UNIVERSITY of KWAZULU-NATAL
COLLEGE OF LAW AND MANAGEMENT STUDIES, SCHOOL OF LAW
Unit of Maritime Law and Maritime Studies

Unmanned and Autonomous Ships and Cyber Piracy: An Analysis of International and National Regulatory Measures

Emily Lewis
Student number: 219095768

A dissertation submitted in fulfilment of the requirements for the degree of:
Master of Laws (LL.M.) in Maritime Law at the University of KwaZulu-Natal

2021

Supervisor: Dr. Vishal Surbun

PRELIMINARIES

REGISTER OF CONTENTS

DECLARATION OF ORIGINALITY

I, Emily Lewis declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.

B. This dissertation has not been submitted for any degree or examination at any other university.

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

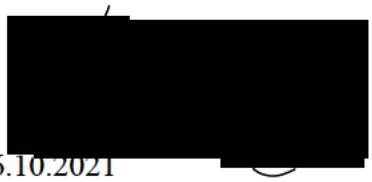
D. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

    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.

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

F. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the sources being detailed in the dissertation/thesis and in the References sections.

Signed: 

Date: 26.10.2021

To my Parents and my Pirate

ACKNOWLEDGMENTS

The submission of this thesis marks the end of an extraordinary experience which was to study in a foreign country. First of all, I would like to express my gratitude to my supervisor Dr. Vishal Surbun for his support, useful comments, remarks, and patience through the learning process of this master's thesis. I also want to thank Prof. Trevor Jones for his precious time and for putting me in touch with Dr. Surbun. And last but not least, a very special thank you to Mr. Pradeep Ramsewak who led me through the registration process like a star and always offered his help and support.

LIST OF ABBREVIATIONS

AAWA	Advanced Autonomous Waterborne Application Initiative
AD	Anno Domini
BC	Before Christ
BGH	Bundesgerichtshof (German Supreme Court)
BIMCO	Baltic and Maritime Council
BKA	Bundeskriminalamt (German Federal Criminal Police Office)
BPolG	Bundespolizeigesetz (German Federal Police Act)
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
BSIG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (German Act on Federal Office for Information Security)
BSI-KritisV	Verordnung zur Bestimmung kritischer Infrastrukturen (German Ordinance to Regulate Critical Infrastructures)
CC	Centre Crew
COLREG	Convention on the International Regulations for Preventing Collisions at Sea
ECT	Electronic Communication and Transactions Act
EUR	Euro
FAL	Convention on Facilitation of International Maritime Traffic
GG	Grundgestz (German Constitution)
GVG	Gerichtsverfassungsgesetz (German Courts Constitution Act)
ICC	International Criminal Court
ICJ	International Court of Justice
ICT	Information and Communication Technology
IMO	International Maritime Organisation
ISM	International Safety Management Code for the Safe Operation of Ships and Pollution Prevention
ISPS	International Ship and Port Facility Code
IT	Information Technology
ITLOS	International Tribunal for the Law of the Sea
LKA	Landeskriminalamt (German Federal State Criminal Police Office)
MARPOL	International Convention for the Prevention of Pollution from Ships
MIR	Maritime Industry Report
MSA	Merchant Shipping Act
MSR	Merchant Shipping (Maritime Security) Regulations
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
OT	Operational Technology
POCDA-TARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act
SAPS	South African Police Service
SCC	Shore Control Centre
SchSG	Schiffssicherheitsgesetz (German Ship Safety Act)
SchSV	Schiffssicherheitsverordnung (German Ship Safety Ordinance)
SeeAufG	Seeaufgabengesetz (German Maritime Labour Act)
SeeArbG	Seearbeitsgesetz (German Maritime Labour Act)

SeeFSichV	Verordnung über die Sicherheit der Seefahrt der Bundesrepublik Deutschland (Ordinance on the Safety of Maritime Navigation oft he Federal Republic of Germany)
SMM	Shipbuilding Machinery and Maritime Technology
SOLAS	International Convention for the Safety of Life at Sea
SRA	Ship Registration Act
SSO	Ship Security Officer
StGB	Strafgesetzbuch (German Criminal Act)
STP	Special Trade Passenger Agreement
StPO	Strafprozessordnung (German Code of Criminal Procedure)
SUA	Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
SUG	Seesicherheits-Untersuchungsgesetz (German Maritime Safety Investigation Act)
TEU	Twenty-Foot Equivalent Unit
U.K.	United Kingdom
UNCLOS	United Nation Convention on the Law of the Sea
U.S.	United States of America
USD	United States Dollar
ZAR	South African Rand

1 INTRODUCTION

1.1 Opening Remarks

'Autonomous shipping is the future of the maritime industry. As disruptive as the smartphone, the smart ship will revolutionise the landscape of ship design and operations.'[1]

Mikael Mäkinen, President of Rolls-Royce Marine

The idea of unmanned, autonomous, or intelligent self-steered machines and systems has fascinated humankind ever since the first computers existed. Countless books and movies portray a future world supported or even run by cyber intelligence including unmanned vehicles and autonomous robots. But what always used to sound like science fiction has already become reality in many cases. Fully automatic subway systems have been around for many years already. In the German city of Nürnberg, the passengers have been using the driverless metro system daily for over ten years now.[2] All operations are automatic: driving and stopping the train, opening and closing the doors, even an immediate stop in a safe location when a breakdown occurs.[3] Autonomous driving in rail transport is already taking place regularly not only in Germany but throughout Europe.[4] When it comes to self-driving cars, the company Waymo takes the lead in the global competition.[5] In 2017, the company was the first to put self-driving cars on United States (U.S.) roads without a safety driver overlooking the operation.[6] According to the company, as of March 2018, Waymo´s self-driving technology had driven more than five million miles (over eight million kilometres[7]) on public roads.[8] In October 2018, Waymo was even the first company to receive a permit for fully driverless cars, that allows day and night testing on public roads and highways in the U.S. state of California.[9] Even the use of unmanned submarines is no longer a dream of the future. The aircraft manufacturer Boeing, for example, sent its autonomous, unmanned, undersea vehicle, the Echo Voyager, on its first test drive into

[1] President of Rolls-Royce Marine Mikael Mäkinen at a conference presenting the Rolls-Royce's Advanced Autonomous Waterborne Applications Initiative in Helsinki in April 2016.
[2] Stadt Nürnberg *'Echtes Pionierstück: Nürnbergs automatische U-Bahn'* available at *https://www.nuernberg.de/internet/digitales_nuernberg/automatische_ubahn_nuernberg.html*, accessed on 21 January 2021.
[3] Ibid.
[4] UITP Advancing Public Transport *'Statistics Brief - World Report on Metro Automation - July 2016'* (July 2016) 1.
[5] A Townsend *'Ghost Road – Beyond the Driverless Car'* (2020) 5.
[6] Waymo LLC *'Our Journey'* available at *https://waymo.com/journey/*, accessed on 21 January 2021.
[7] 1 mile is equivalent to approximately 1.61 kilometres.
[8] Waymo LLC (note 6 above).
[9] Ibid.

the sea in 2017.[10] Off the coast of the U.S. state of California, the approximately 15-meter-long autonomous vessel went on its first test drive.[11] It is designed to stay underwater for months at a time and to move completely autonomously.[12] Unmanned and autonomous technology has already reached the modern maritime shipping industry as well. At this moment, multiple projects are researching and testing unmanned and autonomous onboard ship technology worldwide. The most prominent example of an unmanned and autonomous vessel in the shipping industry is the MV Yara Birkeland which will be the world´s first fully autonomous container ship.[13] The Norwegian company Yara commissioned the building of the ship and is planning to finish its construction this year.[14] It will gradually move from manned operations to fully autonomous and unmanned operations.[15] By 2022, the technology of this vessel is supposed to be so far advanced that it operates entirely autonomously.[16] The 80-meter-long ship will have a capacity of 120 twenty-foot equivalent units (TEUs)[17]. The vessel will navigate on two routes along Norway's coastline, between the cities Herøya and Brevik and between the cities Herøya and Larvik carrying chemicals and fertiliser.[18] The Norwegian Government strongly supports the project and gave about a third of the total costs towards the construction of the ship.[19] But the government does not only support the project financially. The Norwegian maritime authorities have publicly stated that they want Norway to be the first maritime nation deploying a fully autonomous vessel.[20] But not only Norway is interested in the topic. All over the world private companies but also countries and their governments as well as international organisations are interested in the topic of onboard unmanned and autonomous navigation systems:

[10] Boeing '*Echo Voyager Overview'* available at *https://www.boeing.com/defense/autonomous-systems/echo-voyager/index.page*, accessed on 21 January 2021.
[11] D Hambling *'WE: ROBOT The robots that already rule our world'* (2016) 138.
[12] Ibid.
[13] K Desmond *'Electric Boats and Ships: A History'* (2017) 223.
[14] Ibid.
[15] Yara '*Yara selects Norwegian shipbuilder VARD for zero-emission vessel Yara Birkeland'* available at *https://www.yara.com/corporate-releases/yara-selects-norwegian-shipbuilder-vard-for-zero-emission-vessel-yara-birkeland/*, accessed on 21 January 2021.
[16] S Pribyl, A Weigel *'Autonomous Vessels: How an Emerging Disruptive technology Is Poised to Impact the Maritime Industry Much Sooner than Anticipated'* RAIL: The Journal of Robotics, Artificial Intelligence & Law, Vol. 1, Issue 1 (January-February 2018), 18.
[17] The abbreviation TEU describes a unit of cargo capacity based on the volume of a 20-foot-long (6.1 meters) intermodal container.
[18] *'Yara Birkeland Autonomous Container Vessel'* available at *https://www.ship-technology.com/projects/yara-birkeland-autonomous-container-vessel/*, accessed on 21 January 2021.
[19] Ibid.
[20] *'Norway Provides Grant for Construction of Yara Birkeland'* (29 September 2017) available at *https://worldmaritimenews.com/archives/231229/norway-provides-grant-for-construction-of-yara-birkeland/*, accessed on 21 January 2021.

The Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) project is a research project which is co-funded by the European Commission under its seventh framework programme with EUR 2,9 million (over ZAR 58 million[21]) (total budget EUR 3,8 million[22], over ZAR 62 million).[23] Its consortium consists of eight partners located in five European countries: Germany (German partners: Fraunhofer CVL, Hochschule Wismar and Marine Soft), Sweden (Swedish partner: Chalmers University of Technology), Norway (Norwegian partners: Marintek and Aptomar AS), Iceland (Icelandic partner: Marorka ehf), and Ireland (Irish partner: University College Cork).[24] Together they research in maritime autonomous and unmanned ships, which the project defines as a vessel primarily guided by automated on-board decision systems but controlled by a remote operator in the shore control centre (SCC). The MUNIN project defined multiple essential concepts such as an autonomous navigation system that is capable of following a predefined route and an advanced sensor module that is used to fulfil lookout duties on board the ship.[25] The project also carried out a legal feasibility assessment on the operation of an unmanned vessel.[26] Their legal and liability in-depth assessment deals with the navigation and the human lookout, the manning as well as some liability issues and insurance questions. Even though the MUNIN project also concerns about the risk of cyber-attacks they only state that 'software systems, as well as ships, can be designed providing a very high resilience against digital (...) attacks.'[27]

The Advanced Autonomous Waterborne Application (AAWA) initiative is a EUR 6.6 million (over ZAR 108 million) research project funded by the Finnish Funding Agency for Technology and Innovation (Tekes).[28] Twelve partners including the aerospace and motor vehicle manufacturer Rolls-Royce work together on technologies to realise remote-controlled and autonomous shipping for commercial use. Rolls-Royce states that a vessel with a reduced crew and remote support will be able to launch by the end of 2020, remote-controlled unmanned coastal vessels by 2025, remote-controlled unmanned ocean going-ships by 2030, and fully unmanned ocean-going ships by 2035.[29] In particular, the AAWA initiative focuses on what technology is needed for unmanned ships, on how the vessels can become at least as safe as common ships, and on

[21] EUR 1 is equivalent to approximately ZAR 18.01 (Exchange rate on 21 January 2021).
[22] European Commission Project ID: 314286, Funded under: FP7-TRANSPORT.
[23] C Soares *'Progress in Maritime Technology and Engineering'* (2018) 111.
[24] MUNIN *'The MUNIN Consortium'* (2016) available at *http://www.unmanned-ship.org/munin/partner/*, accessed on 21 January 2021.
[25] MUNIN *'Research in maritime autonomous systems project results and technology potentials'* (2019).
[26] Ibid.
[27] Ibid.
[28] AAWA *'Remote and autonomous Ships - The next steps'* (2016) 5.
[29] Ibid.

what incentives ship owners will require to invest in the new technology. The initiative does not only focus on the technical aspects but the legal side as well. The focus of their research is on international regulations. However, their point of view is mostly from the construction site of things. They mainly stress the question of how the technology of unmanned vessels would have to be designed to suit the regulations. For example, they are looking at what camera they would have to use to provide a proper lookout.[30] The initiative also sees a high risk of cyber-attacks and therefore dedicates a short chapter in their final documentation to this issue. Realising that the concerns on cyber security are further increasing in the maritime society as the technology develops and potential attackers get more skilful over time, they state that protection against cyber threats would 'call for the elimination of vulnerabilities in the information and communication technology system (ICT)[31] infrastructure.'[32] However, the AAWA initiative focuses on technical protection from cyber risks only.

Another project is called ONE SEA - Autonomous Maritime Ecosystems. It is a Finnish collaboration that was founded in 2016 to lead the way towards an operating autonomous maritime ecosystem by 2025. At the moment ONE SEA has got eleven mostly Scandinavian partners but was recently joined by the Japanese shipping and logistic company NYK as well. ONE SEA opened the first globally available autonomous maritime test area (Jaakonmeri Test Area) on the west coast of Finland. This area is controlled and managed by its founding partner DIMECC Ltd. and is accessible to anyone who wishes to test autonomous vessels and technology related to the topic.[33] ONE SEA states that a fully unmanned and remote-controlled vessel (unmanned with special approval) can be launched by the end of 2020 and a fully autonomous ship for commercial traffic can be launched by 2025.[34] ONE SEA itself did not present any thoughts on the legal framework. They mainly focus on technological questions. However, one of their advisory board members is a Professor at the Scandinavian Institute of Maritime Law who participates in the AAWA research project.[35]

[30] Ibid.
[31] An information and communication technology system is a set-up that consists of hardware, software, and data and commonly includes communication technology such as the internet.
[32] AAWA (note 28 above).
[33] ONE SEA '*Test Area'* (2017) available at *https://www.oneseaecosystem.net/test-area/*, accessed on 21 January 2021.
[34] ONE SEA '*Roadmap'* (2017) available at *https://www.oneseaecosystem.net/roadmap/*, accessed on 21 January 2021.
[35] ONE SEA '*Advisory Board'* (2017) available *at https://www.oneseaecosystem.net/about/advisory-board/*, accessed on 21 January 2021.

A consequence of the use of autonomous and unmanned ships, especially when it comes to container ships, will be that they will be moving goods across the oceans to their destinations faster, more eco-friendly, and more cost-effective than ever before. The technology for autonomous systems is here and will permanently change the shipping industry: At first near the coastlines and then across the oceans. Highly automated, remote-controlled, or fully autonomous vessels and systems will have far-reaching effects on the entire maritime sector and its law.

The new technology also brings new security risks when it comes to criminal acts launched against such ships. Criminals such as pirates and terrorists will no longer be just a threat offshore but could attack from anywhere in the world.[36] Cyber-attacks are generally not a new problem but will increase further in the context of unmanned and autonomous shipping. The Verizon Data Breach Investigations Report from 2019 has reported over 41,686 confirmed security incidents and 2,013 data breaches spanning 86 countries worldwide.[37] This affects shipping companies as well: The largest container shipping company in the world Maersk reported global information technology outages in 2017.[38] The attack took down a large part of the group over several days and resulted in costs of between USD 250 and 300 million (over ZAR 5 billion[39]).[40] The company was forced to reinstall thousands of computers and servers.[41] Because of the high risk of cyber-attacks, shipping companies around the world have, therefore, intensified their efforts of prevention. In 2019, the Shipbuilding, Machinery and Marine Technology (SMM)[42] Maritime Industry Report (MIR) indicates that 80 per cent of the leaders in the shipping industry consider cyber security as an important or very important issue.[43] The International Maritime Organisation (IMO) states that a ship´s onboard information technology can be hacked just as easily as systems ashore.[44] The risk of cyber-attacks increases constantly with every new type of onboard ICT system that supports automatic operations at sea or any other type of remote onshore control service. In 2017, a cyber penetration test conducted by the Israel-

[36] R Rylander and Y Man *'Autonomous safety in vessels - an international overview and trends within the transport sector'* (2016) *Lighthouse Reports* 37.
[37] Verizon *'2019 Data Breach Investigations Report'* (2019) 2.
[38] L Mathews *'NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million'* (16 August 2017) *Forbes* available at *https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#72efd764f9ae*, accessed on 21 January 2021.
[39] USD 1 is equivalent to approximately ZAR 14.84 (Exchange rate on 21 January 2021).
[40] Mathews (note 38 above).
[41] Ibid.
[42] The SMM is the leading international maritime trade fair that takes place every two years in the city of Hamburg in Germany.
[43] SMM *'SMM insights 2017'* (2017) 15.
[44] IMO *'Cyber Security'* available at *http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx*, accessed on 21 January 2021.

based cyber security specialist Naval Dome demonstrated to the maritime world, that in principle, anybody skilful and capable to access the ICT system could take control of a ship.[45] Under the supervision of the cyber system´s manufacturers and owners, Naval Dome´s cyber security team managed to hack into live, in-operation systems that are used to control a ship´s navigation, radar, engines, pumps, and machinery with the result of being able to change the ship´s operation according to the team´s objectives.[46] Not only were the ship´s position, heading, depth, and speed manipulated, but the system did also not report the incident but displayed a perfectly normal and under control situation for the officer of the watch.[47]

Many incidents show how realistic the threat of cyber-attacks is to the maritime sector. The first example shows that especially ports are very vulnerable to hacker attacks. Over two years starting in June 2011, a hacker group successfully infiltrated the cargo tracking system of the Port of Antwerp in Belgium to smuggle drugs in shipping containers.[48] The group managed to identify the drug-containing containers by hacking into the container tracking system.[49] They gained access to the system by simply emailing malicious software to the staff at the port. The incident was only discovered after entire containers disappeared from the port with no explanation.[50] By then the attackers had been already active for two years and were able to make great use of the tracking system to their objectives.[51]

