/need-to-know/the-daily-need/internet-activist-charged-with-hacking-into-mit-network/*, accessed on 25 November 2018.
[216] *Ibid.*
[217] *Ibid.*

internet use can easily become a legal violation because of the[218] interpretation of "unauthorised user". This prompted Representative Zoe Lofgren to propose a Bill (Aaron's Law) that would amend the CFAA and prevent the disproportionate charges brought against Swartz, because of the broad scope of the CFAA, from being brought against others.[219] Further, this severe punishment of hacktivist is imposed because the technology that hacktivists use is often misunderstood.[220] This push for hard punishment is fuelled by the fact that hacktivist are a large group of people who are seemingly difficult to identify, and often what unites them is just a shared ideology.[221]

The law in the United Kingdom (UK) that deals with cybercrime is the Computer Misuse Act 1990 (CMA), the effects of which, are very similar to that of the USA. Section 3 of the CMA states:

> It shall be an offence to impair the operation of any computer, to prevent or hinder access to any program or data held in any computer and to impair the operation of any such program or reliability of any such data.[222]

The CMA, like the CFAA, casts too wide a net on the list of activities which incur criminal prosecution.

Although cyber hacktivist show a frequency to cause disruption and expensive mischief, hacktivists have not shown a willingness to endanger the lives of people for a political cause.[223] For this reason it would seem as going too far to paint acts of hacktivism with cybercrimes in general. This intention, not to cause harm to civilian population is a very important distinction, as it differentiates hacktivism form other cybercrimes such as cyber terrorism and cyberwar.[224] It is argued by O'Malley, that so long as forms of hacktivism "1) are expressive in nature, 2) are performed without anonymity, with actors willing to take responsibility, 3) have a legitimate purpose, 4) proportionately balances the damage or disruption with the benefits to

---

[218] C Thompson 'Hacktivism: Civil disobedience or cybercrime?' *ProPublica* 18 January 2013 available at https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime, accessed on 25 November 2018.

[219] R J Reilly 'Zoe Lofgren introduces 'Aaron's Law to honour Swartz on Reddit' *Huffington Post* 15 January 2013 available on, https://www.huffingtonpost.com/2013/01/15/zoe-lofgren-aarons-law-swartz_n_2483770.html, accessed on 25 November 2018.

[220] T M Knapp 'Hacktivism –Political Dissent in the final Frontier (2015) 49(259) New England Law Review at 262

[221] *Ibid* at 263.

[222] Computer Misuse Act 1990 s 3(2).

[223] K Hardy 'Operation Titstorm: 'Hacktivism or cyberterrorism' (2010) 33(2) *UNSW Law Journal* 491

[224] O'Malley (n 141 above) at 157.

be achieved, and 5) are non-violent,"[225] they should be afforded the protection of legitimate forms of protest given under the right to freedom of expression, to which I agree.

In the maritime industry, hacktivists seek to publicly put pressure on the shipping industry, for a specific objective for either environmental concerns [226] or prevention of handling of specific cargoes because they are unethical or will endanger the lives of a population. The target may be the shipping company's computer network, the ship itself or third party suppler of recipient of the cargo.[227]

2.4. The effects that threat actors seek to achieve

There are different reasons that maritime cyber security threat actors seek to achieve. These outcomes maybe aimed at the ship or ship subsystem or the overall business. These include:

1. "Destroy - examples may include the destruction of cargo, ship, or port such that they are no longer available for use.[228]
2. Degrade - examples may include impacting the speed or manoeuvrability of the ship, the ability to navigate accurately or monitor the local environment accurately to the point where the ability of the ship to operate is significantly impaired.[229]
3. Deny - examples may include the denial of access to ship systems or information/data possibly for such reasons as extortion for financial gain or to mount a physical attack on the ship for kidnapping and ransom purposes.[230]
4. Delay - examples may include to delay the timely operation of the ship or ship subsystem such that the knock-on effect may impact business operations or cause penalties to be incurred.[231]
5. Deter - examples may include influencing the business from operating in certain areas of the world oceans, operating in specific markets or accessing specific ports from a commercial perspective.[232]

---

[225] O'Malley (n 141 above) at 158.
[226] For example, hacktivist could infiltrate the computer networks of an offshore oil platform to protest against oil drilling.
[227] Langouvardou (note 96 above) at 58.
[228] H Boyes and R Isbell 'Code of Practice: Cyber security for ships' (2017) Institution of Engineering and Technology, London, United Kingdom available *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf*, accessed on 3 November 2018 at 18.
[229] *Ibid.*
[230] *Ibid.*
[231] *Ibid.*
[232] *Ibid.*

6. Detect - examples may include the detection of people cargo or ship locations and o track such that planned physical theft or cargo manipulation might take place.[233]
7. Distract - examples include the ability to alter the state of a sensor so to provide a distraction whilst a data /information extraction takes place. [234]

This list is not exhaustive".[235]

2.5. Cyber vulnerabilities In Marine Transportation Systems

The devices and information systems used in the maritime industry are not immune to cyber threats. While these information and communications technology (ICT) systems and computer networks facilitate increased functionality and accessibility for the industry, which results in efficient operations, these ICT systems and computer networks face complex and unique vulnerabilities.[236] These vulnerabilities can arise from deficiencies or inadequacies in the design of different software and hardware, integration of and maintenance of the Industrial Control System (ICS) which remotely carry and assess information are on-board most modern ships and in onshore infrastructures that support them,[237] as well as lapses in cyber-discipline in the network systems of different.[238] These ICS are often available immediately and are not specially made to suit a particular purpose.[239]

2.5.1. On board a ship

Commercial shipping companies are irreversibly reliant on Global Navigation Satellite Systems (GNSS)[240] which have replaced paper charts in vessels.[241] GNNS signals are vulnerable to:

[233] *Ibid.*
[234] *Ibid.*
[235] *Ibid.*
[236] D M Silgado *Cyber-Attacks; Digital Threat Reality Affecting The Maritime Industry* (unpublished Masters of Science thesis, World Maritime University, Sweden 2018).
[237] Foote (n 87 above) at 237.
[238] IMO 'Interim Guidelines On Maritime Cyber Risk Management' *Maritime Safety Committee MSC.1/circ*.1526 (1 June 2016).
[239] Foote (n 87 above).
[240] Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. Available at, https://www.gsa.europa.eu/european-gnss/what-gnss, accessed on 29 May 2019.
[241] D B Moskoff & W G Kaag 'Threats to Global Navigation' in J Direnzo III…et al (ed) Issues In Maritime Cyber Security (2017) at 5

1. *Jamming and Interference*. “The broadcast of stronger signals that intentionally or unintentionally blocks or impacts a GNSS satellite signal”.[242]
2. *Spoofing*. “The broadcasting of false GNSS signals at slightly greater power. This deceives the GNSS receiver into locking onto the spoofed signal. Once the receiver has locked onto the stronger spoofed signal, the false signal gradually phases out of sync with the actual; GNSS signal, causing the receiver to report false Positioning Navigation and timing (PNT)”.[243]
3. *Meaconing*. “The intentional delay and rebroadcasting of a GNSS signal intended to introduce error to receive”.[244]

Security vulnerabilities in maritime navigation equipment that use GPS (Global Positioning System) as a data input, include the ability to download, read, replace or delete any file stored on machines hosting ECDIS.[245] Close to a million ships have Automatic Identification System (AIS) transceivers,[246] which track ships automatically and electronically link positional data with other ships. A major flaw in AIS lies in the fact that AIS information in assumed to be genuine, “there is not built-in security or verification system that provides a level of backup”.[247] This means that hackers could hack into a ships system and falsify a vessels position, identity or type, speed and heading.[248]

2.5.2. Oil rigs:

A Dynamic Positioning (DP) is “a computer-controlled system to automatically maintain the positioning (and heading) of a vessel, and in particular of an oil rig”[249] The stability of an offshore rig is dependent on the correct information being fed into a computer program, with information such as wind direction, speed, the position and angle of the rig etc.[250]

2.5.3. Cargo:

Cargo handling systems and the management thereof, are now highly digital.[251] Criminals could thus remotely access the schedule of their containers, through malware that spoofs the

---

[242] *Ibid at 7*.
[243] *Ibid at 7*.
[244] *Ibid at 7*
[245] DiRenzo (n 9 above).
[246] *Ibid*.
[247] *Ibid*.
[248] *Ibid*.
[249] *Ibid*.
[250] *Ibid*.
[251] *Ibid*.

system into believing that a regular transactions is taking place, containing illegal substances and releasing them to themselves without being detected.

2.5.4. Port operations

Today port operations rely on the complex network of systems and data flow between logistic companies, IT providers, cargoes, crew and vessels.[252] These include the use gantry cranes now using optical recognition to manage port operations, electronic devices to locate cargo, moving containers automatically using GPS, trucks that transport cargo are also heavily dependent on GPS.[253] This interconnectivity makes ports vulnerable to hackers entering a virus on one system and subsequently connecting to other devices in the port.

[252] Silgado (n 236 above).
[253] *Ibid.*

CHAPTER 3:

LEGAL FRAMEWORK REGULATING MARITIME CYBERSECURITY

3.1. International conventions and guidelines

3.1.1. "United Nations Convention on the Law of the Sea (UNCLOS)"

Trade, travel and conflict have always been a part of the maritime domain. This Chapter examines the relevant international conventions and guidelines that relate to maritime cyber security threats internationally. A discussion on regional Conventions, in particular the African Union Convention on Cyber Security and Personal Data Protection and the European Convention on Cyber Crimes will follow. Lastly South Africa's domestic legal framework will be examined.

On the 10th December 1982 the United Nations Convention on the Law of the Sea[254] was opened up for signatures. The broad base legal framework saw the participation of over 150 countries, culminating in 14 years of working on the drafting of the convention.[255] UNCLOS incorporated the "Convention on the High Seas".[256] The customary laws governing the navigational freedom of the sea were codified in UNCLOS.[257] This legal regime establishes governance of the high seas as one that has "immunity from national appropriation and establishes multilateral governance by treaty, and a limitation on use to only 'peaceful purposes'".[258] Two noteworthy articles in UNCLOS can be interpreted to deal with cyber-attacks at sea. Article 19 affords vessel safe passage in another countries territorial water,[259] barring the following prohibited acts:

> a) "any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal state, or in any other manner in violation of the principles of international law embodied in the Charter if the United Nations;
>
> …

[254] United Nations Convention on the Law of the Sea (10 December 1982).
[255] B H Dubner 'Recent developments in the international law of the sea' (1999) 33(2) *The International Lawyer* at 628.
[256] The Convention on the High Seas was opened for signatories on the 29th April 1958.
[257] South Africa signed the Convention on 5 December 1984 and ratified the Convention on 23 December 1997. Available on the Department of International Relations and Cooperation website , *http://www.dirco.gov.za/foreign/Multilateral/inter/unclos.htm*, accessed on 26 November 2018.
[258] K E Eichensehr 'The cyber-law of nations' (2015) 103 (317) *The Georgetown Law Journal* 341
[259] UNCLOS (n 75 above) Article 19 (1).

c) any act aimed at collecting information to the prejudice of defence or security of the coastal state;

d) any act of propaganda aimed at affecting the defence or security of the coastal state;

…

k) any act aimed at interfering with any system of communication or any other facilities or installations if the coastal state…"[260]

Though not explicitly provided for, these acts could be read to mean the cyber threats on computer networks systems on board a vessel mentioned in chapter two above. Article 109 (a) states that "All states should cooperate in the suppression of unauthorised broadcasting from the high seas".[261] These prohibited acts could extend to unauthorised penetration of a ship's cyber network.[262]

3.1.2. "Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation(SUA)"

The cyber threats to the maritime industry, mentioned in the previous chapter, illustrate why it is necessary for the international community to prepare for and deter cyber threats in order to maintain safety and security in the maritime industry. Many maritime incidents have attracted the attention of the international community, of these incidents there are a number of notable ones that prompted the international maritime security authorities to draft a regulatory framework, as a response.[263] The seizure of the *Achille Lauro*, is one such incident. The case involved the seizure of an Italian-flag ship on the 7th of October 1985, by members of the Palestine Liberation Front, a faction of the Palestine Liberation Organisation (PLO) who had boarded the ship and held the passengers and the crew.[264] The hijackers, who had posed as tourist, threatened to kill the passengers unless 50 Palestinians were released from prisons.[265] This prompted the drafting of a resolution on maritime terrorism[266] and in 1986, the

[260] UNCLOS (n 75 above) article 19 (2)
[261] UNCLOS (n 75 above) article 109 (2) states that for the purpose of the Convention "unauthorized broadcasting" means the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to international regulations, but excluding the transmission of distress calls".
[262] Hathaway (n 8 above) at 873.
[263] *Ibid.*
[264] M Halberstam 'Terrorism on the high seas: The Achille Lauro, piracy and the IMO Convention on maritime security' (1998) 82(2) *The American Journal of International Law* at 269.
[265]*Ibid.*
[266] U.N.G.A. Resolution 40/61, 9 December 1985. The resolution included a note that requested the IMO to recommend appropriate action.