The next example shows that no matter how big and well prepared the company may be, hackers still find a way to infiltrate the system. A few years after the incident at the Port of Antwerp a major cyber-attack caused immense financial loss to the world´s largest container ship and supply vessel operator. In June 2017, the Danish business conglomerate A.P. Moller – Maersk became the victim of a cyber-attack that disrupted the company's operations in transport and caused lost revenue of nearly USD 300 million (over ZAR 5 billion).[52] In this case, Ransomware

[45] V Wee *'Naval Dome exposes vessel vulnerabilities to cyber-attack'* (22 December 2017) *Seatrade Maritime News* available at *https://www.seatrade-maritime.com/news/asia/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack/*, accessed on 21 January 2021.
[46] Ibid.
[47] Ibid.
[48] *'Antwerp incident highlights maritime IT security risk'* (21 October 2013) *Seatrade Maritime News* available at *https://www.seatrade-maritime.com/news/europe/antwerp-incident-highlights-maritime-it-security-risk/*, accessed on 21 January 2021.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] J Novet *'Shipping company Maersk says June cyberattack could cost it up to $300 million'* (16 August 2017) available at *https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html*, accessed on 21 January 2021; C Baraniuk '*How hackers are targeting the shipping industry'* (18 August 2017) available at *https://www.bbc.com/news/technology-40685821*, accessed on 21 Janury 2021. '

was used to shut down all the applications and data affecting the Maersk Line, Damco, and APM terminals.[53]

London-based leading provider of integrated shipping services Clarkson PLC became a victim of a cyber security breach just a few months later in November 2017.[54] An unauthorised third party gained access to the company´s computer system in the UK, copied data, and demanded ransom for its return.[55]

In July 2018, the Chinese shipping and logistics company China Ocean Shipping Group Company (COSCO) confirmed that they had been hit by a cyber-attack.[56] Even though their vessels were not impacted the company´s internet connection within the American region was not working.[57] This affected local emailing and network telephones, the ability to communicate with vessels and maritime terminals, and lead to the company´s decision to shut down the connections with other regions for further investigation.[58]

The last example of how cyber-attacks impacted the maritime sector took place in October 2018. Australia´s ferry and defence shipbuilder Austal was hit by a cyber-attack.[59] The company provides defence vessels to both the U.S. and Australian navies and has clients spanning 54 nations including customers such as the Royal Navy of Oman. An unknown Iranian offender breached the company´s data management systems and managed to steal internal data including ship design drawings.[60] Some of the information hacked was later offered for sale on the dark web.[61]

---

[53] Ibid.
[54] *'Clarksons Falls Victim to Cyber Security Breach'* (29 November 2017) available at *https://worldmaritimenews.com/archives/236548/clarksons-falls-victim-to-cyber-security-breach/*, accessed on 21 January 2021; M Schuler *'Clarkson Plc Reveals Details of 2017 Cyber Security Incident'* (31 July 2018) available at *https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/*, accessed on 21 January 2021.
[55] Ibid.
[56] *'COSCO Shipping Lines Falls Victim to Cyber Attack'* (25 July 2018) available at *https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/*, accessed on 21 January 2021; *'CSOCO Shipping Lines back to Normal after Cyber Attack'* (30 July 2018) available at *https://worldmaritimenews.com/archives/257916/cosco-shipping-lines-back-to-normal-after-cyber-attack/*, accessed on 21 January 2021.
[57] Ibid.
[58] Ibid.
[59] *'Austal falls victim to cyber-attack'* (2 November 2018) available at *https://worldmaritimenews.com/archives/263840/austal-falls-victim-to-cyber-attack/*, accessed on 21 January 2021.
[60] Ibid.
[61] Ibid.

A cyber-attack on an unmanned and autonomous ship could be understood as more than just a simple cybercrime. In the thesis, it will be discussed that such an attack could include two elements: the technical act of hacking into the system of the vessel (the cybercrime) and the act of piracy. For this reason, this thesis refers to a cyber-attack on an unmanned and autonomous vessel as cyber piracy.

Cybercrimes and piracy have more in common than it appears at first glance. To start with both crimes are transnational and are likely to involve more than one jurisdiction. Usually more than one country is involved in such a cross-border incident. Also, the environments are surprisingly alike: they are international spaces. They are being shared globally and connect countries, companies, and individuals from all around the world. Their spaces are used to trade, transport, and share goods and information. One could say that the internet is like the high seas or the high seas can be an analogy of the cyberspace. Both spaces for themselves also attract criminals. But what happens if these spaces overlap and are brought together as one? This thesis will show that cyber piracy includes elements of both crimes. It could therefore be considered the most international crime of them all. Imagine a container ship on the high seas being hacked by a third party through the cyberspace. This simple scenario results on many very interesting legal questions.

1.2 Purpose and Objective of the Research

The purpose of this thesis is to define the term cyber piracy and to examine the term and its regulations from an international and national law perspective. Because it would be impossible to go into detail about every sector of the maritime industry the focus of this thesis will only be on cyber-attacks on unmanned and autonomous vessels at sea and its SCC. The main problem for the shipping industry at the moment is, that the very fast technical progress regarding unmanned and autonomous operations outruns the legal framework that is supposed to protect such operations from threats such as cyber piracy. Cyber piracy can have a significant impact on the safe and secure journey of an unmanned and autonomous ship. Therefore, the purpose of this thesis is to create awareness for challenges in the future, to define the term ‘cyber piracy’ for future discussion, and to take a look at some international and national legal instruments regarding this topic.

1.3 Research Methodology

This thesis will be based on doctrinal desktop research of all relevant primary sources such as international conventions, regulations, and guidelines as well as national law focusing on South African and German legislation. For me, as a German lawyer who is living and studying in South Africa, it is very interesting to compare how the two coastal countries handle the topic legally. This is why German and South African law was chosen for the thesis. In addition to this, the thesis will make use of official reports as well as secondary resources such as books, relevant case law, journal articles, and media reports.

1.4 Architecture of the Research and Primary Research Questions

This thesis consists of six chapters. The current chapter is an introduction, setting out the background of the research topic, giving information on the purpose and objective of the research, the research methodology, and the scope of the applicable legal instruments. The following five chapters deal with the act of cyber piracy on unmanned and autonomous ships. In this context, the thesis deals with three main research questions:

(i) What is 'cyber piracy'?

(ii) How is cyber piracy regulated from an international law perspective?

(iii) How is cyber piracy regulated from a national law perspective?

To answer these questions, the thesis is structured as follows:

- **Chapter Two** will first take a look at the historical and legal development of piracy and cybercrime. This is to find out what law is currently in place. Furthermore, it is to develop an understanding of the terms and to prepare the reader for the definitions of the terms in the following chapter and their overlap with the term 'cyberpiracy'. After that, the chapter will provide some important definitions. To be able to follow the subsequent elaborations, the terms 'unmanned' and 'autonomous' will be defined. After that, the terms 'ship', and 'master' are discussed.

- **Chapter Three** is focused on the term 'cyber piracy'. This is done by analysing the two elements of the term 'piracy' and 'cybercrime'. The chapter will first examine the definitions of the terms on an international and then on a domestic level focusing on German and South African law. This is to find out if the terms 'piracy' and 'cybercrime' include the term 'cyber piracy' in their definition or somehow overlap with it.

- **Chapter Four** will analyse cyber piracy from an international law perspective. The focus will first be on regulations that may be helpful to prevent cyber piracy. This is done by taking a look at both maritime- and cyber-relate international legal instruments. After that, the chapter will focus on international jurisdiction regarding cyber piracy by taking a look at jurisdiction on 'piracy' and 'cybercrime' and using those results to explain the jurisdiction on 'cyber piracy'. In the end, this chapter will take a look at what international court could prosecute cyber piracy. This is also done by looking at where piracy and cybercrime are prosecuted.

- **Chapter Five** will focus on cyber piracy from a national law perspective. The focus will be on German and South African maritime- and cyber-related domestic law. The first part will deal with German law and will take a look at regulations that may help to prevent cyber piracy, at regulations that qualify cyber piracy as a criminal offence, and those regarding its sentence. Also, this subchapter will take a look at the national implementation of international jurisdiction in the case of cyber piracy, law enforcement, and the court's jurisdiction in such a case. The second part of the chapter will take a look at the same topics under South African law.

- **Chapter Six** contains the conclusion of the thesis and will present possible changes within the legislation.

1.5 Scope of the Applicable Legal Instruments

To answer the three main research questions, the thesis will take a look at international, German, and South African law. International conventions are only considered when both Germany and South Africa have signed the convention. For chapter three, the thesis will take a look at the most notable international conventions that define the terms 'piracy' and 'cybercrime'. For the term 'piracy' these are the 1982 United Nations Convention on the Law of Sea[62] (UNCLOS) and the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation[63] (SUA Convention). For the term 'cybercrime', the most notable international convention is the 2001 Convention on Cybercrimes of the Council of Europe[64] (Convention on Cybercrimes). On a domestic level, the thesis will take a look at relevant German and South African law that helps to define the terms 'piracy' and 'cybercrime'. In Germany, the

[62] 1833 UNTS 3, (1982) 21 ILM 1261. Adopted: 10.12.1982; EIF: 16.11.1994.
[63] 1678 UNTS 221, 27 ILM 668. Adopted: 01.03.1988; EIF: 01.03.1992.
[64] ETS No 185. Adopted: 23.11.2001; EIF: 01.07.2004.

Strafgesetzbuch of 1998[65] (StGB - German Criminal Act) is the main law that deals with criminal law including piracy and cybercrime as well as with its definitions. In South Africa, the main legislation that deals with the term 'piracy' is the Defence Act No. 42 of 2002[66]. For the term 'cybercrime' the thesis will take a look at the Cybercrimes and Cybersecurity Bill of 2017[67] (Cybercrimes and Cybersecurity Bill). Even though this Bill is still in the process of being enacted it will be discussed instead of the Electronic Communication and Transactions Act 25 of 2002 (ECT Act)[68]. This is because the Cybercrimes and Cybersecurity Bill repeals the relevant provisions that were regulated under the ECT Act.[69]

For chapter four, the thesis will then examine a broader scope of international legal instruments that deal with maritime security and cybercrime. The scope includes UNCLOS, the 2002 International Ship and Port Facility Code[70] (ISPS Code), the International Safety Management Code[71] (ISM Code), the International Maritime Organisation Guidelines (IMO) on Maritime Cyber Risk Management[72], the IMO Maritime Cyber Risk Management in Safety Management Systems[73], the Baltic and International Maritime Council (BIMCO) Guidelines on Cyber Security Onboard Ships[74], and the Information Security Management Standards on Information technology - Security techniques - Information security management systems - Requirements[75] (ISMS).

For chapter five, the thesis will take a look at a wider range of national maritime- and cyber-related legislation. For Germany, the thesis will take a look at all relevant maritime security legislation. This is namely the Schiffssicherheitsgesetz of 1998[76] (SchSG - Ship Safety Act), the Schiffssicherheitsverordnung of 1998[77] (SchSV - Ship Safety Ordinance) and the

[65] Strafgesetzbuch, BGBl. S. 3322 of 1998; official English translation available at *https://www.gesetze-im-internet.de/stgb/BJNR001270871.html*, accessed on 21 January 2021.
[66] Defence Act No. 42 of 2002.
[67] Cybercrimes and Cybersecurity Bill B6 of 2017.
[68] Electronic Communication and Transactions Act No. 25 of 2002.
[69] Compare for more information chapter 2.2 of the thesis.
[70] 2002 International Ship and Port Facility Code.
[71] International Safety Management Code.
[72] MSC-FAL.1/Circ.3. Issued 05.07.2017.
[73] Resolution MSC.428(98). Adopted: 16.06.2017.
[74] Baltic and International Maritime Council *'Guidelines on Cyber Security Onboard Ships – Version 3'* (2018).
[75] ISO/IEC 27001; International Organisation for Standardisation and the International Electrotechnical Commission *'Information Security Management Standards on Information technology – Security techniques – Information security management systems – Requirements'* (June 2017).
[76] Schiffsicherheitsgesetz BGBl. I S. 2860, from 9 September 1998; no official English translation available.
[77] Schiffssicherheitsverordnung BGBl. I S. 3013, 3023 from 18 September 1998; no official English translation available.

Verodnung über die Sicherheit der Seefahrt der Bundesrepublik Deutschland of 1993[78] (SeeFSichV - Ordinance on the Safety of Maritime Navigation of the Federal Republic of Germany). For the cybercrime-related legislation, Germany only has the Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme of 2009[79] (BSIG - Act on Federal Office for Information Security) and Verordnung zur Bestimmung kritischer Infrastrukturen from 2016[80] (BSI-KritisV - Ordinance to regulate critical infrastructures) in place. For South Africa, the thesis will also take a look at all relevant maritime security law and cybercrime-related legislation. These are namely the Merchant Shipping (Maritime Security) Regulations of 2004[81] (MSR) and the Cybercrimes and Cybersecurity Bill.

[78] Verordnung über die Sicherheit der Seefahrt der Bundesrepublik Deutschland BGBl. I S. 1417 from 27 July 1993; no official English translation available.
[79] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik BGBl. I S. 2821 from 14 August 2009; official English translation available at *https://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html*, accessed on 21 January 2021.
[80] Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz BGBl. I S. 958 from 22 April 2016; no official English translation available.
[81] Merchant Shipping (Maritime Security) Regulations of 2004, published under section 356 of the Merchant Shipping Act No. 57 of 1951.

2 BACKGROUND AND DEFINITION

2.1 The Historical and Legal Development of Piracy

Piracy is a phenomenon as old as the beginning of seafaring.[82] The earliest recorded incident of piracy dates back to the 14th century BC when the Lukkans, a group of sea raiders, attacked ships that were sailing in the Aegean and Mediterranean waters.[83] Starting in the 8th century BC, the Illyrians, Tyrrhenians, Greeks, Romans, Carthaginians, as well as the Phoenicians, had been involved in acts of piracy.[84] During the 1st century BC, pirates threatened the trade of the Roman Empire in the Mediterranean by setting up a large nation along the Anatolian coast.[85] Around the year 300 AD, Frankish, Saxon, and Irish pirates were a threat to the coastlines.[86] During the middle ages, the Vikings from Scandinavia were a threat to the north-western European coasts.[87] At the same time Arab pirates, privateers, and the Barbary corsairs were famous pirates.[88] The so-called golden age of piracy occurred between 1620 and 1735.[89] During this time, states commissioned pirates to attack vessels of enemy states. This was especially done between England and France and England and Spain in the 17th century.[90] In the 19th century, piracy develops also along the coast of China.[91] These pirates mainly attack vessels of their nationality and kill passengers and crew.[92] Piracy grew again rapidly during the last decade of the 20th century and became a major problem for international commerce in the first decade of the 21st century. Today, there are several hot spots for modern piracy including the Gulf of Aden, off the Somali and Nigerian coasts, the Strait of Malacca, and the Indian Ocean.[93]

In modern times, the first international attempt to provide an agreement to combat piracy was made in 1924 during the era of the League of Nations.[94] But the issue was dropped because it

---

[82] M Kelly *'The Pre-History of Piracy as a Crime & Its Definitional Odyssey'* (2014) 28; D Burgess *'Hostis Humnni Generi: Piracy, Terrorism and a New International Law'* University Miami International & Comparative Law Review Volume 13, Issue 2 (2006) 301; E Barrios *'Casting A Wider Net: Addressing the Maritime Piracy Problem in Southeast Asia'* Boston College International & Comparative Law Review, Volume 28, Issue 1 (2005) 149.
[83] G Berlusconi *'History of Piracy'* Encyclopaedia of Transnational Crime and Justice (2014) 301.
[84] Ibid 303.
[85] Ibid 302.
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Burgess (note 82 above).
[91] Berlusconi (note 83 above) 303.
[92] Q Le *'A short review: the situation of piracy in the world and proposed solutions for prevention'* International Journal of Mechanical Engineering and Technology, Volume 10, Issue 1, (January 2019) 262.
[93] Ibid.
[94] L Azubuike *'International Law Regime Against Piracy'* Annual Survey of International & Comparative Law, Volume 15, Issue 1, Article 4 (2009) 48.

was 'perhaps doubtful whether the question of piracy is of sufficient real interest in the present state of the world to justify inclusion in the programme of the conference'[95]. The United Nations Conference on the Law of the Seas was more successful on the issue. In 1958, they adopted the Geneva Convention on the High Seas[96] which contains provisions that deal with piracy under Articles 14 to 21 of the Convention including the definition of the term 'piracy' in Article 15 of the Convention.

In 1982, the United Nations Conference adopted the United Convention on the Law of the Sea (UNCLOS). Even though UNCLOS did not replace the Geneva Convention, the contracting states to UNCLOS include most of the states that were previously bound to the Geneva Convention.[97] As a result, the Geneva Convention remains binding for those states that are not parties to UNCLOS, for example, the United States of America.[98] Currently, UNCLOS has 166 contracting parties. UNCLOS includes provisions on piracy in Articles 100 to 111 including the definition of the term 'piracy' in Article 101 of UNCLOS.

On 10 March 1988, the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention) was adopted following the incident onboard the Achille Lauro in 1985.[99] The Achille Lauro was an Italian cruise ship that was seized in the high seas by a group of Palestinians posing as passengers.[100] They took the passengers and crew hostage and killed one passenger, demanding the release of 50 Palestinians that were being held in jails in Israel.[101] They were eventually captured and brought to trial in Italy where they were convicted of terrorism offences.[102] The event was considered to fall outside the international law definition of piracy under UNCLOS.[103] This is why the SUA Convention complements the provisions on piracy that are found in UNCLOS, as it provides further definitions of offences that threaten the safety of maritime navigation.[104]

---

[95] Polish Minister for Foreign Affairs M. Zaleski at the Council of the League of Nations in 1927.
[96] 450 UNTS 11, 13 UST 2312. Adopted: 29.04.1958; EIF: 30.09.1962.
[97] United Nations Conference on Trade and Development *'Maritime Policy - Part II - An Overview of the International Legal Framework and of Multilateral Cooperation to Combat Piracy - Studies in Transport Law and Policy - 2014 No. 2'* (2014) 4.
[98] Ibid.
[99] Ibid 15.
[100] Azubuike (note 94 above) 56.
[101] Ibid.
[102] Ibid.
[103] P Mukherjee *'The SUA Convention 2005: a critical evaluation of its effectiveness in suppressing maritime criminal acts'* Journal of International Maritime Law, Volume 12, Issue (2006) 170.
[104] United Nations Conference on Trade and Development (note above 97) 15.