International Maritime Organisation (IMO) established an Ad Hoc Preparatory Committee, open to all states, to consider a convention against maritime terrorism, based on a draft submitted by Austria, Egypt and Italy. [267] The Convention for the "Suppression of Unlawful Acts against the Safety of Maritime Navigation (the SUA Convention)" was adopted and opened for signatures in March 1988, at a conference in Rome[268]. This Convention provided for a range of acts "connected with attacks against ships or persons on board a ship."[269] The purpose of the SUA Convention, which South Africa has signed and ratified,[270] is to ensure that persons who commit unlawful acts against a ship, have the appropriate action taken against them.[271] Though the SUA Convention does not make specific mention to cyber security, Article 3 lists the acts which if done intentionally or unlawfully, would render [272]individuals guilty of committing an offence if:

1. "Seizes or exercises control over ship by force or threat thereof or any other form of intimidation; or…
3. Destroys a ship or causes damage to a ship or its cargo which is likely to endanger the safe navigation of the ship; or
4. places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; or
5. destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship".

The "Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (The 2005 Protocol)"[273] made the following amendments to the SUA Convention.

Article 3, paragraph 1(f) of the convention is replaced by the following text:

[267] Halberstam (n 264 above) at 270.
[268] The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (10 March 1988).
[269] G Plant 'The Convention for the Suppression of Unlawful Acts against the Safety of maritime Navigation' (1990) 39 *International and Comparative Law Quarterly* 28
[270] Available on the Department of International Relations and Cooperation website, available at http://www.dirco.gov.za/foreign/Multilateral/inter/imo.htm, accessed on 27 November 2018.
[271] International Maritime Organisation 'Maritime security' available at http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx, *accessed* on 27 November 2018.
[272] The SUA Convention (n 256 above), Article 3 (1).
[273] The Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (14 October 2015).

(f) "Communicates information which that person knows to be false, thereby endangering the safe navigation of a ship."[274]

Article 3, paragraph 2 of the Convention is replaced by the following text:

> 2 Any person also commits an offence if that person threatens, with or without a condition, as is provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraphs 1 (b), (c), and (e), if that threat is likely to endanger the safe navigation of the ship in question.[275]

Article 3*bis* was added and in effect holds that when the purpose of an act, by its nature or context is to intimidate a population, or compel a government or an international organisation to do or abstain from doing any act that uses a ship in a manner that causes death or serious…[276] if done unlawfully and unintentionally that person commits an offence as per the Convention.

The act also makes mention of "any equipment, materials or software or relate Technology"[277], however, this is only as it relates to biochemical weapons.

Though the 2005 Protocol , have gone a long way in ensuring that the security framework established under the SUA Convention is capable of responding to contemporary maritime threats, by "introducing offences relating to maritime terrorism; the illicit trafficking of weapons of mass destruction".[278] Further the SUA Convention simplified several of the issues surrounding jurisdiction and the list of offences covered.[279] However, it loses its power and relevance if it cannot be applied to *sui generi*s emerging threats to transportation, such as maritime cyber threats. The wording of both the SUA Convention and the 2005 Protocol is broad enough to include some of the cyber threats listed in chapter 2. If the nature of the cyber threats listed in chapter two, is such that they interfere with the safe navigation of a ship, then a wide interpretation of the Convention would mean that those cyber threat perpetrators would be guilty of an offence, giving states that are party to this convention the right and duty to respond. For example a cyber attack on an oil carrier, that would disrupt the navigation or steering of the vessel, resulting in the vessel grounding, could cause an oil spill and have

---

[274] The 2005 Protocol Article 4 (2).
[275] The 2005 Protocol Article 4 (4).
[276] The 2005 Protocol Article 5 (1)(a)(iii).
[277] The 2005 Protocol Article 5 (1)(a)(iv).
[278] R Abeyrantne 'New and emerging threats to maritime security' (2010) 18 (2) *Asia Pacific Law Review at* 177.
[279] J S C Mellor 'Missing the boat: The legal and practical problems of the prevention of maritime terrorism' (2002) 18(2) *American University International Law Review at* 383.

devastating effects to the environment. A shortfall in this broad list of acts that constitute an offence under the Convention, as it pertains to cyber security, would be the interpretation of different words and provisions. As it stands there is no consensus as to the meaning of *maritime security*[280], and maritime cyber security has also seen many different definitions being attached to what it is. Article 4 (2) of the 2005 is a good example of this problem in interpretation. The words "Communicates information" necessitate further interpretation when it comes to cyber security, does this mean that the person has to physically communicate this information? Malware and coding allow hackers to remotely communicate information into computer networks, which could give hackers' access to the GPS of a ship or alter the direction of a ship.

Lastly while the SUA Convention provides states with a positive obligation to either extradite or prosecute offenders[281], the nature of maritime cybercrimes give the perpetrators the advantage of anonymity, which "enables the hacker to obviate checkpoints or any physical evidence being traceable to him or her" which would make the issues of jurisdiction and extradition obsolete as there would be no identified perpetrator.[282]

3.1.3. "International Ship and Port Facility Security Code"

The IMO is the regulatory body of the United Nations entrusted with the responsibility for safety of life at sea and environmental protection. Devastating world events, which threatened maritime security, have prompted the IMO to draft regulations and conventions to respond to such events. One such incident was the terrorist attacks on the Pentagon and the World Trade Centre in the USA, launched in September 11 2001.[283] After discussions of the vulnerability of international maritime community and vessels at sea, the IMO drafted maritime security instruments including Assembly resolution A.924 (22) in November 2001.[284] The aim of the resolution was "to reduce risks to passengers, crews and port personnel on board ships and in

[280] C Bueger 'What is maritime security?' Marine Policy (2015) 53 *Elsevier* at 160.
[281] Article 10 (1) of the SUA Convention, supra note 13, states "The State Party in the territory of which the offender or the alleged offender is found shall, in cases of which article 6 applies, if it does not extradite him, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State."

[283] P L Bergen 'September 11 attacks' (15 November 2018) available at https://www.britannica.com/event/September-11-attacks, accessed on 27 November 2018.
[284] IMO Resolution A. 924(22) Agenda item 8 'Review of the measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships'. Adopted on 20 November 2001.

port areas and to the vessels and their cargoes and to enhance ship and port security and avert shipping from becoming a target of international terrorism".[285] As a result of the resolution, the IMO adopted a number of amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended.[286] The 2002 SOLAS Conference was held in the London headquarters of the IMO, from the 9th to the 13th of December 2002. The "International Ship and Port Facility Security Code (ISPS Code)" was enshrined under Chapter XI-2 of SOLAS on 1 July 2004. This code together with the other amendments to SOLAS 1974, seeks to establish an international framework of security-related "standards" to be achieved by different stakeholders, including governments, local governments , local administrators and port and shipping authorities.[287]

The ISPS code is divided into two parts, a mandatory section (Part A) and a recommendatory section (Part B). The code requires ships on the high seas and ports that serve them to take appropriate preventative measure against security threats, conduct security assessments, develop security plans, have designated security officers and conduct training and drills.[288] Being a signatory of IMO, South Africa has ratified and implemented the ISPS Code.[289] The ISPS Code has been given effect by the "Merchant Shipping (Maritime Security) Regulations, 2004"[290](hereinafter referred to as Regulations 2004) which are enabled under section 356 of the Merchant Shipping Act 1951.[291] The discussion of the requirements for international ship and port security will be discussed below.

3.1.4. Maritime Industry Practice Guidelines

There have been significant developing threats to maritime cyber security in recent years. While the international community have recognised the seriousness of these threats and the possible magnitude of their consequences, these threats have been subject to comparatively less regulations and guidelines.

---

[285] Resolution A. 924(22)
[286] The International Convention for the Safety of Life at Sea (SOLAS), 1974, currently in force, was adopted on 1 November 1974 by the International Conference on Safety of Life at Sea, which was convened by the International Maritime Organization (IMO), and entered into force on 25 May 1980.
[287] IMO maritime security policy -Background paper EEF.IO/3/08 (23 January 2008).
[288] R B Brailer 'Protecting US ports with layered security measures for container ships' (2005) 185 Military Law Review 23.
[289] South African Maritime Safety Authority Marine Notice No.12 of 2018, available at https://www.samsa.org.za/sites/samsa.org.za/files/mn%2012%20of%202008.pdf , accessed on 8 June 2019.
[290] Department of Transport GN R.751 of GG 26488, 21/06/2004 at 97.
[291] The South African Merchant Shipping Act 57 of 1951

3.1.4.1. International Maritime Organisation

In its ninety-sixth session (from 11 May 2016 to 20 May 2016), having regard to the urgent need to raise cyber awareness on cyber vulnerabilities and threats in shipping, the Maritime Safety Committee approved the "*Interim Guidelines on Maritime Cyber Risk Management*.[292] Article one of the guidelines states that the guidelines aim to provide "high level recommendations for maritime cyber risk management."[293] The IMO guidelines were designed to be incorporated with existing industry regulations and procedures, referencing both the BIMCO guidelines and the NIST Framework. These recommendatory guidelines focus on a risk management approach, which is defined as "the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders."[294] Both the IMO Guideline and the NIST Framework focus on the same five functional elements to sustain a culture of risk awareness, which are concurrent and continuous,[295] namely:

1. "Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations."[296]
2. "Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations."[297]
3. "Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner."[298]
4. "Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event."[299]
5. "Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event."[300]

While the guidelines may be a good tool for smaller shipping companies, ships with complex cyber related systems would require additional resources through reputable industry and

[292] IMO 'Interim Guidelines on Maritime Cyber Risk Management' *Maritime Safety Committee MSC.1/circ.1526* (1 June 2016) at 1.
[293] *Ibid* at 1..
[294] *Ibid* at 3.1.
[295] Foote (n 87 above) at 258.
[296] MSC.1/Circ.1526 (n 235 above) at 3.5
[297] *Ibid.*
[298] *Ibid.*
[299] *Ibid.*
[300] Ibid.

Government partners[301] The guidelines are also recommendatory, as stated in section 2.2 of Annexure 1, and thus hold no real obligations on shipping companies and shipping nations on how to implement good cyber risk management tools.[302] The MSC Guidelines, though they recognised the issue at hand, were broad and not specific enough on a number of issues, including their application, response and deterrence of maritime cyber threats.[303]

The IMO amended two of their general security management codes in 2017 to explicitly include cyber security. The ISPS and the International Safety Management Code (ISM)[304] provide direction on how ship operators and port officials should regulate cyber risk management processes.[305] Resolution MSC.428 (98) *Maritime Cyber Risk Management in Safety Management Systems*[306]*"*was adopted on 16 June 2017. The Resolution affirms "that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM code"[307] and encourages "administrators to ensure that the cyber risks are appropriately addressed in safety management systems not later than the first annual verification of the company's Document of Compliance after 1 January 2021"[308]

The Baltic and International Maritime Council (BIMCO) and other influential maritime organisations[309] sought to change this by releasing "The Guidelines on Cyber Security On board Ships" in February 2016.[310] The IMO followed example and released interim guidelines

[301] IMO 'Interim Guidelines on Maritime Cyber Risk Management' Maritime Safety Committee MSC.1/circ.1526 (1 June 2016). Annexure 1 Page 3.
[302] MSC.1/circ.1526 (n 235 above) at page 3.
[303]Martin (n 63 above).
[304] The ISM Code in its mandatory code was adopted in 1993 by Resolution A.741(18) and entered into force on 1 July 1998.
[305] V L Forbes 'The global maritime industry remains unprepared for future cybersecurity challenges' 21 August 2018, available at *http://www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/* , accessed on 8 June 2019.
[306] Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems Annexure 10, available at *http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf* accessed on 8 June 2019.
[307] Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems Annexure 10 Article 1.
[308] Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems Annexure 10 Article 2.
[309] Supported by BIMCO, CLIA(Cruise lines International Association),ICS(International Chamber of Shipping), INTERCARGO(International Association of Dry Cargo Ship Owners) and INTERTANKO(International Association of Independent Tanker Owners).
[310] The Guidelines on Cyber Security On Board Ships, published by BIMCO (Version 1.1- February 2016) .

addressing cyber risk in June 2016[311]. These guidelines must be aligned with the recommendations given in the IMO's recommendations.

3.1.4.2. The Baltic and International Maritime Council (BIMCO)

Many of the existing international safety guidelines cover security issues for on-shore operations. The BIMCO guidelines focused on minimum requirements for assessing operations and implementing the necessary procedures for maintaining cyber security on board a ship.[312] The aim of the BIMCO guidelines is to "offer guidance to ship-owners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems on board their ships"[313] According to the BIMCO guidelines a shipping companies cyber risk management policies should be seen as completing to the exiting security requirements contained in ISM Code[314] and the ISPS Code.

The BIMCO guidelines are split into four categories:

1. Understanding the cyber threat
   Different "cyber risks exist that are specific to the company ship operation or trade. When a company assess the cyber risks that they are exposed to, they should be aware of any specific aspect of their operations that may increase their vulnerability to different cyber threats. In the same way shipping companies need to understand the cyber risks and vulnerabilities that they are exposed to, users of IT systems on board a ship must be aware of potential cyber security risk, and must be trained to identify and mitigate such risks."[315]
2. Assessing the risk
   Cyber security in a company should take a top down approach instead of being immediately being delegated to the Ship Security Officer (SSO) or the head of the IT department. The maritime industry has a range of characteristics that affect its vulnerability to cyber incidents and the level of these risks will reflect on the company, ship, the IT and OT systems used, and the information and/or data stored. Companies are encourages to utilise the (NIST) Cyber Security Framework [316] to qualify the approach being taken to cyber security using common principles and
   Standards. The guidelines also advocate for robust approaches to cyber

[311] MSC.1/Circ. 1526 Interim Guidelines on Maritime Cyber Security Management (1 June 2016).
[312] Foote (n 87 above) at 255.
[313] The Guideline (n 46 above).
[314] IMO Assembly Resolution A.741 (18) The International Safety Management Code (1993).
[315] The Guidelines(n 46 above).
[316] National Institute of Standards and Technology (NIST) Cyber Security Framework Version 1.1 (16 April 2018) available at, https://www.nist.gov/cyberframework/framework, accessed on 28 November 2018.

Security, both now and in the future.[317]

3. Reducing the risk

   The main deliverable of a company's cyber security strategy should be reducing the risk. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security. Considerations should also be made to deal with occasions in the life cycle of the ship where the normal controls are invalidated. Technical controls should be in place to that ensure that on board systems are designed and configured to be resilient to cyber-attacks, as well procedural controls should be covered in company policies, safety management procedures, security procedures and access controls. Both technical and procedural controls should be compatible with the confidentiality, integrity and availability (CIA) model for protecting data and information.[318]

4. Developing contingency plans

   Ships should "have access to appropriate contingency place that are developed by companies in order to effectively respond to cyber incidents. Where responding to a cyber-incident is beyond the competencies held within the company and on board due to the complexity of the cyber incident or severity thereof, external experts' assistance should be available for and effective response. Contingency plans should include consideration of who has decision-making authority, when to call in external experts (and whom), as well as communication."[319]

The second addition of the BIMCO guidelines[320] were released in June 2017 and build on the existing Version 1.0 guidelines. Are now considered to be the most comprehensive guidelines for the shipping community. The updated sections focus on:

1. Cyber security and safety management

   Cyber "safety and cyber security are equally important as both have the potential to affect the safety of the ship, personnel on board the ship and cargo. Version 2.0 of the guidelines aim to provide essential guidance on managing cyber safety and cyber security" risks.[321]

2. Managing Ship to shore interface

   There "is a need to control the ship to shore interface, as ships are becoming more and more integrated with shore side operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. The risks of misunderstood, unknown, and uncoordinated remote access to an operating ship should be taken into consideration as an important part of the risk assessment. The guidelines

[317] The Guidelines (n 46 above).
[318] The Guidelines (n 46 above).
[319] The Guidelines (n 46 above).
[320] The Guidelines on Cyber Security On board Ships, published by BIMCO (Version 2.0- June 2017)
[321] Version 2.0 of the guidelines, *ibid.*

recommend that companies fully understand the ships OT and IT systems and how they connect to the off shore side of their operations. [322]"

3. Effectively segregate networks

   Care "should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. Stand-alone systems will be less at risk to external cyber-attacks compared to those to uncontrolled networks there for care has to be, further human interaction with these networks also has to be considered.[323]"

4. Insurance Issues

   For insurers, "the term 'cyber' includes many different aspects and it is important to distinguish between them and their effects on insurance cover." Companies should be able to demonstrate that they are acting with reasonable care in their approach to managing cyber risk and protecting the ship from any damage that may arise from a cyber-incident.[324]

3.1.4.3. Seaworthiness

Shipowners and operators are cautioned against ignoring these industry guidelines. If a ship owners systems were penetrated, and they could not show that they acted with reasonable care in managing cyber vulnerabilities and protecting their ship, then the ship could be unseaworthy, which would be a breach of the contract of carriage.[325]The carrier's obligation to provide a seaworthy ship has always underpinned a carriage of goods contract. At common law this duty by the carrier to provide a seaworthy vessel was absolute.[326] A sea worthy vessel, as defined in *McFadden v Blue Star*[327] as "a vessel must have that degree of fitness which an ordinary carful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it".[328] While South Africa did not ratify the Hague Visby Rules[329], it did incorporate[330] the rules into the "Carriage of Goods by Sea Act 1986 (SA COGSA)".[331] Article III Rule 1 of the Hague Visby Rules provide that,

---

[322] Version 2.0 of the guidelines ,*ibid.*
[323] Version 2.0 of the guidelines ,*ibid.*
[324] Version 2.0 of the guidelines ,*ibid.*
[325] M Montgomery 'New BIMCO cyber security guidelines' HFW Briefings (July 2017), available at *http://www.hfw.com/New-BIMCO-Guidelines-July-2017*, accessed on 28 November 2018.
[326] Riverstone Meat Co. Pty. Ltd. V Lancashire Shipping Co. (The Muncaster Castle) [1961] 1 Lloyd's Rep. 57
[327] Mcfadden v Blue Star Line, [1905] 1 K.B. 697.
[328] Mcfadden v Blue Star Line, [1905] 1 K.B. 697 at 706
[329] The Hague-Visby Rules - The Hague Rules as Amended by the 1 Brussels Protocol 1968.
[330] J Hare "Shipping Law and Admiralty Jurisdiction in South Africa" 2 ed (2009) at page 625.
[331] "The South African Carriage of Goods by Sea Act 1 of 1986" .

"1. The carrier shall be bound before and at the beginning of the voyage to exercise due diligence to:

(a) Make the ship seaworthy;
(b) Properly man, equip and supply the ship;
(c) Make the holds, refrigerating and cool chambers, and all other parts of the ship in which goods are carried, fit and safe for their reception, carriage and preservation."[332]

The introduction of the carriers' obligation to exercisedue diligence, shows the shift to provide a lower measure of obligation as opposed to the absolute duties stipulated under common law, Furthermore, this duty is a positive obligation on the part of the carrier, which "must be discharged, in order for the carrier to be protected by Article IV (2) of the Hague Visby Rules." [333] Seaworthiness thus hinges on the interpretation of the term "due diligence", which has been defined as "the efforts of the prudent carrier to take all reasonable measures that can be possibly taken, in the light of available knowledge and means at the relevant time, to fulfil his obligation to provide a seaworthy vessel".[334] The conclusion is therefore, that on a reading of this definition of the carriers obligation to exercise due diligence, where a carriers fails to the measures provided for in the BIMCO guidelines on cyber security, it can be said that they did not meet the standard required for seaworthiness. This in turn could also have ramifications for insurance claims. For a vessel in the current cyber maritime climate, to be seaworthy, there must be crew members that are specifically trained to address cybercrimes, and an adequate number of crew with the knowledge to address cyber threats should they become a reality. The ship must be equipped with critical security (both IT and OT) controls that will sufficiently protect a vessel against cyber-attacks.

An assessment of the guidelines reveal that the guidelines mentioned above represent industry best practice to approaching maritime cyber vulnerabilities and threats. The guidelines differ in their scope however they encompass the same fundamental principles.[335] These include, advocating for the NIST Framework principles into maritime cyber security approach. The guidelines suggest that the best way to approach cyber security is through a cyber awareness.

---

332 Article III Rule 1 of the Hague Visby Rules.
333 M Naidu *A comparative Analysis of the Carriers Liability under the Hague Visby and Rotterdam Rules* (unpublished LLM thesis, University of KwaZulu- Natal 2016, 25)
334 AH Kassem *The Legal Aspects of Seaworthiness: Current Law and Development* (unpublished PHD, University of Wales, 2006)
335 Foote (n 87 above) at 255.

The guidelines further point out that "each entity must have knowledge and understanding of any protection measures already in place and the capabilities and limitations of these measures".[336]

3.2. Regional Framework

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

ICT and internet penetration has increasingly grown in the African continent, this has in turn raised concerns on over the need "to promote cybersecurity governance and cyber stability in the continent".[337] The AU was then prompted to establish a regional treaty on cyber security. In "June 2014 the African Union Convention on Cyber Security and Personal Data Protection was established."[338] The AU Cyber Convention took into account the Oliver Tambo Declaration adopted by the Conference of African Ministers in charge of ICT, which was held on 5 November 2009 in Johannesburg South Africa.[339] It is stated in the Preamble of the AU Cyber Convention that "the major obstacle to the development of electronic commerce in Africa are linked to security issues particularly:

a) "The gaps affecting the regulation of legal recognition of data communications and electronic signature;"[340]
b) "The absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems;"[341]
c) "The absence of e-services and telecommuting legislations;"[342]
d) "The application of electronic techniques to commercial and administrative acts;"[343]

[336] Ibid at 256
[337] U J Oriji, 'The African Union Convention on Cyber security: A regional response towards cyber stability' (2018) 12(2) Masaryk University Journal of Law and Technology at 92.
[338] Adopted by the twenty-third ordinary session of Assembly, held in Malabo, Equatorial Guinea on 27 June 2014.
[339] U J Oriji 'The Defects on the Draft African Union Convention on the establishment of a credible legal framework for cyber security' available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6780881 accessed 6 November 2018. The Declaration instructed the AU and the UN Economic Commission for Africa to joint develop a Convention on cyber legislation based on the continent's needs.
[340] African Union Convention on Cyber security and Personal Data Protection, 27 June 2014, at page 1.
[341] *Ibid.*
[342] *Ibid.*
[343] I*bid.*

e) “The probative elements introduced by digital techniques (time stamping, certification etc);”[344]
f) “The rules applicable to cryptology devices and service;”[345]
g) “The oversight of on-line advertising;”[346]
h) “The absence of appropriate fiscal and customs legislations for electronic commerce.”[347]

The goal of the AU Cyber Convention is “to address the need for harmonised legislation in the area of cyber security in member States of the African Union…”[348] South Africa is not party to this convention.[349] While the AU Cyber Convention does deserve praise for prioritising Africa’s need to address cyber security threats and cybercrimes, there have been concerns about the overreaching provisions of the Convention,[350] as it seeks to regulate many different uses of ICT, which could infringe other existing rights of use of technology.[351] This is of particular concern to countries with existing legislation that governs cyber security and cybercrimes such as Kenya, Mauritius, Zambia and South Africa.[352] The convention places onerous requirements for these countries to reconcile their exiting cyber laws with the Au Convention.[353]

Regionally South Africa is faced with another challenge that is, the challenge of having competing bilateral and multilateral cybercrimes conventions, draft works and model laws, cyber instruments available to it in Africa. These include

- “East African Draft Legal Framework for Cyber Laws (2008)”;[354]
- “Economic Community of West African States (ECOWAS) Draft Directive On Fighting Cybercrime (2009)”;[355]

---

344 *Ibid.*
345 *Ibid.*
346 *Ibid.*
347 *Ibid.*
348 *Ibid.*
349 List of signatories of the AU Cyber Convention available on *https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf* accessed on 7 December 2018.
350 E Tamarkin ‘The AU’s cyber-crime response: A positive start, but substantial challenges ahead’ (January 2015) Policy Brief 73 Institute for Security Studies available at *https://www.files.ethz.ch/isn/187564/PolBrief73_cybercrime.pdf* accessed on 7 December 2018 at 5.
351 *Ibid at 3.*
352 *Ibid* at 4.
353 *Ibid* at 4.
354 *Ibid* at 5.
355 *Ibid* at 5.

- “Common Market for Southern Africa (COMESA) Cyber Security Draft Model Bill (2011)”;[356]
- “Southern Africa Development Community (SADC) Model Law On Computer Crime and Cybercrime (2012)”.[357]

These regional instruments champion the cause of developing the legal framework on a regional scale that governs cyber security. The real challenge for the South African legislature will be deciding which Conventions it decides to be party to and ratify with the understanding that South Africa is a Constitutional democracy and the Constitutional values of privacy, freedom of expression and right to security will have to be taken into consideration.

3.2.2 European Convention on Cyber Crimes (ECCC)

The Council of Europe, in an attempt to address the issue of the increasing number of countries falling victim to cybercrimes, decided to draft the Convention on cybercrimes. The Convention on Cyber Crimes (The Budapest Convention)[358] was open for signatories in a conference held in Budapest on 23 November 2018.[359] The purpose of the ECCC, amongst other things, is to combat cybercrime on an international level and the universal harmonisation of laws relating to cyber offenses, prosecution and punishment.[360] The premise on which this international treaty was built on is that cybercrimes are a new category of crime, necessitating their own legal framework.[361] The ECCC mandates signatories to:

> “Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.”[362]

The Convention contains four parts. Part I contains the definitions section. Part II consists of the provisions that deal with substantive and procedural law and measures to be taken at a domestic level. The substantive law provisions cover criminalisation provisions by creating nine offences grouped into four categories.[363] These nine offences pertain to illegal access, data

---

[356] *Ibid* at 5.
[357] *Ibid* at 5.
[358] The Convention on Cyber Crimes ETS no 185 (23 November 2001).
[359] S L Marler ‘The Convention on cyber-crime: should the United States Ratify’ (2002) 37(1) *New England Law Review* at 183. The Convention had forty-three European state member signatories, and Japan, Canada, United States of America and South Africa were also signatories.
[360] *Ibid* at 194.
[361] *Ibid* at *194.*
[362] Article 2 of the ECCC.
[363] Explanatory Report to the Convention on Cybercrime, Budapest 23.XI.2001, European Treaty Series – No.185 at page 4, paragraph 17.

interference; computer related forgery; illegal interception system interference; misuse of devices; offences related to child pornography; computer related fraud as well as copyright and neighbouring rights.[364] Section 2 of chapter two deals with the procedural provision by first establishing that the Convention applies to any offence carried through by means of a computer system or the evidence of which takes an electronic form.[365] It then sets out procedural provisions relating to "expedited preservation of stored data; expedited preservation and partial; disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data".[366] Lastly the first Chapter details the Jurisdiction provisions.[367] Article 22 of the Budapest Convention requires states that are party to the Convention to adopt legislative measures that establish jurisdiction in accordance with Article 3 through 11 of the Budapest Convention,[368] when an offence is committed:

a) "In its territory;"[369] or
b) "On board a ship flying the flag of that Party;"[370] or
c) "On board and aircraft registered under the laws of that Party;"[371] or
d) "By one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence committed outside the territorial jurisdiction of any State."[372]

Because the jurisdiction provisions of the Budapest are linked to the state and not focused on the perpetrator, the Budapest Convention progressively allows a state to exercise its jurisdictional powers "in a computer crime involving a computer system within its territory, even if the perpetrator committed the offense form a remote location outside of the state"[373]

Part III consists of international co-operation and the final chapter, chapter IV consists of miscellaneous provisions that are generic to most Conventions.