On a national level, most countries also combat piracy. Surprisingly, German criminal law does not provide a section dealing with piracy exclusively but only includes definitions of related crimes such as theft, robbery, and armed robbery. German courts apply two different offences to combat piracy. This was done in 2010 when ten alleged pirates from Somalia were prosecuted in the city of Hamburg in Germany.[105] It was the first trial on charges of piracy in Germany for almost 400 years.[106] The defendants were accused of having taken possession of a German container ship off the coast of Somalia.[107] When the main court hearing commenced on 27 October 2010, the crime was prosecuted as a joint attack on maritime traffic according to section 316c(1) number 1b of the StGB in conjunction with abduction for the purpose of blackmailing according to section 239a(1) of the StGB.[108]; [109] In South Africa, the Defence Act deals with piracy. The definition of the term can be found in section 24 of the Defence Act.

2.2 The Historical and Legal Development of Cybercrimes

Compared to the long history of piracy, the history of cybercrime is a fairly short but speedy one. If one assumes that computer-related crime emerged already shortly after the invention of the first digital computer in 1943, the first out of four stages of cybercrime began from the late 1940s and lasted through the late 1960s.[110] Even though the installations of computers increased rapidly over those two decades from 400 at the beginning of the 1950s to 60,000 by the end of the 1960s[111] there was hardly a commercial market for computers. In addition to a small number of computers, the internet did also not yet exist. Its development started in the 1960s as a network that was used by the U.S. Department of Defence to provide communication between the Department's sectors in the event of a nuclear war or attack.[112] Nevertheless, the first prosecuted

---

[105] Taipan Case; Oberlandesgericht Hamburg (Higher Regional Court Hamburg) *'Landgericht Hamburg entscheidet über Eröffnung des Hauptverfahrens gegen zehn somalische Angeklagte – Verhandlungsbeginn am 22. November 2010'* Official press release (29 October 2010) available at *https://justiz.hamburg.de/pressemitteilungen/2601882/pressemeldung-2010-10-29/*, accessed on 21 January 2020; Landgericht Hamburg (Regional Court Hamburg) 6*03 KLs 17/10* (19 October 2012).

[106] D Herder *'Erster Piraten-Prozess in der Hansestadt seit 400 Jahren'* (05 June 2010) available at *https://www.abendblatt.de/hamburg/article108540468/Erster-Piraten-Prozess-in-der-Hansestadt-seit-400-Jahren.html*, accessed on 21 January 2021.

[107] Oberlandesgericht Hamburg (note 105 above).

[108] Oberlandesgericht Hamburg *'Poolführung im Strafverfahren gegen 10 Somalier wegen Angriffs auf den Seeverkehr und erpresserischen Menschenraubs'* Official press release (19 November 2019) available at *https://justiz.hamburg.de/pressemitteilungen/2639402/pressemeldung-2010-11-19/*, accessed on 21 January 2021.

[109] The same criminal offences were also relevant in the judgment in another pirate trial four years later. In this case a chemical tanker vessel 'Marida Maguerite' with 22 crew members was kidnapped by pirates from Somalia. Compare Landgericht Osnabrück (Regional Court Osnabrück) *10 KLs - 710 Js 21274/13 - 31/13* (17 April 2014).

[110] J Li *'Cybercrime and Legal Countermeasures: A Historical Analysis'* International Journal of Criminal Justice Sciences – Official Journal of the South Asian Society of Criminology and Victimology, Volume 12, Issue 2 (2017) 197.

[111] D Hamilton *'Technology, Mn and the Environment'* (1973) 82.

[112] K Hafner, M Loyn *'Where Wizards Stay up Late: The Origins of the Internet'* (1998) 11.

computer crime occurred in 1958 when it was revealed that a bank employee had utilised the institution's computer to embezzle cents from interest on long-term accounts.[113] At the beginning of this stage, there was neither cybercrime nor cyber-criminal law, neither on an international nor on a national level and when the first computer crimes occurred, no law was there to deal with them.[114]

The following stage lasted from the 1970s to the end of the 1980s.[115] During this time the threat of computer crimes increases along with the dependence upon computers.[116] Even though the computers changed in technological ability and size[117] the operations remained straightforward and vulnerable to manipulation. This starts to attract hackers. The threat of malicious programs such as viruses, the Trojan Horse, and worms start to increase. As a response, the first antivirus is programmed in 1987.[118] Many countries now try to eliminate legal gaps to punish cybercrime. At the beginning of the 1970s, most developed countries present the first legislation regarding computer crimes.[119] However, the overall feeling was that the law was not effective enough.[120]

The pace of cybercrime increases in the third stage covering the 1990s when personal computers find their way into private homes and offices and go online.[121] From now, the growth of the internet and its commercial use develops fast and criminals use the new platform regularly. They find their way into electronic communication such as emails.[122] They attack private and public targets.[123] Cybercrime is starting to become a global threat.[124] The business of antivirus and internet security develops quickly during this period.[125]

---

[113] D Parker *'Computer Crime: Criminal Justice Resources Manual'* (1989) 5.
[114] C Chen *'Computer Crime and Computer Fraud and Abuse Act of 1987'* Computer Law Journal, Volume 10, Issue 1 (1990), 72.
[115] Li (note 110 above) 199.
[116] Ibid.
[117] V Mosco 'The Digital Sublime: Myth, Power, and Cyberspace' (2004) 21.
[118] J Li (note 110 above) 200.
[119] U Sieber *'Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission'* (1998).
[120] M Dierks *'Computer Network Abuse'* Harvard Journal of Law and Technology, Volume 6, Issue 2 (1993) 307-342; A Bequai *'White-Collar Crime: A 20th Century Crisis'* (1978) 5-6.
[121] V Mosco *'The Digital Sublime: Myth, Power, and Cyberspace'* (2005) 2.
[122] Ibid.
[123] Ibid.
[124] J Li (note 110 above) 201-202.
[125] Ibid.

The fourth stage starts with the new century.[126] The 2000s brought social media and saw a rise in identity theft.[127] But the law develops much faster now to keep up with the threat. The European Convention on Cybercrimes also known as the Budapest Convention on Cybercrimes is the first international treaty on crimes committed via the internet and other computer networks. Its main objective, as set out in the preamble of the Convention, is to pursue a common criminal policy aimed at the protection of society against cybercrime. The Convention particularly deals with infringements of copyright computer-related fraud, child pornography, and violations of network security. [128] The Convention aims to increase cooperation among the nations and by harmonising and adopting appropriate national legislation with regard to cybercrime.[129] Germany and South Africa both signed the Convention on 23 November 2001. Not only Europe but also the African Continent aims to protect from cybercrime. The African Union Convention on Cyberspace Security and Personal Data Protection[130] also known as the Malabo Convention represents a political commitment by the African States to take measures on a range of issues including cybercrimes. It was adopted on 27 June 2014. However, the Convention is not yet in force and South Africa has not signed it yet.

Besides those international conventions, many countries also implement cybercrime legislation on a domestic level. This also includes Germany and South Africa. South African cyber-related law recently underwent some important changes to implement the goals of the European Cybercrime Convention into its national law. The old legal framework relating to cyber-security used to be a hybrid of different pieces of legislation. In the past, cybercrime offences were primarily regulated under the ECT Act. The new Cybercrimes and Cybersecurity Bill repeals the relevant provisions under the ECT Act most notably chapter 9 and sections 85, 86, 87, 88, and 90. The Cybercrimes and Cybersecurity Bill is in the process of being enacted and codifies numerous offences relating to cybercrimes. The Bill will provide the structure for preventing cybercrime and addresses computer-based criminal activity such as unlawful access to, interference with or distribution or date, electronic communications, information systems, and networks.

[126] Ibid.
[127] Ibid.
[128] J Kosseff *'Cybersecurity Law'* (2019) 266.
[129] Ibid.
[130] *African Union Convention on Cyberspace Security and Personal Data Protection*, Adopted: 27.06.2014.

Germany implemented the goals of the European Cybercrime Convention in the StGB. In addition to that, the German BSIG which is in force since July 2015, aims to make German IT systems and digital infrastructures the safest in the world.[131] In particular, in the field of critical infrastructures such as electricity and water supply, finance, and food a failure or impairment of supply services would have dramatic consequences for the economy, the state, and the society in Germany.[132] The availability and security of information technology (IT) systems, therefore, play an important and central role, especially in these critical areas. The BSIG aims to also improve IT security in companies and the federal administration, as well as better protection of citizens using the internet.[133] For this reason, the Bundesamt für Sicherheit in der Informationstechnik (BSI - Federal Office for Information Security) was established. Operators of critical infrastructures must regularly prove compliance with up to date IT security to the BSI.[134] Where security deficiencies are detected, the BSI can order their removal and can also hold the manufacturers of the IT products or systems to improve their standards.[135] The BSI is also granted the power to examine IT products for their safety. According to section 10(1) BSIG, the Federal Minister of the Interior shall specify the statutory instruments further. This was done by drafting the BSI-KritisV that presents the critical infrastructures in the seven following sectors: energy, water, information technology and telecommunication, health, food, finance- and insurance, government and administration, media and culture, and transportation and commerce.[136] For every mentioned sector, specific standards are drafted. This is done by experts of each sector and must get approved by the BSI before they get published and come into force as a mandatory standard.