---

[364] *Ibid p*age 4, paragraph 18.
[365] *Ibid* page 4, paragraph 19.
[366] *Ibid* page 4, paragraph 19.
[367] *Ibid* page 4, paragraph 19.
[368] Convention on Cybercrime, Budapest 23.XI.2001 Article 22.
[369] *Ibid* Article 22(1)(a).
[370] *Ibid* Article 22(1)(b).
[371] *Ibid* Article 22(1)(c).
[372] *Ibid* Article 22(1)(d).
[373] A M. Weber 'The Council of Europe's Convention on Cybercrime' (2003) 18(1) *Berkeley Technology Law* Journal at 423.

While South Africa is the only African county to sign the ECCC, it still has to ratify and accede to the ECCC.[374] South Africa is in compliance with part one of the Budapest Convention, with the enactment of ECT Act and RICA which mandates member states to[375]:

1. "Criminalise the illegal access to computer systems,
2. Illegal interception of data to a computer system,
3. Interfering with computer systems without right, intentional interference with computer data without right,
4. Use of inauthentic data with intent to put it across as authentic (data forgery),
5. Infringement of copyright related rights online,
6. Interference with data or functioning of computer system,
7. Child pornography related offences (which are also covered in the Copy right Act[376] and The Film and Publications Act[377])"

The practical implications of the ECCC, are a cause for great concern. The ECCC does not recognise universal jurisdiction and relies the use of domestic laws and cyber cooperation for prosecution of cyber perpetrators.[378]Although the convention seeks universal harmonisation of laws relating to cyber offences, it is not recognised as reflecting customary international norms[379] and for states that are victim to cyber attacks the difficulty lies in the implementation.[380]

3.3. Domestic legal framework

National governments have started realise the need for adopting cybersecurity strategies to address the wide range of cyber threats. Africa has long been considered as an opportune place to commit cybercrime, due to very weak network and information security.[381] The complex issues surrounding cyber security span all government instructions, as well as in all private

---

[374] F Cassim 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) 15 (2) *PER/PERLJ* at 402.
[375] S Snail 'Cyber-crime in South Africa- Hacking, cracking and other unlawful online activities' 2009 (1) Journal of Information, Law & Technology 9.
[376] Act 98 of 1978(as amended).
[377] Act 65 of 1996.
[378] Stahl(n 94 above) at 264.
[379] Stahl(n 94 above) at 264.
[380] F Cassim 'Formulating specialized legislation to address the growing spectre of cyber-crime: A comparative study' (2009) 12(4) PER 42.
[381] United Nations Economic Commission for Africa Policy Brief NTIS/002/2014 'Tackling the challenges of cyber security in Africa'.

sectors. This is need is for robust regulation is further exacerbated by the increasing reliance on technological advancements. This section will examine the South African government's responses to maritime cyber security threats.

3.3.1. Merchant Shipping (Maritime Security) Regulations, 2004[382]

The Regulations, to the MSA , 2004 apply to all seven of South Africa's major ports namely Durban, Cape Town, Richards Bay, Mossel Bay, Saldanha, Port Elizabeth and East London.[383] The Key purpose of the Regulations 2004 is to:

1. "safeguard against unlawful interference with maritime transport"[384]
2. "achieve this purpose, these regulations establish a regulatory framework centred around the development of security plans for ships and other maritime transport operations"[385]
3. "the implementation of this framework will enable the Republic to meet its obligations under Chapter XI-2 Safety Convention and the ISPS Code"[386]

The Regulations 2004 have 10 parts which are:

- Part one: Preliminary
  "This part details the objective of the Regulations 2004, their application and definitions. The Regulations 2004 define the meaning of unlawful interference with maritime transport which then clarifies the scope of application of the Regulation 2004."[387]
- Part two: Maritime Security level and security direction
  This part provides for the application of the security levels, system notifications and security directions. The Regulations state that the default security level is maritime security 1, and places a duty on Director-General to declare, when it is appropriate for a higher level of security to be put in place, maritime security level 2 and level 3 as well as to direct maritime participants to comply with additional security measures when an unlawful interference is imminent or probable."[388]

[382] Merchant Shipping (Maritime Security) Regulations, 2004 GN R. 142 of GG 25997, 9 February 2004.
[383] South African Maritime Authority Marine Notice No. 12 of 2018.
[384] Regulations 2004 (n 382 above) at page 9.
[385] Regulations 2004 (n 382 above) at page 9.
[386] Regulations 2004 (n 383 above) at page 9.
[387] Merchant Shipping (Maritime Security) Regulations, 2004 Explanatory Note GN R. 142 of GG 25997, 9 February 2004 at 84.
[388] *Ibid* at 84.

- Part three: Maritime security plans

  “This part requires certain maritime industry participants to have maritime security plans in force which must include security measures to be implements at security levels 1, 2 and 3.”[389] Additional detail on the form and content of the security plans is set out in Annexure 2 of the Regulations 2004.

- Part four: Ship plans and ISSC

  “This part requires certain South African ships to security plans in force which include the activities to be embarked on in the different maritime security levels. In addition, this part requires ships to have ISSCs that will be issued once the ISSC has been verified. Schedule 5 of part four of the Regulations 2004 contain the requirements for obtaining the certification.”[390]

- Part five: Foreign regulated ships

  “This part requires certain foreign ships to provide pre- arrival information and their ISSCs to determine their compliance with the Regulations”[391]. Foreign ships also under an obligation under the Regulations to comply with the existing security levels.[392] This Part further includes “compliance checks and control directions that foreign regulated ships are subject should they not comply with the Regulations 2004.”[393]

- Part six: Powers of officials

  “This part deals with authorised officers, who may exercise powers for the purpose of checking compliance with these Regulations and/or preventing unlawful interference with maritime transport.”[394]

- Part seven: Information Gathering

  “This part permits the Director-General to collect security compliance information form participants in the maritime industry, which enables the Director General to deal with, and resolve compliance concerns, before a security threat compromises the maritime industry.” [395]

- Part eight: Enforcement orders

[389] *Ibid* at 85.
[390] *Ibid* at 85.
[391] *Ibid* at 85.
[392] Ibid at 85.
[393] *Ibid at* 85.
[394] *Ibid at* 85.
[395] *Ibid at* 85.

"This Part deals enforcement orders that are issued in instances when a contraventions of the Regulations has occurred or it is suspected that such contravention of the Regulations has occurred. The two types of orders that may be issued are enforcement orders and ship enforcement orders. With the realisation that prosecutions are resource extensive, and while they may be the appropriate option in serious maritime security breaches, the Regulation's allow the Director General of SAMSA the option to enforce compliance with the regulations by issuing orders instead of and in addition to prosecution."[396]

- Part nine: Miscellaneous

  "Thus Part deals with security alert systems. It requires certain South African regulated ships to be fitted with a ship security system complying with SOLAS regulations XI-2/6."[397]

- Part ten: Administrative arrangements and fees

  "This Part pertains to "administrative matters including security agreements, exemptions, the exercise of the Director General's powers and functions and fees." [398]

The Regulations 2004, are an important legal instrument and South African Marine Agencies and shipping companies need to adhere to them. This will ensure the deterrence of perpetrators of cybercrimes and other forms of criminal activity, from unlawful interference with maritime transportation.

3.3.2. Electronic Communications and Transactions Act[399]

Electronic transactions have changed South Africa's economic landscape. Businesses are gravitating to conducting their business online, because of the global economy that they can tap into. This has led to emerging cyber threats and a need for legal consequences to be promulgated. More so, because the "conventional legal frameworks governing the offline are proving to be inadequate in the online world".[400] The "Electronic Communications and Transactions Act (ECT Act)" came into force on the 30th of August 2002, with an objective to "enable and facilitate electronic communications and transactions in the public interest",[401]

---

[396] *Ibid* at 85.
[397] *Ibid* at 85.
[398] *Ibid* 85.
[399] Electronic Communications and Transactions Act 25 of 2002.
[400] S L Gereda 'Electronic Communications and Transactions Act' available at *https://www.wits.ac.za/media/migration/files/cs-38933-fix/migrated-pdf/pdfs-5/telelaw12.pdf* , accessed on 30 November 2018 263.
[401] ECT Act section 2(1).

ensure legal certainty[402] and address security issues.[403] The ECT Act works in conjunction with other relevant pieces of legislation and should be read and interpreted as such.[404] The Act applies to any electronic transaction or data message.[405]

Chapter 13 of ECT Act comprehensively deals with cyber-crimes and makes the first regulator provisions in South African jurisprudence. Section 88 of the ECT Act lists five statutory criminal offences, that a person or group of persons may be held liable for:

(1) "Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence;"[406]

(2) "A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence;"[407]

(3) "A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence;"[408]

(4) "A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence;"[409]

(5) "A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."[410]

This list is wide enough to encompass the maritime cyber threats identified in chapter two of this dissertation. The ECT Act specifically provides that a court in the Republic will have

[402] ECT Act section 2(1)(e).
[403] ECT Act section 2(1)(j) and (r).
[404] ECT Act section 3.
[405] Ibid Section 4 (1).
[406] ECT Act section 86 (1).
[407] *Ibid* 86 (2).
[408] *Ibid* 86 (3).
[409] *Ibid* 86 (4).
[410] *Ibid* 86 (2).

jurisdiction to try an offence, where “the offence was committed on board any ship or aircraft in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed”.[411] Section 90 of the ECT Act, is very progressive in that it covers a wide range of instances where a South African court will have jurisdiction[412] to prosecute an offence in terms of this act that was committed outside the country if:

a) “Where the offence was committed in the Republic;
b) Where part of the offence was committed in the Republic or the result of the offence has an effect in the Republic;
c) Where the offence was committed by a South African citizen or a person with permanent residence in the Republic or a person carrying on business in the Republic;
d) Or the offence was committed on board a ship or aircraft registered in the Republic or on a voyage or flight from the Republic at the time that the offence was committed.”[413]

Particularly for maritime cyber security, as the nature of a cybercrime or cyber offence is that it can be initiated from anywhere in the world and still have devastating effects for maritime security, including critical infrastructure like ports. For a country like South Africa that is heavily reliant on proper functioning of its ports, with approximately 96 per cent of the country’s exports being conveyed by sea[414], this piece of legislation, in particular The ECT jurisdictional provision will go a long way in deterring maritime cyber attacks.?

There are also other statutes that can be used in cases of cybercrimes in South Africa, including:

3.3.3. Regulation of Interception of Communication and Provision of Communication-Related Information(RICA)[415]

With the aim of making South Africa a safer country, RICA requires cell phone users to register their details (full name, copy of identity document and address)[416] with their perspective networks as of 1 August 2009.[417] The objective of RICA is to assist law enforcement agencies identify individuals who use their phones for illegal activities.[418] Section 2 of RICA provides

[411] Ibid Section 90 (d).
[412] The general rule in South Africa to establish jurisdiction, which is the competence of a particular court to hear a matter, is found in S v Maseki 1981 4 SA 374 (T) which submitted that in order for a a court to establish jurisdiction that offence must have taken place within the Republic.
[413] Section 90 of ECT Act (n 340 above).
[414] ‘Africa Gearing up’ PWC report available at https://www.pwc.com/gx/en/transportation-logistics/publications/africa-infrastructure-investment/assets/south-africa.pdf , accessed on 30 November 2018.
[415] Act 70 of 2002.
[416] RICA (n 78 above) Section 39.
[417] F Cassim (n 374 above) at 398.
[418] *Ibid*

that "subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any person to intercept or attempt to intercept, at any place in the republic, any communication in the course of its occurrence or transmission".[419] RICA can be used to track down cyber criminals who use a cell phone to plan or execute their malicious cyber-attacks in the maritime industry. RICA provides harsher penalties for persons found to have committed and offence under the Act, with fines not exceeding R 200 000.00 or imprisonment not exceeding ten years.[420] Thus the criminal penalties in ECT appear to be insufficient to deter cyber perpetrators.[421]

3.3.4. National Prosecuting Authority Act [422](NPA Act)

In instances of insiders committing cybercrimes, the question of criminality often rests on the matter of unauthorised access. Mainly is establishing whether, where a person who had/has authorised access to a computer or a network of computers exceeded the scope of that authority. According to the NPA Act 'unauthorised access' includes "access by a person who I authorised to use the computer but is not authorised to gain access to a certain program or to certain data held in such computer or is unauthorised at the time when the access is gained…"[423]