2.3 Definitions

2.3.1 The terms 'unmanned' and 'autonomous'

When speaking about unmanned and autonomous ships, it must first be clear what can be defined as such ships. The term 'autonomous' means that the vessel can perform a set of defined operations with no or reduced attention from a ship bridge or the SCC.[137] 'Automation' is a general term for computerised processes that give the vessel the ability to perform certain

[131] Bundesamt für Sicherheit der Informationstechnik *'Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz-BSIG)'* available at *https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html*, accessed on 21 January 2021.
[132] Ibid.
[133] Ibid.
[134] Compare section 8a of the BSIG.
[135] Compare section 8b of the BSIG.
[136] Compare especially section 2(6) of the BSIG.
[137] Norwegian Forum for Autonomous Ships (NFAS) *'Definition for Autonomous Merchant ships'* (October 2017) 7.

operations without human control.[138] The term 'autonomy' means that the system has control functions that can use different options to solve selected classes of problems and is a result of applying automation to a ship.[139] The term 'autonomous' does not imply that there is no crew onboard the ship.[140] It only refers to the way of controlling and navigating a ship. This means that there could still be a bridge crew onboard that could overlook or take over the navigation of the ship if need be. Autonomous vessels can also be categorised according to their degree of autonomy.[141] The following terms are generally used to describe the different degrees of an autonomous ship: remote-controlled ship, automatic ship, constrained autonomous ship, and fully autonomous ship.[142]

The remote-controlled ship is continuously under control of the SCC. Every operation needs input from the centre which means that there is a continuous connection between the ship and the remote-controller on land.[143] Strictly speaking, this type is not one that falls under the scope of the term of autonomy because it is remotely controlled at all times. But the ships will, in most cases, need fall-back procedures that can be activated autonomously in case of communicative failures and can, therefore, still be considered as a backward degree of autonomy.[144] Unlike the remote-controlled ship, the automatic ship is controlled by the bridge system, meaning that the ship can complete certain operations without human interaction following a pre-programmed sequence.[145] The ship could, for example, be pre-programmed to follow a certain route at a set speed, slowing down or picking up speed at a defined part of the journey. However, the operation of the ship is always under human oversight. The ship is either being supervised by the SCC on land or the bridge crew on board which both continuously monitor the situation and can intervene either through remote controlling or direct control at any time if any unexpected events occur.[146] The next degree of autonomy is the constrained autonomous ship. Ships using this technology can operate fully automatic as described above and also have a variety of options for solving occurring problems on their own.[147] This means the ship could, for example,

[138] Ibid 5.
[139] H Huang *'Autonomy Levels for Unmanned Systems (ALFUS) Framework Volume I; Terminology Version 2.0'* (October 2008) 15.
[140] M Suri 'Autonomous vessels as ships – the definition conundrum' IOP Conference Series: Materials Science and Engendering, Volume 929, (2020)
[141] Ibid.
[142] NFAS (note 137 above); AAWA (note 28 above) 7; IMO *'IMO Takes First Ste[s to Address Autonomous Ships'* available at *IMO takes first steps to address autonomous ships*, accessed on 21 January 2021.
[143] F Koscielecki *'Autonomous shipping – Revolution by evolution'* Legal Briefing (July 2019) 3-4.
[144] Ibid.
[145] Ibid.
[146] NFAS (note 137 above) 11.
[147] Ibid 12.

decide without previous human consultation on how to avoid the collision with an unexpected object at sea by calculating different ways around it. The SCC or bridge crew personnel only take actions in an operation if the ship´s system requests it, meaning the ship´s system cannot calculate a solution for an upcoming quest. In any other case, the ship will manage all upcoming tasks by itself.[148] The last degree of autonomy is the fully independent ship. This type is never supervised and operates completely on its own, meaning that there will not be any SCC or bridge crew that is overlooking or supervising at any time.[149] This type of ship needs highly advanced technology onboard as it must be able to calculate and solve every upcoming task independently.[150]

Unlike the term 'autonomous', the term 'unmanned' refers not to the way the ship is navigated but to the physical presence of humans on board. The term 'unmanned' means that there is no human presence on board the ship to perform or supervise the operation of the ship.[151] Unmanned ships can also be classified into different degrees. A ship can have a periodically unmanned bridge, meaning that the ship can operate without a bridge crew for limited defined periods, for example, when it is navigating across the high seas.[152] This type of ship does not qualify as an unmanned vessel in the proper sense as it always has a crew on board. The second type is the periodically unmanned ship.[153] This ship operates without a crew on board but also only for a limited period, for example, a deep-sea passage. The last degree is the ship that is continuously unmanned, meaning it is designed for unmanned operations at all times which implies that there is no one on the ship that is authorised to take control of the bridge.[154] Other people, for example, passengers or a maintenance crew may still be on the ship as they are not in charge of the operations of the ship.[155]

In conclusion, the term 'autonomous' describes the way a ship is navigated and the term 'unmanned' refers to the physical presence of people on board a ship. An unmanned ship always operates with some degree of autonomy, supposing that remote-controlling can be considered

[148] Ibid.
[149] Koscielecki (note 143 above) 4.
[150] Ibid.
[151] World Maritime University 'Conventional Vessels and Marine Autonomous Surface Ships – a Love marriage' (2018) 3; J Delgado 'The Legal Challenges of Unmanned Ships in the Private Maritime Law: What Laws Would You Change?' SSRN Electronic Journal (January 2018) 498.
[152] NFAS (note 137 above) 5.
[153] Ibid 15.
[154] Ibid.
[155] Ibid.

as the lowest degree of autonomy.[156] An autonomous ship, on the other hand, is not necessarily always unmanned. The automatic and the constrained autonomous ship could both have a bridge crew on board. Only a fully autonomous ship is, by definition, always also an unmanned ship as it has neither an SCC nor bridge crew supporting or supervising it at any time.

To underline the importance of the distinguished use of terms, the following example illustrates how the difference in the meaning of the terms can lead to different legal problems. Article 98 of UNCLOS, for example, places a qualified obligation on every state to rescue a person at sea in distress. For a ship that is unmanned, it is now questionable how the duty can be fulfilled because it is unclear how physical assistance can be given by a ship without a crew on board. This question is irrelevant for an autonomous ship that operates, for example, automatic but is not unmanned in the described way as it can be overlooked by a bridge control team. That same crew could assist the person in distress and could, therefore, at any time fulfil the duty of rescue at sea.

After distinguishing between the above terms, it is also important to understand the differences between the terms 'bridge' and 'SCC'. Both terms describe the main centre from where the ship is navigated and managed. The bridge of a ship is the room or platform onboard the ship from which the ship can be commanded.[157] A common ship is under the control of a bridge crew.[158] Under normal circumstances, the bridge is manned by an officer of the watch aided usually by an able seaman acting as a lookout.[159] The bridge crew is sometimes supported but always overseen by the master of the ship.[160] The SCC is the ship owner´s centre for monitoring and controlling the ship and is located on land.[161] Depending on the degree of autonomy, either a remote-controller, a supervisor, or a pre-programmer will be responsible for the navigation of the ship.

---

[156] If argued that remote-controlling a ship is not a degree of autonomy because the ship is under the control of the SCC at all times, the remote-controlled ship would have to be considered an unmanned but not an autonomous ship.

[157] A Menon *'Bridge of a Ship - Design And Layout'* Naval Architectures (May 2020) available *at https://www.marineinsight.com/naval-architecture/bridge-of-a-ship-design-and-layout/*, accessed on 21 January 2021.

[158] Ibid.

[159] Compare Rule 5 of COLREGs.

[160] Compare, for example, German national law: section 9(2) of the Schiffsbesatzungsverordnung BGBl. I S. 2575 from 1981 (SchBesV - German Save Manning Ordinance; Official English translation available at *https://www.gesetze-im-internet.de/englisch_schbesv/englisch_schbesv.html*, accessed 21 January 2021) '(...) the master has specially to ensure that, under the master´s general direction, officers in charge of the navigational watch during their periods of duty shall be physically present on the navigating bridge (...).'

[161] M Schuler *'Rolls-Royce Reveals Vision of Shore-Control Centres for Unmanned Cargo Ships'* (22 March 2016) available at *https://gcaptain.com/rolls-royce-reveals-details-on-shore-based-control-rooms-for-operation-of-unmanned-cargo-ships/*, accessed on 21 January 2021.

2.3.2 The term 'ship' in an autonomous and unmanned context

A question of real importance is whether or not unmanned and/or autonomous ships be considered vessels or ships within an international and national legal understanding. If not, it is questionable whether or not such a ship is governed by maritime law.[162] If maritime law would not apply at all to such ships, many international maritime-related instruments, as well as national maritime law that could help to combat cyber piracy, would not be applicable. To answer this question the thesis will take a look at the current definitions of the terms 'vessel' or 'ship' under international and domestic law. Numerous international maritime conventions dealing with specific topics apply their own definitions.[163] The following examples are chosen to present an overview of the term and to generalise the definitions by comparing and categorising the different components of the definitions.

The 1973 International Convention for the Prevention of Pollution from Ships, as modified by the Protocol of 1978 (MARPOL)[164] defines the term 'ship' in Article 2(4) as follows: 'Ship means a vessel of any type whatsoever operating in the marine environment and includes hydrofoil boats, air-cushion vehicles, submersibles, floating craft and fixed or floating platforms.' Article 1(d) of the 1924 International Convention for the Unification of Certain Rules of Law relating to Bills of Lading and Protocol of Signature (Hague Rules)[165] gives the following definition of the term 'ship': 'Ship means any vessel used for the carriage of goods by sea.' The 1972 Convention on International Regulations for Preventing Collision at Sea (COLREGs)[166] define the term 'vessel' in Rule 3(a): 'The word vessel includes every description of water craft, including non-displacement craft, WIG craft, and seaplanes, used or capable of being used as a means of transportation on water.' Article 2 of the 1986 United Nations Convention on Conditions for Registration of Ships[167] provides a definition as follows: 'Ship means any self-propelled sea-going vessel used in international seaborne trade for the transport of goods, passengers, or both with the exception of vessels of less than 500 gross registered tons.'