3.3.5. Cybercrimes and Cyber Security Bill[424]

The Department of Justice and Constitutional Development was given a mandate to analyse the cyber laws of the republic, and determine whether, the current laws makes adequate provisions for the investigation and prosecution of cybercrimes, as well as whether the laws relating to cybercrimes could be consolidated to one single law.[425] The analysis uncovered that South Africa's cyber laws which is a hybrid legal system consisting of different articles of legislation and the common law (which was developed on a case by case basis) were not in line with those of the international community.[426] It was further determined that our legal system with different laws only criminalising cybercrime as they relate to certain government

[419] The Act defines "'communication' as being both direct and indirect communication, and 'intercept' as the aural or other acquisition of contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person either than the sender or receipting or intended recipient of the communication, found at section 1 of Act 70 of 2002."
[420] RICA (n 74 above) Section 51.
[421] Cassim (n 374 above) at 399.
[422] National Prosecuting Authority Act Act 32 of 1998
[423] *Ibid* Section 40A (1)(d)
[424] Cyber-crimes and Cyber Security Bill B6- 2017.
[425] D Mangena 'Will legislation protect your virtual space? Discussing the draft cybercrime and cyber security bill' *De Rebus* 2016 33.
[426] F Ameer-Mia and C Pienaar 'South Africa :Cybersecurity 2019' available on https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa accessed on 17 June 2019.

institutions.[427] The Cybercrimes and Cyber Security Bill (herein after referred to as the 2017 Bill) was first published on 28 August 2015[428], and was introduced in Parliament on 21 February 2017.[429] According to the then "Deputy Minister of Justice and Constitutional Development, the Honourable JH Jeffery,

> The development of the proposed legislation to enhance cyber security is a necessity. It is a milestone towards building safer communities as envisaged n the National Development Plan…the Department of Justice and Constitutional Development has been tasked with the review and alignment of cybersecurity laws to ensure that these laws are aligned with the National Cybersecurity Policy Framework (NCPF) and provide for an integrated cyber security legal framework for the Republic."[430]

The 2017 Bill contains 13 chapters. Chapter one of the 2017 Bill contain definitions which are technical in their nature, and will assists in interpretation,[431] as the nature of cybercrimes is so complex. Chapter two and three of the 2017 Bill establishes the different offences and creates new offences which will regulate illegal conduct in cyber space.[432] The 2017 Bill further adapts "various other common law and statutory offences, which are currently used to prosecute conduct relating to cybercrime, to make the ore 'usable' for prosecution".[433] Section twelve criminalises involvement in cybercrimes by persons whether direct or indirectly.[434] The jurisdiction clause found in section 23, Chapter 4, of the 2017 Bill, is very expansive, giving South African courts a number of ways to establish criminal jurisdiction.[435] The 2017 bill, in chapter seven, proposes a 24/7 point of contact relating to cooperation in cybercrime matters, which would be a first for South Africa.[436] Of particular importance to maritime trade is Chapter 12, which allows the national executive to enter into agreements with foreign states, in investigations and prosecutions of cybercrimes. This is essential because of the borderless nature of cybercrimes.

---

[427] Mangena (n 421 above) at 33.
[428] GN 878 GG3961, 2/9/2015.
[429] No 20 – 2017 Fourth Session, fifth Parliament of the Republic of South Africa, Tuesday 21 February 2017.
[430] Media Briefing Statement by the Deputy Minister of Justice and Constitutional Development, the Honorable JH Jeffery, MP on the new proposed Cybercrime and cyber security Bill, 19 January 2017, available at http://www.justice.gov.za/m_speeches/2017/20170119-CyberCrimeBillBriefing.html accessed on 17 June 2019.
[431] Cybercrimes and Cyber Security Bill B6- 2017
[432] *Ibid.*
[433] Mangena (n 421 above) at 33.
[434] Cybercrimes and Cyber Security Bill (n 370 above).
[435] In particular Section 23 (2)(a)(b)(c)(d) and (e), which will give a South African court jurisdiction, even when the commission of the act occurred outside of the country where there is a connection to the country.
[436] Mangena (n 421 above).

In July 2017 the Portfolio Committee on Justice and Correctional Services issued an invitation for interested stakeholders and persons make written submission.[437] Forty such stakeholders made written submissions[438] including The South African Human Rights Commission (SAHRC), the Centre for Constitutional Rights (CFCR) and Right 2 Know (R2K), whose submissions will be considered below.

The SAHRC submitted that while it recognised the need for a legislative framework to address cyber security and cybercrimes in South Africa, there needed to be a delicate balance between the right to freedom of expression and the right to privacy within the context of the Bill. It found issue with the definition clause of the Bill.[439] The SAHRC noted with concern that a reading of the definition of the words "access" and "article" found in clause one of the Bill could potentially impact the right to privacy, which is protected in our Constitution.[440] The SAHRC contended that the broad aspects of some of the Bill's provisions may impact on investigative journalism, informants and whistle-blowers, including clauses 16 ('malicious communications') and 17 ('data message which is harmful') of the 2017 Bill.[441] In addition the SAHRC stated that under the 2017 Bill terms needed to be more narrowly defined and the intention of the parties should play a factor when prosecuting crimes.[442]

The Centre for Constitutional Rights delivered its submission on 10 August 2017. The CFCR recorded that there is a real need in South Africa for legislative measures to address the increasing cybercrimes and cyber security breaches. The CFCR welcomed the amendments made to the 2015 version of the Bill in particular he removal of "computer related espionage"; "personal information and financial offences"; "infringement of copyright" and "prohibition on dissemination of data messages which advocate , promote or incite hate , discrimination or violence", but cited areas of concern in the 2017 Bill which it feels still infringe significantly on an individual's constitutional rights to privacy, freedom of expression and access to courts.[443] The CFCR stated that it is important that the measures which the Bill proposed "do not stifle the free flow of communication out of fear of possible interception of

---

437 The Cybercrimes Bill *Ellipsis* (6 February 2019) available at https://www.ellipsis.co.za/cybercrimes-and-cybersecurity-bill/ accessed on 17 June 2019.
438 Summary Of Written Submissions And Responses Thereto: Cybercrimes And Cybersecurity Bill [B 6 - 2017] available at *https://www.ellipsis.co.za/wp-content/uploads/2017/09/171107Part_A.pdf* accessed on 23 June 2018.
439 SAHRC Submission – Cybercrimes and Cybersecurity Bill, August 2017 at page 3.
440 Section 14 of the Constitution, 1996.
441 SAHRC Submission (n 435 above) at page 8.
442 SAHRC Submission (n 435 above) at page 9.
443 Centre for Constitutional Right "CONCISE SUBMISSION ON THE CYBERCRIMES AND CYBERSECURITY BILL [B 6-2017]" 10 August 2017, at paragraph

communication".[444] In this regard the CFCR further stated that terminology used in the Bill that relates to the prohibition of "malicious communication" has to be in line with the Constitutional provisions relating to limitation of the right to freedom of expression[445] order to ensure "certainty and avoid confusion".[446]

Lastly the CFRC in paragraph 8.8 noted with concern the following:

> "Various provisions in the Bill are currently vaguely stipulated and of special concern to the CFCR is the extent to which this causes confusion with the regulatory measures provided for in RICA and unintentionally created a parallel system of surveillance. This needs to be clarified in order to be in line with the Rule of Law. This vagueness further creates potential abuse of the legal process."[447]

The CFCR therefore suggested the removal of clause 16 and 17, in their current format of the Bill. [448] The terms in clause 19 and 38 will not withstand constitutional scrutiny.[449]

The Right2Know Campaign made its submission on the Cybercrimes and Cybersecurity Bill on 10 August 2017. R2K noted with great concern the different cyber threats both at home and abroad which threaten internet freedom[450] and the approves of the aim of the Bill to "improve the state's capacity to fight actual cybercrime and out measures in place to upgrade security around all our cyber infrastructure to prevent further crime"[451] In doing so however, R2K stated that any legislation that regulates cybercrime must clearly and narrowly be so as to prevent possible misuse, state interference in its citizens data use and infringement on legitimate online activates.[452] R2K submitted that it approved the changes to the 2015 Draft Bill that related to the removal of the 'secrecy bill clauses', which would have criminalised the accessing of classified information by whistle-blowers and journalists.[453] Secondly it welcomed the removal of the copyright offenses created by the 2015 Cybercrimes draft Bill, which it identified to be "outrageously broad and inappropriate".[454]

---

[444] *Ibid* at paragraph 8.2.
[445] Section 16(2) of the Constitution 1996
[446] CFCR Submission (n 439 above) at paragraph 8.3.
[447] Ibid at paragraph 8.8.
[448] *Ibi*d at paragraph 10.1.
[449] *Ibi*d at paragraph 11.18.
[450] "Cybercrime, cybersecurity, and Internet Freedom" Right2Know Campaign submission on the Cybercrimes and Cybersecurity Bill, 10 August 2017 at page 2.
[451] *Ibid* at page 3.
[452] *Ibid* at page 3.
[453] *Ibid* at page 3.
[454] Ibid at page 4.

R2K identified the following four problems with the 2017 Bill:

1. The Bill places a heavy burden on the State to define internet governance by making cyber security to fall under the domain of intelligence
2. The Bill uses a top-down approach, to make internet users less prone to cyber-attacks, has the potential to make users less secure.
3. The bill has not addressed many of the serious problems with RICA, which is currently South Africa's main surveillance law.
4. The offences created by the Bill relating to 'malicious communication' found in Chapter 3 of the Bill raise great concerns on infringements to the right to freedom of expression.

R2K thus submit that "with the exception of the 'revenge porn' clauses the Malicious Communication sections of the Bill should be rejected. This is in line with the submissions made by the CFCR. According to R2K "there are already mechanisms to combat the ills of harmful and malicious commination."[455] It put forward that these existing mechanisms have been poorly implemented, and the solution is not to create new legal mechanisms to combat cyber security threats, but the solution is to "create a mot just and responsive justice system."[456]

In regards to the issues with freedom from surveillance R2K submitted that significant abuses have been noted by the states surveillance powers which it felt were enabled by the loopholes created by RICA.[457] The UN Human Rights Committee make findings to the effect that South Africa's surveillance laws are not in line with international human rights laws.[458] Further to this, the *AmaBhungane* Centre or Investigative Journalism, has challenged the constitutionally of some RICA provision.[459] R2K stated that Section 38 of the Bill seeks to change some provisions of RICA. R2K thus concluded that "the lack of clarity, even form within state institutions and policy makers, about how the state's surveillance polices work, as made it extremely difficult to reach consensus on what Section 38 means.[460]

Finally, as regards the Cybersecurity part of the Bill, R2K submitted that any cybersecurity legal framework need to safeguard against state invasion of privacy and over-reach by the state security structures. It contended that it is inappropriate to give the primary stewardship over

[455] *Ibid* at page 8.
[456] *Ibid* at page 8.
[457] I*bid* at page 9.
[458] *Ibid* at page 9.
[459] *Ibid* at page 9.
[460] *Ibid* at page 9.

cybersecurity to state security structures because this could lead to lack of transparency and abuse.[461] The appropriate stewardship should lie with the civil department, in this case the Ministry of Communications. Therefore, Chapters 10 and 11 should be redrafted in its entirety.[462]

The Minister of Justice and Correctional Services announced that a revised version of the Bill was to be laid before Parliament in 2017, however it failed to publish the comments of an analysis of their content which has received criticism.[463] In October 2018 the Department of Justice and Constitutional Development a notably different version of the Bill to the Portfolio Committee for Justice and Correctional Services. The biggest changed being the removal of part two of the Cybercrimes and Cybersecurity Bill 2017 which primarily related to cybersecurity.[464] The removal of the Cybersecurity part of the Bill has thus necessitated the renaming of the Bill to the Cybercrimes Bill.[465] This change came after an extensive public participation process where serious concerns regarding the states possible encroachment on the Right to freedom of expression, which is provided for in the Constitution, and the freedom of internet.[466] It was submitted that the approach by the South African legislature did not strike the right balance between the rights of an individual rights and freedoms and the interest pf the State in securing cyberspace and protecting the interest of the country, businesses and individuals.[467] Other changes to the Cybercrimes and Cybersecurity Bill include:

- The definition of 'unlawful' in the cybercrimes Bill has been more narrowly defined and has been aligned with the provisions of Protection of Personal Information, 2013.[468]
- The scope of the provisions relating to 'malicious communications' found in Part II of the Bill is now limited to data, messages of an intimate image without consent which threaten and individual to bodily harm and violence.[469]

---

[461]Ibid at page 18
[462] Ibid at page 19
[463] E Sutherland 'Governance of cybersecurity-The case of South Africa' (2017) 20 The African Journal of Information and Communication at 91.
[464] F Ameer-Mia and L Shacksnovis 'Cybercrimes Bill- a positive step towards the regulation of cybercrimes in South Africa' 13 February 2019, available at *https://www.cliffedekkerhofmeyr.com/en/news/publications/2019/technology/technology-alert-13-february-cybercrimes-bill-a-positive-step-towards-the-regulation-of-cybercrimes-in-south-africa.html* accessed on 25 June 2019.
[465] Cybercrimes Bill [B 6B – 2017] , available at http://pmg-assets.s3-website-eu-west-1.amazonaws.com/NA_bills2017_bill06B-2017.pdf accessed on 25 June 2019.
[466] F Ameer-Mia & L Shacksnovis (n 460 above).
[467] F Ameer-Mia & L Shacksnovis (n 460 above).
[468] Protection of Personal Information Act 4 of 2013.
[469] The Cybercrimes Bill *Ellipsis* (n 437 above).