None of the above definitions are identical. By comparing the different definitions, it turns out though, that essentially two different aspects are mentioned. First, each of the four definitions

[162] E Van Hooydonk *'The law of unmanned merchant shipping – an exploration'* Journal of International Maritime Law, Volume 20, Issue 6 (2014) 406.
[163] Ibid.
[164] 1340 UNTS 61. Adopted 1973; EIF: 2.11.1973
[165] 1412 UNTS. Adopted: 21.12.1979; EIF:14.02.1984.
[166] 1050 UNTS 16. Adopted: 20.10.1972; EIF: 15.07.1977.
[167] 26 ILM 1229. Adopted: 07.02.1986.

includes that the object must be navigated by water to be defined as a ship. The terminology differs slightly by using the terms 'marine environment'[168], 'by sea'[169], 'watercraft'[170], and 'sea-going'[171]. The definitions merely depend on the object´s ability to move on water and make clear that vessels navigated by land or air are not considered ships. The wording only refers to *where* the ship will be navigated not *from where*. Therefore, a ship controlled from land but navigation by water fulfils the requirement of the definitions. The second characteristic of a ship in most definitions is a specific intended use of the object. The phrases 'used for the carriage of goods'[172], 'capable or used as a means of transportation'[173], and 'used (…) for the transport of goods'[174] all describe the purpose of a ship as transporting something. This part of the definition serves to delineate a ship from other moving objects such as buoys and floating navaids. The new technology does not intend to change the purpose of a ship. As with any common ship, the unmanned and autonomous version suits the purpose to transport goods from one port to another. Additionally, some definitions also explicitly include some special types of ships such as air-cushion boats[175] and non-displacement crafts[176] or exclude some types of vehicles according to the size[177] of the ship. None of the definitions, however, focus on the aspect of manning or the way of operating a ship. They do not state that a ship can only be considered a ship if there is a bridge crew on board that is in charge of the operation or could at least interfere if necessary. They also do not require manual control of the ship and therefore allow any degree of autonomy.

National maritime-related law gives a similar picture. South African merchant shipping law, for example, provides a definition of the term ship in section 2(1) of the Merchant Shipping Act 57 of 1951 (MSA)[178] as follows: 'ship means any kind of vessel used in navigation by water, however propelled or moved, and includes - (a) a barge, lighter or other floating vessel; (b) a structure that is able to float or be floated and is able to move or be moved as an entity from one place to another; and (c) a dynamically supported craft.' The definition also requires the ability of the object to be navigated by water. Second, it must be propelled or moved. The

[168] Article 2(4) of MARPOL.
[169] Article 1(d) of the Hague Rules.
[170] Rule 3(a) of the COLREG.
[171] Article 2 of the Convention on Conditions for Registration of Ships.
[172] Article 1(d) of the Hague Rules.
[173] Rule 3(a) of the COLREG.
[174] Article 2 of the Convention on Conditions for Registration of Ships.
[175] Article 2(4) pf MARPOL.
[176] Rule 3(a) of COLREG.
[177] Article 2 of the Convention on Conditions for Registration of Ships.
[178] Merchant Shipping Act No. 57 of 1951.

method of propulsion is irrelevant. An unmanned and autonomous ship only differs from a common ship in regards to its type of control and navigation as it does not operate manually. However, it is still propelled and moved.

German merchant shipping law does not give any legal definition of the term 'ship'. However, the Bundesgerichtshof (BGH - German Supreme Court) defines a ship as the following: 'A ship is any hollow body of not insignificant size with the intended purpose to move on or underwater carrying persons or goods.'[179] This definition follows the pattern of international definitions mentioning the ability to be navigated by water and the purpose of transporting. Like Article 2 Convention on Conditions for Registration of Ships, the German definition excludes some ships because of the size.

In conclusion, the general international and national understanding of the terms 'vessel' and 'ship' also includes unmanned and autonomous vessels as ships as the law does not explicitly prohibit treating unmanned and autonomous ships as a vessel or ship. The definitions do not aim to exclude ships because of how it is controlled and navigated. This means that in general, unmanned and autonomous ships can be governed by maritime law.

2.3.3 The term 'master' autonomous and unmanned context

Since unmanned ships no longer need a master or a crew onboard the question is whether the person in charge of navigating a vessel from land could be considered to be the master of the ship. This question is especially interesting for unmanned ships with no bridge crew onboard that overlooks the operation.[180] A master is responsible for the navigation of a ship and its safety.[181] Whenever an incident occurs, the master is the person in charge whose personal judgement and skill must be used to deal with the situation[182]. He or she is the leader and has the highest position. He or she gives the command on how to react and could be held liable in case of negligence.[183] If the onshore controller would be considered the master of the ship the same regulations would have to apply to him or her in case the of an incident. He or she would have to act and for example inform the authorities, guide the onshore team, and collect evidence such

[179] Bundesgerichtshof *BGH 1951, Az.: I ZR 84/51, NJW 1952, 1135* (14 December 1951).
[180] E Van Hooydonk *'The law of unmanned merchant shipping – an exploration'* Journal of International Maritime Law, Volume 20, Issue 6 (2014) 411 ff.
[181] A Nelson '*The legal Obligations of Ship Masters and Seaplane Pilots'* (February 2003) 3.
[182] F Ilordanoaia *'Master of the Ship, Manager and Instructor'* Management and Marketing Journal, University of Craiova, Faculty of Economics and Business Administration, Volume 0(S1) (2010) 133.
[183] Nelson (note 181 above).

as the date, the time, and the position of the vessel at the time of the incident. An example of the master's responsibility and authority with regard to safety can be found in section 5 of the ISM Code. Section 5.1 of the Code reads as follows:

'The Company should clearly define and document the master's responsibility with regard to:

1. implementing the safety and environmental protection policy of the Company;
2. motivating the crew in the observation of that policy;
3. issuing appropriate orders and instructions in a clear and simple manner;
4. verifying that specified requirements are observed; and
5. reviewing the SMS and reporting its deficiencies to the shore based management.'

The term 'master' is not defined in any international convention. However, definitions of the term can be found in the literature as follows: 'The master of the ship is the person on the board who has the qualification and the necessary certificate of competency for running a maritime transport ship'[184] or the term master 'refers to the person on board the vessel who holds the highest legal position'[185]. Both definitions state clearly that the master must be *on board* the ship. This does not include a person navigating a ship from the SCC on land.

On a national level, the definition of the term 'master' can be found in the German Seearbeitsgesetz[186] (SeeArbG - German Maritime Labour Act). According to section 5(1) of the SeeArbG, the term 'master' is defined as follows: 'The master shall be the crew member appointed by the shipowner to command the ship.' The definition of the term 'master' does not state whether the master has to be onboard a ship. The section simply states that the master is the person who is appointed to command the ship. Based only on section 5(1) of the SeeArbG, one could conclude that the location of a person in command over a ship is not relevant.[187] Therefore, an onshore remote-controller who was appointed by the shipowner to command the ship could still fulfil the definition of the master. However, section 5(1) of the SeeArbG must be read in context to section 3(1) of the SeeArbG.' Section 3(1) of the SeeArbG defines the term 'crew member' and reads as follows: 'Seafarers within the meaning of the present Act shall be all persons working onboard the ship, regardless of whether they are employed by the

[184] Ilordaniaia (note 182 above).
[185] M Toremar *'The legal position of the ship master'* (2000) 10.
[186] Seearbeitsgesetz BGBl. I S. 868 from 2013; official English translation available at *https://www.gesetze-im-internet.de/englisch_seearbg/englisch_seearbg.html#p0064*, accessed on 21 January 2021.

shipowner or by another person or are self-employed, including those employed for the purpose of their vocational training (crew members)'. The difference between the master of a ship and the crew onboard is the different role distribution. The master holds the command on board a ship and is superior to his or her crew. Nevertheless, he or she is considered part of the crew according to section 5(1) of the SeeArbG. As a result, section 3(1) of the SeeArbG also applies to the master. According to the definition, a crew member is a person working *on board the ship*. The wording onboard requires physical presence. A person who is located anywhere else than on the ship itself cannot be considered on board. That means the management, the control, and any other work related to the ship´s journey cannot be performed from an optional location. The onshore remote-controller, the supervisor, or the pre-programmer do not comply with the requirements of physical presence on board.

South African national law provides two definitions of the term 'master'. The first one can be found in section 2(1) of the MSA: 'Master means, in relation to a ship, any person (other than a pilot) having charge or command of such ship.' The Ship Registration Act of 1998 (SRA)[188] defines the term 'master' in section 1(1) as follows: 'Master means the person having lawful command or charge, or for the time being in charge, of a ship, but does not include a pilot aboard a ship solely for the purpose of providing navigational assistance.' The term 'master' must be understood in the context of the law. The master is in charge of the ship and controls the crew. Section 2(1) of the SRA defines the term 'crew' as follows: 'Crew means all seamen onboard a ship'. According to the definition, a crew member is a person *onboard a ship*. In addition, the definition uses the term 'seamen' which indicates that the person must be *at sea*. The South African definition uses the same terminology as the German one and also requires physical presence because a person who is located anywhere else than on the ship itself cannot be considered on board.[189] In order for the master to overlook a crew onboard a ship, he or she must be on board as well. The fact that South African law does not state literally that the master must be onboard results simply from the thought that a master by the very nature of things should be on board. Consequently, any person at the SCC does not qualify as a master of a ship under South African law.