- The Cybercrimes Bill has removed clauses that deal with critical infrastructure.[470]

Given the complex nature of cybercrimes, and the maritime cyber security threat environment, the cybercrimes Bill is a step in the right direction for South Africa. It will also prove to be an important piece of legislation in South Africa once it is assented to by the president of the Republic, in its final version. The Cybercrimes Bill has closed the gaps identified in the ECT Act and RICA. The new offences which were created by the Bill, which have been listed above, and which were difficult to prosecute under RICA and ECT, are now provided for in the Cybercrimes Bill. This is so, because the jurisdiction provisions that are provided for in the Bill are expensive. Further, the penalty provisions created by the bill, which include a maximum penalty of up to 15 years imprisonment will mean that cybercrime perpetrators are deterred from committing cyber transgression.

[470] *Ibid.*

CHAPTER 4:

CONCLUSION AND RECOMMENDATIONS

4.1. Conclusion

The maritime sector was shown to be susceptible to maritime cyber threats. Frew, BIMCO's Secretary General and CEO stated that "ignorance is no longer an option, as we are all rapidly realising".[471] The aim of this dissertation was to survey the extent of the legislative framework governing maritime cyber security and provide a road map on the development of the legal regime governing maritime cyber security both internationally and domestically, and then critically evaluate the implementation and enforceability of the legal regime to handle cyber security threats in the maritime industry. This dissertation has shown that the maritime sector has unique factors, including dynamic changes in maritime technology, social, economic and environmental elements that provide significant challenges to national infrastructure, and domestic and international security.[472]

It has been shown in chapter two of the dissertation that cyber transgressions are complex and cybercrimes know no border. Cyber criminals and victims of cybercrimes do not have to have had any physical encounter, but the unlawful act may have a "direct and immediate effect to the victim".[473] It is evident from the discussion on cyber threats to South Africa and international shipping companies, and the cost repercussions thereof, that cyber security is a priority for international maritime security and national security as South Africa is port state that relies on the efficient and effective functioning of all its ports. The rapid rate with which technological advancements and with which cyber criminal's conduct their transgressions has created a gap that needs to be regulated comprehensively. The study was of great importance as marine transportation is a critical international industry as provided for in chapter one. The prevalence of cyber security threats was shown to be increasing. The scale of the maritime cyber security incidents that were discussed in chapter two have shown that the world and more importantly shipping companies and port states like South Africa, need to be better equipped legally to deal with the above discussed maritime cyber vulnerabilities and threats. A stating point in addressing the issue of maritime cyber security, with a focus on a global approach to

---

[471] J Clark 'Cybercrime in the shipping industry' A presentation by Hill Dickinson LLP available at *https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf* accessed on 2 November 2018.
[472] K Tam and K D Jones 'Maritime cyber security policy: the scope and impact of evolving technology on international shipping' (2018) 3 (2) Journal of Cyber Policy at 161.
[473] Cassim (n 89 above) at 124.

the issue, may be in looking at the regulation of piracy on the high seas as it is similar to maritime cybercrimes as they too are borderless in nature.[474]

The current international, regional and domestic legal framework has been responsive rather than taking a more pre-emptive robust approach to creation of legislation. The SUA, ISPS Code and even the Tallinn Manual, are all examples of reactionary legal instruments. A global approach to addressing the threats, discussed in chapter two above, faced by the maritime industry is needed, as the nature of cybercrimes is transnational and borderless.

The legal framework, both international and domestic, governing maritime cyber security in South Africa was discussed in Chapter three of this dissertation. From the discussion in chapter three above, it has been established that a legal framework regulating maritime cyber security does exist internationally, however it is mostly on a state-by- state basis or perceived to be regionally focused.[475] The Budapest Convention is the first international treaty that has attempted to tackle this mammoth problem of cybersecurity vulnerabilities,[476] which is a step in the right direction and commendable. However international cooperation is needed in order to comply with International Conventions such as the ECC.[477] While the ECC aims at international cooperation in combating cybercrimes, no specific provisions are contacted in the convention for cooperation in securing these networks, which therefore makes implementation in practice difficult.[478] The buy-in from port states and the international community as a whole has proven to be very low. The current conventions in place that specifically regulate maritime cyber security, such as the ECCC, have not received the number of signatures needed to be a serious deterrence to cyber criminals. Further the countries that are signatories to the ECCC have not acceded to the Convention or ratified the convention. These factors make regulating the cyber domain of the maritime industry very difficult and prosecution of cyber offences, even more difficult.

The AU Convention on Cyber Security has gone a long way in prioritising the need for African states to address cyber security concerns. However there are great concerns as to whether the Convention had tackled the issues that lead to its delay in January 2014. These concerns include criticism on the over the content-related offences, as it was felt that it "imposed dangerously

[474] Gliha (n above 145) at 237.
[475] J Healey & H Pitts 'Applying international environmental legal norms to cyber statecraft' (2012) 8(2) ISJLP at 361.
[476] Marler (n 459 above) at 183.
[477] Cassim (n 89 above) at 126.
[478] *Ibid.*

broad limitations of free speech".[479] It should be remembered that South Africa has not signed the AU Convention on Cyber Security, the broad nature of the AU Convention on Cyber Security does not explicitly establish a comprehensive legal framework that South Africa can adopt into their legal framework. It is submitted that for a country like South Africa that already has existing laws that regulate cybercrimes and that has its own draft Bill that is being considered, the AU Convention on Cyber Security is too cumbersome[480] and would require the South African legislature to reconcile its domestic laws with that of the Convention. According to Cassim "African countries have been criticised for dealing inadequately with cybercrimes, as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure".[481]

In South Africa, a legal framework exists that partially regulates cyber security, though it is not specific to maritime cyber security. Maritime cyber transgressions can be read into the Acts discussed in Chapter 3.2 above as the wording of the Acts are broad enough to encompass maritime cyber security transgressions. The domestic regulatory provisions in South Africa are inadequate for these jurisdictional problems. The problem in South Africa is exacerbated by the fact that an unknown number of cybercrimes are undetected as they are not reported to relevant structures.[482] This detection problem is compounded by the fact that "African countries have long and permeable Borders"[483] Prosecution of cybercrimes is therefore not possible without adequate laws in place that procedurally and substantively criminalise cyber transgressions. The introduction of the Cybercrimes Bill will hopefully go a long way in eradicating these challenges. The bill seeks to introduce structure, as discussed in chapter three, that will be mandated to monitor cybercrimes, and take measures in deterring cybercrimes in the country. Political-will plays a major role in this regard, as more pressure needs to be placed on the legislature by interested industry stakeholders, and civil society, to enact laws that will protect the South African population and critical infrastructure such as ports and ships against cyber threats, as well as to ensure the current Cybercrimes Bill is assented to by the President of the Republic. There is also a great need to have the laws relating to cyber offences in South Africa to be consolidated in to one Act and harmonised. Currently one has to look at multiple pieces of legislation and interpret words broadly in order to deal with a cyber-attack, or to

[479] Tamarkin (n 350 above) at 4.
[480] *Ibid.*
[481] Cassim (n 89 above) 127.
[482] E Sutherland (n 463 above) at 84.
[483] Cassim (n 89 above) at 125.

prosecute cyber offences. It is submitted that the South African legislature seeking to regulate the maritime cyber security legal environment, should resist the overregulated the legal paradigm and make sure that all new legislation is in line with the constitution.

4.2. Recommendations:

In order for South Africa to address the challenges in providing a comprehensive regulatory framework for governing maritime cyber security, some amendments to the current legislative landscape are necessary. Currently there is no international instrument that comprehensively regulates maritime cyber security. The recommendations based on the findings of the study are as follows.

- A holistic and pre-emptive approach:

South African law makers, must avoid a reactionary approach to legislation creation, firstly because this reactionary approach could lead to legislation that does not fully address the issue of maritime cyber security threats or encroaches on existed constitutional provisions such as the right to freedom of expression and the right to privacy. Secondly, a reactionary approaches requires for a catastrophic event to have already have happened. This could have devastating economic consequence to the economy of the country.

- Comprehensive statute to address cyber security explicitly providing for maritime cybercrimes and security

As has been found no single statute enforce exists in South Africa to deal with cyber threats. The South Africa Legislature thus has to assent to the Cybercrimes Bill. The current version of the Bill saw drastic improvements to the cybercrimes section and took into consideration the submissions made by the different stakeholders that were discussed in Chapter 3 above. This was done by taking a narrow approach to definitions provided in section and addressing the concerns regarding freedom of expression. While the Bill still needs to be considered by the National Assembly[484] and awaiting comments from the public this appears to be a great stride for South Africa to deter and ensure a deterrence against cyber attacks.

Second, the Department of Justice and Constitutional Development needs to redraft or create a Bill that encompasses the cybersecurity section that was removed from the Cybercrimes Bill

[484] The Cybercrimes Bill Ellipsis (n 437 above).

with a great sense of urgency. This must be done while balance the need to enact progressive cyber legislation and ensuring that the State does not infringe on the existing rights of its people. This will also assist companies like those in the maritime shipping industry to become cyber secure, and implement cyber security strategies within their companies.

- Amendments to existing domestic instruments:

In the alternative to the recommendation provided above, relating to the enactment of a comprehensive legal instrument that explicitly deals with the regulation of cyber security and in effect maritime cyber security, the following recommendations are made:

- o Amendments to chapter thirteen of the ECT Act will need to be made to narrowly and more tightly define cyber transgression/offences.
- o Amendments to the ECT Act will need to be made to provide for stricter punishments for cyber transgression/offences which lead to a stronger deterrence of cybercrime. The current penalties in section 89 of ECT Act is not sufficient to deter cybercrime perpetrators, this more so when compared to the potential financial ramifications of a cyber-attack to, for example, to big shipping companies like Maersk or MSC.
- o Amendments to the ECT Act will need to be made to provide clarity on the effect of Section 15 of the ECT Act on the hearsay rule and authenticity rule,[485] which is binding in our legal system.

- South Africa should ratify the ECCC

Not only does the ECCC makes mandatory provisions for its signatories to enact robust procedural provision that regulate matters to jurisdiction, extradition and mutual assistance, it further provides national legislatures to criminalise a wide range of narrowly defined[486] cybercrimes that are provided for in chapter above. It is therefore important for South Africa to ratify this important legal convention so as to deter cyber criminal's form targeting South Africa.[487]

- Maritime Industry guidelines

---

[485] F Cassim 'Addressing the challenges posed by cybercrime : a South African perspective' (2010) 5(3) *Journal of International Commercial Law and Technology* at 121.
[486] Healey & H Pitts (n 66 above) at 361.
[487] Cassim (n above 485) at 123.

With regards to Marine shipping companies and Maritime Industry guidelines the following recommendations are made:

- Shipping companies and operators need to develop, implement and maintain the provisions and standards provided in the BIMCO Guidelines that relating to security of cyber systems on board a ship.
- Shipping operators and port officials to ensure that they have an approved safety management system as mandated by the ISM Code.
- Shipping operators and port officials need to take robust and comprehensive steps that ensure that their cyber risk management processes are in line with the ISM Code and ISPS Code provisions that deal with cyber security discussed in chapter three above.[488]
- Ship Security Plans and Safety Management Manuals on board ships should include cybersecurity controls, procedures and policies that are in line with the Regulations 2004, and other best practice guidelines and codes.

Lastly it is recommended that both domestic and international legislatures develop maritime cyber security regulatory framework that is based on international cooperation to ensure for a more secure maritime industry.

Considering the risk of financial loss and the fact that shipping companies are prone to face heavy fines or legal issues arising from cyber threats, it is equally important for shipping companies to lobby for rapid and robust change in the domestic and international legal framework governing cyber security incidents.

[488] A G Bermejo 'Maritime cybersecurity using ISPS and ISM Codes' available at *www.erawat.es* accessed on 28 June 2019 at 5.

BIBLIOGRAPHY

Primary Sources

Cases

Riverstone Meat Co. Pty. Ltd. V Lancashire Shipping Co. (The Muncaster Castle) [1961] 1 Lloyd's Rep. 57

S v Maseki 1981 4 SA 374 (T)

Mcfadden v Blue Star Line, [1905] 1 K.B. 697

Conventions

African Union Convention on Cyber security and Personal Data Protection

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

Convention on the International Maritime Organization

Charter of the United Nations and Statute of the International Court of Justice, 1945

International Convention on Civil and Political Rights

United Nations Convention on the Law of the Sea

Universal Declaration of Human Rights

The Convention on the High Seas

The Convention on Cyber Crimes

International Ship and Port Security Code, Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended.

Guidelines and Regulations

Guidelines on Cyber Security On Board Ships, published by BIMCO (Version 1.1- February 2016)

Tallinn Manual on the International Law Applicable To Cyber Warfare

National Institute of Standards and Technology (NIST) Cyber Security Framework Version 1.1 (16 April 2018)

The Guidelines on Cyber Security On board Ships, published by BIMCO (Version 2.0- June 2017)

South African Maritime Safety Authority Marine Notice No.12 of 2018

Department of Transport GN R.751 of GG 26488, 21/06/2004

South African Maritime Authority Marine Notice No. 12 of 2018

Resolutions

IMO Resolution A.358 (ix)

MSC.1/circ.1526

U.N.G.A. Resolution 40/61

IMO Resolution A. 924(22)

IMO Resolution A.741 (18)

Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems Annexure 10

IMO Assembly Resolution A.741 (18) The International Safety Management Code (1993)

The Hague-Visby Rules - The Hague Rules as Amended by the 1 Brussels Protocol 1968

Legislations

Electronic Communications and Transactions Act 25 of 2002

Regulation of Interception of Communication and Provision of Communication-Related Information Act 70 of 2002

The South African Carriage of Goods by Sea Act 1 of 1986

The National Ports Act 12 of 2005

The South African Merchant Shipping Act 57 of 1951

Merchant Shipping (Maritime Security) Regulations, 2004 GN R. 142 of GG 25997, 9 February 2004

National Prosecuting Authority Act 32 of 1998

Protection of Personal Information Act 4 of 2013

Electronic Communications and Transactions Act 25 of 2002

Cybercrimes and Cyber Security Bill B6- 2017

Cybercrimes and Cyber Security Bill GN 878 GG3961, 2/9/2015.

Foreign

Computer Misuse Act 1990 s 3(2)

United States Code

USA Patriot Act, 2002

Secondary Sources

Books

Hare, J *Shipping Law and Admiralty Jurisdiction in South Africa* 2 ed Cape Town: Juta (2009)

Kaag, WG & Moskoff, DB ‘Threats to global navigation’ in J DiRenzoIII… *et a*l, *Issues in Maritime Cyber Security* Washing DC: Westphalia Press, (2017)

Sturdevant L, ‘Cyber warfare and maritime security: A call for international regulation’ in J DiRenzoIII… *et al, Issues in Maritime Cyber Security* Washing DC: Westphalia Press, (2017)

McNicholas, M Maritime Cyber Security An Introduction Burlington: Butterworth-Heinemann, (2008)

Journal Articles

Abeyrantne, R 'New and emerging threats to maritime security' (2010) 18 (2) *Asia Pacific Law Review*.

Balkin, R 'The International Maritime Organisation and Maritime Security' (2006) 30(1&2) *Tulane Maritime Law Journal*.

Bambauer, DE 'Ghost in the Network' (2014) 162 *U. PA. L. REV.*

Besliu, D 'Cyber Terrorism- A growing threat in the field of cyber security' (2017) 6(2) *International Journal of Information Security and Cybercrime*.

Brailer, RB 'Protecting US ports with layered security measures for container ships' (2005) 185 *Military Law Review.*

Brenner, SW & Goodman, MD 'In Defence of Cyber of Cyber terrorism: An Argument for Anticipating Cyber-Attacks' (2002) *Journal of law, Technology and Policy.*

Bueger, C 'What is maritime security?' Marine Policy (2015) 53 *Elsevier*.

Cassim, F 'Addressing the challenges posed by cybercrime : a South African perspective' (2010) 5(3) *Journal of International Commercial Law and Technology.*

Cassim, F 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) 15 (2) *PER/PERLJ*.

Cassim, F 'Addressing the spectre of phishing: Are adequate measures in place to protect victims from phishing' (2014) 41 *Comparative and International Journal of South Africa.*

Cassim, F 'Formulating specialized legislation to address the growing spectre of cyber-crime: A comparative study' (2009) 12(4) *PER.*

Chandler, JA 'Security in cyberspace: Combating distributed denial of services attacks' 2003-2004 *University of Ottawa law and Technology Journal.*

Chung, JJ 'Critical infrastructure, cybersecurity and market failure' (2018)96 *Oregon Law Review.*

DeMuro, PR 'Keeping Internet pirates at bay: Ransomware negotiation on the health industry (2017) 14 *Nova Law Review*.

Dubner, BH 'Recent developments in the international law of the sea' (1999) 33(2) *The International Lawyer.*

Ebersohn, EJ 'Internet law: Port scanning and ping flooding- a legal perspective' (2003) 66 *Journal for Contemporary Roman Dutch law THTHR.*

Edwards, L 'Dawn of the death of distributed denial of services: How to kill zombies' (2006) 24 (23) *Cardozo Arts and Entertainment Law Journal.*

Eichensehr, KE 'The cyber-law of nations' (2015) 103 (317) *The Georgetown Law Journal.*

Foote, R 'Cybersecurity in the marine transportation sector: Protecting intellectual property to keep our ports, facilities and vessels safe from cyber threats' (2017) 8 *Cybris Intell. Prop. L. Rev*.

Garrie, DB, Blakely, AF, Armstrong, MJ 'Legal status of spyware' (2006) 59 *Federal Communications Law Journal.*

Gliha, D 'Maritime cybercrime-21st Century piracy' (2017) 20 *Annals Fac. L.U. Zenica*.

Goode, AC 'Cyberterorists : The identification and classification of non-state actors who engage in cyber hostilities' 2015 (223) *Military Law Review.*

Halberstam, M 'Terrorism on the high seas: The Achille Lauro, piracy and the IMO Convention on maritime security' (1998) 82(2) *The American Journal of International Law.*

Hampson, NCN 'Hactivism: A new breed of protest in a networked world' (2012) 35(2) *Boston College International and Comparative law Review.*

Hathaway, OA… et al 'The Law of cyber attack' (2012) 100(817) *California Law Review.*

Hardy, K 'Operation Titstorm: 'Hacktivism or cyberterrorism' (2010) 33(2) *UNSW Law Journal.*

Healey, J & Pitts, H 'Applying international environmental legal norms to cyber statecraft' (2012) 8(2) *ISJLP*.

Illig, AT 'Computer age protesting: Why hacktivism is a viable option for modern social activists' *Penn State Law Review* (2015) 119(4).

Kelly, B ‘Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cyber reform (2012) 92 (1663) *Boston University Law Review.*

Kilovaty, I ‘World Wide Web of exploitations- The case of peacetime cyber espionage operations under international law: Towards a contextual approach’ (2016) 18 *The Columbia Science and Technology Law Review.*

Knapp TM ‘Hacktivism –Political Dissent in the final Frontier (2015) 49(259) *New England Law Review*.

Mangena, D ‘Will legislation protect your virtual space? Discussing the draft cybercrime and cyber security bill’ *De Rebus* 2016.

Marler, SL ‘The Convention on cyber-crime: should the United States Ratify’ (2002) 37(1) *New England Law Review.*

Maskun, ‘Cyber security: rule of use internet safely’ (2013) 15 *Journal of Law, Policy and Globalization.*

Matsyshyn, AM ‘CYBER’ 2010 *BYU L. REV* .

Matwyshyn, AM ‘Cyber Harder’ (2018) 24 *B.U.J SCI & Tech. L.*

McCormack, T ‘The Sony and OPM double whammy: International law and cyber attacks’ (2015) 18 *SMU Science and Technology Law Review.*

McCurdy, JL ‘Computer Crimes’ (2010) 47 (287) *African Criminal Law Review*.

Mellor, J S C ‘Missing the boat: The legal and practical problems of the prevention of maritime terrorism’ (2002) 18(2) *American University International Law Review.*

Minnaar, A ‘Organised crime and the ‘new more sophisticated ‘criminals within the cybercrime environment: How ‘organised ‘are they in the traditional sense?’ (2016) 29 (2) *Acta Criminologica: Southern African Journal of Criminology.*

Moshirnia, A ‘Not security through obscurity: changing circumvention law to protect our democracy against cyber attacks’ (2018) 83 (4) *Brooklyn Law Review.*

O’Malley, G ‘Hacktivism: Cyber activism or cybercrime’ (2013) 16 *Trinity College Law Review*.

Oriji, UJ 'The African Union Convention on Cyber security: A regional response towards cyber stability' (2018) 12(2) *Masaryk University Journal of Law and Technology*.

Plant, G 'The Convention for the Suppression of Unlawful Acts against the Safety of maritime Navigation' (1990) 39 *International and Comparative Law Quarterly.*

Reimer, DM 'Judicial and Legislative Responses to Computer crimes' 1986 *Insurance Counsel Journal*.

Schmidt, AV 'Cyberterrorism: Combating the aviation Industry's vulnerability to cyber-attack' (2016) 39(1) *Suffolk Transnational Law Review.*

Snail, S 'Cyber-crime in South Africa- Hacking, cracking and other unlawful online activities' 2009 (1) *Journal of Information, Law & Technology.*

Stahl, W M 'The Uncharted waters of Cyber space: Applying the Principles of the International Maritime Law to the Problem of Cyber '(2011) 40 (247) *GA. J.INT'L & COMP.L.*

Sutherland, E 'Governance of cybersecurity-The case of South Africa' (2017) 20 The *African Journal of Information and Communication*.

Tafoya, WL 'Cyber Terror' (2011) 1 *FBI Law Enforcement Bulletin.*

Tam, K & Jones, K D 'Maritime cyber security policy: the scope and impact of evolving technology on international shipping' (2018) 3 (2) *Journal of Cyber Policy*

Tsuchiya, M 'Japan's response to cyber threats in the surveillance age' (2015-2016) 7 *Section Hall Journal of Diplomacy and International Relation.*

Tully, S 'Protecting Australian cyberspace: Are our international lawyers ready?' (2012) 19 *Australian International Law Journal* 50.

United Nations Economic Commission for Africa Policy Brief NTIS/002/2014 'Tackling the challenges of cyber security in Africa'.

Van Niekerk, B 'An analysis of cyber incidents in South Africa' (2017) 20 *The African Journal of Information and Communication*.

Watkins, J 'No good deed goes unpunished: The duties held by malware researchers, penetration testers and "white hat" hackers' (2018) 19(2) *Minn J.L.SCI.& Tech*.

Weber, AM 'The Council of Europe's Convention on Cybercrime' (2003) 18(1) *Berkeley Technology Law Journal*.

Weissbrodt, D 'Cyber Conflict, Cyber Crime and Cyber Espionage' (2013) 22 (2) *Minnesota Journal of International Law*.

Yang, D W & Hoffstadt, B M 'Countering the Cyber-crime Threat' (2006) 43 (201) *American Criminal Law Review*.

Internet Sources

Ablon, L 'Social engineering explained: The human element in cyber attacks' (20 October 2015) available at https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html, accessed on 11 November 2018.

'Africa Gearing up' PWC report available at h*ttps://www.pwc.com/gx/en/transportation-logistics/publications/africa-infrastructure-investment/assets/south-africa.pdf*, accessed on 30 November 2018.

Ameer-Mia, F & Pienaar C 'South Africa: Cybersecurity 2019' available on *https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa* accessed on 17 June 2019.

Ameer-Mia, F and Shacksnovis, L 'Cybercrimes Bill- a positive step towards the regulation of cybercrimes in South Africa' (13 February 2019) available at *https://www.cliffedekkerhofmeyr.com/en/news/publications/2019/technology/technology-alert-13-february-cybercrimes-bill-a-positive-step-towards-the-regulation-of-cybercrimes-in-south-africa.html* accessed on 25 June 2019.

'Anonymity of a of an attack: Zombie zero' *TrapX Research Labs* 1 March 2017, availablejhat http://trapx.com/wpcontent/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf ,accessed on 17 November 2018.

Bergen, PL 'September 11 attacks' (15 November 2018) available at *https://www.britannica.com/event/September-11-attacks* , accessed on 27 November 2018.

Bowline Report 'Cyber-Security Threats to the Maritime Industry' available at *http://www.mile.org.za/QuickLinks/News/1st%20Annual%20Maritime%20Summit%20Presentations/Day%201.6-Carl%20Uys-Cyber%20Security%20Threats.pdf*, accessed on 5 November 2018.

Boyens, J… *et al* ‘Supply chain risk management practices for federal information systems and organisations’ (2015) *NIST Special Publication* 800-161 available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf* accessed on 20 November 2018.

Boyes, H & Isbell, R ‘Code of Practice: Cyber security for ships’ (2017) *Institution of Engineering and Technology, London, United Kingdom,* Available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf* accessed on 3 November 2018.

Brickey, J ‘Defining cyberterrorisim: capturing a broad range of activities in cyber space’ *Center for Security Studies* (2 October 2018) available on *http://www.css.ethz.ch/en/services/digital-library/articles/article.html/153108/pdf,* accessed on 20 November 2018.

Cannols, B & Ghafarian, A ‘hacking experiment by using USB rubber ducky scripting’ *Systemic, Cybernetics And Informatics* (2017) 15 (2) at 68, available at *http://www.iiisci.org/journal/CV$/sci/pdfs/ZA340MX17.pdf*, accessed on 12 February 2019.

Cassim, F ‘Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role player” available at https://core.ac.uk/download/pdf/79170924.pdf accessed on 30 May 2019.

Centre for Constitutional Right “CONCISE SUBMISSION ON THE CYBERCRIMES AND CYBERSECURITY BILL [B 6-2017]” 10 August 2017 available at https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_CFCR.pdf, accessed on 23 June 2019.

Clark, J ‘Cybercrime in the shipping industry’ A presentation by Hill Dickinson LLP available at *https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf* accessed on 2 November 2018.

‘Consequences to seaport operations from malicious cyber activity’ *Home Land Security National Protection and Programs Directorate* (3 March 2016), available at https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf, accessed on 17 November 2018.

Cosper, A 'History & Evolution of Computers' *Techwalla* available at *https://www.techwalla.com/articles/history-evolution-of-computers*, accessed on 17 April 2019.

'Cyber-attack' *Merriam Webster*, available at *https://www.merriam-webster.com/dictionary/cyberattack*, accessed on 11 November 2018.

"Cybercrime, cybersecurity, and Internet Freedom" Right2Know Campaign submission on the Cybercrimes and Cybersecurity Bill, 10 August 2017, available at https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_R2K.pdf , accessed on 23 June 2019.

CyberKeel, 'Maritime cyber security: Virtual Pirates at large on the cyber seas' (2014),available at https://docplayer.net/19421672-Maritime-cyber-risks-virtual-pirates-at-large-on-the-cyber-seas-10-15-2014.htm,l,accessed on 17 November 2018.

Department of International Relations and Cooperation website, available at http://www.dirco.gov.za/foreign/Multilateral/inter/imo.htm, accessed on 27 November 2018.

DiRenzo,J 'The little known challenges of maritime cyber security' available at *http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf* accessed on 3 June 2019.

Explanatory Report to the Convention on Cybercrime, Budapest 23.XI.2001, European Treaty Series – No.185

Elkind, P 'Inside the Hack of the Century' (1 July 2015) Fortune available at *http://fortune.com/sony-hack-part-1/* accessed on 7 November 2018.

Fittion, O…et al 'The future of maritime cyber security' (2015) available at *http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf* , accessed on 2 November 2018.

Forbes, VL 'The global maritime industry remains unprepared for future cybersecurity challenges' 21 August 2018, available at *http://www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/* , accessed on 8 June 2019.

Garcia-Parez A, Thurlbeck M, How Eddie 'Towards cyber security readiness in the maritime industry: A knowledge –based approach' available at *https://pdfs.semanticscholar.org/0bca/56d7f4c56899540d3ee9180ee6c8557a813b.pdf* , accessed on 7 November 2018.

Gereda, SL 'Electronic Communications and Transactions Act' available at *https://www.wits.ac.za/media/migration/files/cs-38933-fix/migrated-pdf/pdfs-5/telelaw12.pdf* , accessed on 30 November 2018.

Gercke, M 'Understanding cybercrime: phenomena, challenges and legal response' *The ITU Publication*, available at *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*, accessed on 28 May 2019.

Greenberg, A 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (22 August 2018) WIRED available at *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/* accessed on 13 May 2019.

'How a cyber-attack transformed Estonia' *BBC New online* (27 April 2017) available at *https://www.bbc.com/news/39655415*, accessed on 5 November 2018

Ihmor, S & Muller, C 'Monitoring and Remote Control for MTU Ship Propulsion Systems' (2014) available at *https://www.mtu-online.com/fileadmin/fm-dam/mtu-global/technical-info/white-papers/3100701_MTU_General_WhitePaper_BlueVisionNG_2014.pdf* , accessed on 20 May 2019.

IMO maritime security policy -Background paper EEF.IO/3/08 (23 January 2008)

International Maritime Organisation 'Maritime security' available at *http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx*, accessed on 27 November 2018.

Jensen 'challenges in maritime cyber-resilience' 2015 *Technology Innovation Management Review*, (April 2015) available at

https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=35 accessed on 28 May 2019.

Kelion, L ' Ships hack 'risk chaos in English Channel' '*BBC News Online* (7 June 2018) available at *https://www.bbc.com/news/technology-44397872*, accessed on 19 February 2019.

List of signatories of the AU Cyber Convention available on *https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf* accessed on 7 December 2018.

'Maersk says global IT breakdown caused by cyber-attack' *Reuters online*, 27 June 2018 available at *https://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1NO*, accessed on 5 November 2018.

'Malware' in *Merriam Webster Online Dictionary* available at https://www.merriam-webster.com/dictionary/malware,accessed on 13 May 2019.

Martin, K & Hopcraft, R 'Why 50,00 ships are so vulnerable to cyber attacks' *The Conversation* (14 June 2018) available at *https://phys.org/news/2018-06-ships-vulnerable-cyberattacks.html* , accessed on 28 May 2019.

Media Briefing Statement by the Deputy Minister of Justice and Constitutional Development, the Honorable JH Jeffery, MP on the new proposed Cybercrime and cyber security Bill (19 January 2017) available at *http://www.justice.gov.za/m_speeches/2017/20170119-CyberCrimeBillBriefing.html* accessed on 17 June 2019

Mehlman, M 'How CFOs Can Mitigate the Risk of Ransomware' (31 May 20018*) Tax Executive* available at *https://taxexecutive.org/how-cfos-can-mitigate-the-risk-of-ransomware/*, accessed on 23 February 2019.

Montgomery, M 'New BIMCO cyber security guidelines' HFW Briefings (July 2017), available at *http://www.hfw.com/New-BIMCO-Guidelines-July-2017* , accessed on 28 November 2018.

'National Strategy to secure cyberspace' (2013) *Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program*, available at https://www-heinonline-org.ukzn.idm.oclc.org/HOL/Page?public=true&handle=hein.beal/nastsecyb0001&div=10&start_page=27&collection=beal&set_as_cursor=31&men_tab=srchresults ,accessed on 18 November 2018.

'Net losses: Estimating the Global cost of cybercrime. Economic impact of Cybercrime II' *Center for Strategic and International Studies* available at *https://collabra.email/wp-*

content/uploads/2015/04/rp-economic-impact-cybercrime-2014.pdf, accessed on 6 November 2018.

Oriji, UJ 'The Defects on the Draft African Union Convention on the establishment of a credible legal framework for cyber security' available at *https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6780881*, accessed 6 November 2018.

Parms J '10 Common social engineering tactics used by attackers' (22 February 2015) available at *https://www.business.com/articles/10-common-social-engineering-tactics-used-by-attackers/*,accessed on 11 November 2018.

Perlroth, N…*et al* 'Cyberattack hits Ukraine and then spreads internationally' *The New York Times Online* (27 June 2017) available at *http://www.vis-am.ch/uploads/allegati/Cyberattack_Hits_Ukraine_Then_Spreads_Internationally_-_The_New_York_Times.pdf*, accessed on 15 February 2019.

Reilly, RJ 'Zoe Lofgren introduces 'Aaron's Law to honour Swartz on Reddit' *Huffington Post* (15 January 2013) available on, https://www.huffingtonpost.com/2013/01/15/zoe-lofgren-aarons-law-swartz_n_2483770.html, accessed on 25 November 2018.

'Saaff develops container inspection database' *Freight &Trading Weekly* (7 July 2017) (no.2253),available at http://storage.news.nowmedia.co.za/medialibrary/Feature/6319/FTW-7-July2017.pdf, accessed on 21 November 2018.

SAHRC Submission – Cybercrimes and Cybersecurity Bill, August 2017, available at https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_SAHRC.pdf accessed on 23 June 2019.

Seidman, B 'Internet activist charged with hacking into MIT network' *The Daily Need* (22 July 2011) available at *https://www.pbs.org/wnet/need-to-know/the-daily-need/internet-activist-charged-with-hacking-into-mit-network/*, accessed on 25 November 2018.

Shactman, N '26 Years after Gibson, Pentagon defines 'cyberspace' *WIRED* available at *https://www.wired.com/2008/05/pentagon-define/* accessed on 22 May 2019.

'Software' in *Merriam Webster Online Dictionary* available at https://www.merriam-webster.com/dictionary/malware,accessed on 13 May 2019.

Stahl, W M 'The Uncharted waters of Cyber space: Applying the Principles of the International Maritime Law to the Problem of Cyber '(2011) 40 (247) *GA. J.INT'L & COMP.L.*

Summary Of Written Submissions And Responses Thereto: Cybercrimes And Cybersecurity Bill [B 6 - 2017] available at *https://www.ellipsis.co.za/wp-content/uploads/2017/09/171107Part_A.pdf* accessed on 23 June 2018.

Sutherland, E 'Governance of cybersecurity-The case of South Africa' (2017) 20 The *African Journal of Information and Communication*.

Tafoya, WL 'Cyber Terror' (2011) 1 *FBI Law Enforcement Bulletin.*

Tam, K & Jones, K D 'Maritime cyber security policy: the scope and impact of evolving technology on international shipping' (2018) 3 (2) *Journal of Cyber Policy*

Tamarkin, E 'The AU's cyber-crime response: A positive start, but substantial challenges ahead' (January 2015) Policy Brief 73 Institute for Security Studies available at *https://www.files.ethz.ch/isn/187564/PolBrief73_cybercrime.pdf* accessed on 7 December 2018.

Thompson, C 'Hacktivism: Civil disobedience or cybercrime?' ProPublica (18 January 2013) available at https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime, accessed on 25 November 2018.

The Cybercrimes Bill Ellipsis available at *https://www.ellipsis.co.za/cybercrimes-and-cybersecurity-bill/* , accessed on 17 June 2019

The 'icefog' Apt :A tale of cloak and three daggers' *Kaspersky Lab Global Research and Analysis Team* (2013) available at https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf, accessed on 17 November 2018.

'The risk of cyber-attack to the maritime sector' Marsh and McLennan Companies (July 2014)hatlavailablejat https://www.ahcusa.org/uploads/2/1/9/8/21985670/the_risk_of_cyber-attack_to_the_maritime_sector-07-2014.pdf , accessed on 17 November 2018.

Torbati, Y & Saul, J 'Iran's top cargo shipping line says sanctions damage mounting' *Reuters* (22 October 2012) available at https://www.reuters.com/article/us-iran-sanctions-shipping/irans-top-cargo-shipping-line-says-sanctions-damage-mounting-idUSBRE89L10X20121022 , accessed on 16 November 2018.

Transnet Port Terminals Report (2018) available at *https://www.transnet.net/InvestorRelations/AR2018/TPT.pdf*, accessed on 21 November 2018.

Tsuchiya, M 'Japan's response to cyber threats in the surveillance age' (2015-2016) 7 *Section Hall Journal of Diplomacy and International Relation.*

Tully, S 'Protecting Australian cyberspace: Are our international lawyers ready?' (2012) 19 *Australian International Law Journal* 50.

UNCTAD Handbook of Statistics (2017) Maritime transport, available at *https://unctad.org/en/PublicationChapters/tdstat42_FS13_en.pdf*, accessed on 20 November 2018.

United Nations Economic Commission for Africa Policy Brief NTIS/002/2014 'Tackling the challenges of cyber security in Africa'.

United States Department of Homeland Security 'Understanding denial-of service attacks' available at *https://www.us-cert.gov/ncas/tips/ST04-015*, accessed on 12 November 2018.

Van Niekerk, B 'An analysis of cyber incidents in South Africa' (2017) 20 *The African Journal of Information and Communication*.

Watkins, J 'No good deed goes unpunished: The duties held by malware researchers, penetration testers and "white hat" hackers' (2018) 19(2) *Minn J.L.SCI.& Tech*.

Weber, AM 'The Council of Europe's Convention on Cybercrime' (2003) 18(1) *Berkeley Technology Law Journal*.

Webster's New World College Dictionary (201) 4th Edition.

Weissbrodt, D 'Cyber Conflict, Cyber Crime and Cyber Espionage' (2013) 22 (2) *Minnesota Journal of International Law.*

'When trade and security clash' *The Economist* (4 April 2002) available at https://www.economist.com/special-report/2002/04/04/when-trade-and-security-clash, accessed on 22 November 2018.

'Who is Edward Snowden, the man who spilled the NSA's secrets?' *NBC New online* (31 May 2014) available at *https://www.nbcnews.com/feature/edward-snowden-interview/who-edward-snowden-man-who-spilled-nsas-secrets-n114861*, accessed on 18 November 2018.

‘Who was behind the behind the Estonia cyber-attack?’(07 December 2010) *Foreign Policy* available at *https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/* accessed on 5 November 2018.

Yang, D W & Hoffstadt, B M ‘Countering the Cyber-crime Threat’ (2006) 43 (201) *American Criminal Law Review.*

Zhao, J …*et al* ‘A fleet technical condition management system for connected ships’ (2013) 33 *The Italian Association of Chemical Engineering Online* available at *https://www.aidic.it/cet/13/33/134.pdf* accessed on 20 April 2019.

Theses

Hayes, CR *Maritime Cyber Security: The future of National Security* (Master’s thesis, Naval Postgraduate School, 2016).

Kassem, AH *The Legal Aspects of Seaworthiness: Current Law and Development* (unpublished PHD, University of Wales, 2006)

Langouvardou, S *Maritime Cyber Security: Concepts, Problems and Models* (Master’s Thesis, Technical University of Denmark, 2018).

Naidu A comparative Analysis of the Carriers Liability under the Hague Visby and Rotterdam Rules (unpublished LLM thesis, University of KwaZulu- Natal 2016, 25)

Silgado,DM *Cyber-Attacks; Digital Threat Reality Affecting The Maritime Industry* (unpublished Master of Science thesis, World Maritime University, Sweden 2018)

UNIVERSITY OF ™
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

18 March 2020

Ms Sibusisiwe Nothando Mthembu (212509261)
School of Law
Howard College Campus

Dear Ms Mthembu,

Protocol reference number: HSS/0734/016M

Project title: Navigating the complex maritime cyber regime: A review of the international and domestic regulatory framework on maritime cyber security.

Approval Notification – Amendment Application

This letter serves to notify you that your application and request for an amendment received on 04 March 2020 has now been approved as follows:

- Change in title

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

Best wishes for the successful completion of your research protocol.

Yours faithfully

....

Professor Urmilla Bob
University Dean of Research

/ss

cc Supervisor: Vishal Surban
cc. Academic Leader Research: Professor Donrich Thaldar
cc. School Administrator: Mr Pradeep Ramsewak