[188] Ship Registration Act Number 58 of 1998.
[189] Comite Maritime International (CMI) *'CMI Questionnaire on unmanned ships – response by Maritime Law Association of South Africa'* 4.

In conclusion, the definitions of the term ‘master’ does not include the onshore personnel.[190] Currently, a master must be located onboard a ship. This means that regulations that concern the duties and responsibilities of a ship’s master including those that regulate the actions to be taken in the case of an incident do not apply to onshore controllers. This also means that unmanned operations do not have a master.

[190] Ibid.

3 THE TWO ELEMENTS OF CYBER PIRACY

3.1 Introduction

The origin of today's word 'cyber' comes from the word 'cybernetics' which has its roots from the Greek words 'kubernētēs' meaning 'steersman', from the verb 'kubernan' which means 'to steer.'[191] The etymological meaning of the word 'cyber' is, therefore, 'to guide or control the movement of something'. The English word 'pirate' comes from the Latin word 'pirata' which has its roots from the Greek word 'peiratēs' meaning 'attacker' as the noun originated from the Greek verb 'peirein' which can be translated to the word 'to attack'.[192] Therefore, etymologically speaking a pirate is a person that attacks someone or something, and the word 'piracy' refers to the attack itself committed by the pirate. The words put together to the term 'cyber piracy' describe an attack that aims for or leads to the control of the movement of something. This being said the aim to define the term 'cyber piracy' could be considered as reached because etymologically speaking the definition of the term 'cyber piracy' perfectly summarises the action of hacking into a ship's ICT system and bringing it under unauthorised control. However, legally speaking it is not that easy.

At this moment, there is no definition of the term 'cyber piracy' in the context of this thesis referring to a cyber-attack that is launched against the ICT system of an autonomous and unmanned ship or its ICT system to bring the ship under control. However, if the motivations, actions, and objectives of a cyber pirate overlap with those of pirates and cybercriminals why not examine the existing definitions on these terms? If cyber piracy includes elements of both crimes it is of interest to discover if the term 'cyber piracy' is sufficiently included in the current definitions of the terms 'piracy' and 'cybercrime'.

One motivation that all three types of criminals have in common is to gain financial benefits from the attack.[193] To achieve this goal a cyber pirate has to options. He or she could achieve it by selling or ransoming stolen data from commercial and industrial espionage such as the location of the ship and its cargo, the handling plans, the onboard technology, or other secret

[191] Online Etymology Dictionary *'cybernetics'* available at *https://www.etymonline.com/word/cybernetics*, accessed on 21 January 2021.
[192] Online Etymology Dictionary *'pirate'* available at *https://www.etymonline.com/search?q=Pirate*, accessed on 21 January 2021.
[193] N Stracke and M Bos *'Piracy: Motivation and Tactics - The Case of Somali Pirates'* (2009) 12; X Li *'A review of Motivations of Illegal Cyber Activities'* Kriminologija & Socijalna Integracija, Volume 25, Issue 1 (February 2017), 115; BIMCO *'Guidelines on Cyber Security Onboard Ships - Version 3'* (December 2018) 9.

information.[194] This alternative overlaps with the option a cybercriminal would have to gain financial benefits. The other option would be to use the cyber-attack to directly steal goods by arranging fraudulent transportation of cargo or to misuse a ship for their objectives as shown in the Port of Antwerp example.[195] The option of using the cargo and the ship itself is the one that a cyber pirate shares with a pirate. Another motivation of a cyber pirate could be to use the ship as a weapon. A ship under unauthorised control could cause immense damage when, for example, navigated to collide with another ship or to damage port facilities. This motivation to use the ship as a weapon could also be one of the pirates. The general idea of using a hacked object as a weapon could also be one of cybercriminals. A cyber pirate attack could even be launched from people working in the maritime sector itself.[196] Competitors, for example, are likely to perform cyber-attacks to increase their market influence by gathering knowledge about trade secrets of other companies, publishing sensitive data that could cause financial loss, or disrupting the flow of transportation.[197] Insiders, for example, disgruntled employees, could aim for negative media attention of a company to ruin its reputation in response to personal issues with the company.[198] Launching an attack with the motivation to gain a personal benefit by hurting somebody else's company could be shared with pirates and cybercriminal. A cyber pirate could also gain unauthorised access to computer files or networks to further social, ideological, or political ends trying to harm or pressure particular companies, politicians, or countries.[199] The motivation to threaten, for example, companies operating in controversial fields such as the energy sector, the oil sector, or the defence industry could also be the one of either a pirate[200] or a cybercriminal[201]. A cyber pirate could also hack into the ICT system simply to show off his or her hacking skills. This motivation is shared with some cybercriminals that are known to hack into systems just for the challenge itself of getting through cyber security defences.[202] Whatever motivation and objective the cyber pirate may have, he or she will try to reach the goal the same way a cybercriminal would. This is by accessing the ICT system of the ship or the SCC system. This could for example be done by using malware-injecting devices. In this case, the cyber pirate could use a malware-ridden USB stick or similar device that gives the

[194] BIMCO (note 193 above).
[195] Li (note 193 above).
[196] P Beaumont and S Wolthusen *'Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts'* ISG MSc Information Security thesis series (2017) 3.
[197] Ibid.
[198] Ibid.
[199] BIMCO (note 193 above).
[200] Stracke (note 193 above) 13.
[201] Li (note 193 above) 117.
[202] Ibid 113.

cyber pirate remote access to the ICT system.[203] The cyber pirate could also use missing security patches to access the systems.[204] He or she could also obtain the system's credentials through a practice called keylogging. Through a social engineering attack, the software could accidentally be downloaded that records keystrokes, saving usernames and passwords. This and other forms of 'spyware' are malware that tracks any activity until a hacker has what they need to strike.[205] All of the above-stated shows that cyber piracy includes elements of both piracy and cyber-crime. At first glance, cyber piracy resembles an act of piracy as it is directed against a ship. The motivations and objectives of the cyber pirate include those of pirates and cybercriminals. The act of accessing the ICT system of a ship is one of cybercriminals.

3.2 Piracy: Definition and Overlap to Cyber Piracy

3.2.1 United Nation Convention on the Law of the Sea

The definition of the term 'piracy' can be found in Article 101 of UNCLOS as follows:

'Piracy consists of any of the following acts:
(a) any illegal act of violence or detention, or any act of depredation, committed for private ends by the crew or the passenger of a private ship or a private aircraft, and directed:

> (i) on the high seas, against another ship or aircraft, against persons or property on board such a ship or aircraft;
>
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making is a pirate ship or aircraft; (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).'

It is generally assumed that the term 'piracy' described in subparagraph (a) consists of three different elements: the private-ends requirement, the two-ship-requirement, and the high-seas requirement.[206] Even though most literature only focuses on those three elements the definition can be divided into many more components that are commonly analysed in the three mentioned

[203] A Andronja, T Brcko, I Pavic, and H Greidanus '*Assessing Cyber Challenges of Maritime Navigation'* Journal of Marine Science and Engineering Volume 8, Issue 10 (3 October 2020), 6-8.
[204] Ibid.
[205] Ibid.
[206] Azubuike (note 94 above) 51.

groups.[207] For this thesis, the definition of the term 'piracy' will be broken down into four elements including the three commonly discussed elements and the element of 'violence or detention, or any act of depredation'[208].

To fulfil the first element, the act of piracy has to be 'any illegal act of violence or detention or any act of depredation'[209]. The 'act of violence' is not defined in UNCLOS. In the literature, the term 'violence' is described as 'the use of physical force, usually accompanied by fury, vehemence or outrage'[210] or '[the] behaviour involving physical force intended to hurt, damage, or kill'[211]. The World Health Organisation's (WHO) states that violence is 'the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation'[212]. All these definitions have in common that violence is an offence that includes the use, the attempted use, or the threatened use of physical force against a person and could include any offence against a person´s life such as murder, or manslaughter, or offences against the physical integrity of a person such as any physical injury. For a cyber piracy attack this means that the act has to qualify as one of violence. However, the attack of a cyber pirate is an electronic attack that takes place, for example, via an internet connection in the virtual cyber space, initially intended to circumvent an existing security barrier of a computer system.[213] Such an act does not classify as an offence against a person exercised by physical coercion or harm and is, therefore, not an act of violence. As an alternative to violence, an act can also qualify as piracy when it is an act of detention. The term 'detention' in the widest sense means the holding of a person in custody.[214] This means that any person could restrict the freedom of another person to move freely according to his or her intention which could include offences such as deprivation of liberty, kidnapping, or hostage-taking. In case of a cyber piracy attack, the attack would be directed against an autonomous and/or unmanned ship. If the ship is unmanned an act of detention against another person is physically not possible. An autonomous ship, however, may have people onboard that could

[207] A Logina *'The international law related to maritime security: an analysis of its effectiveness in combating piracy and armed robbery against ships'* (2009) 5.
[208] Article 101(a) of UNCLOS.
[209] Article 101(a) of UNCLOS.
[210] B Garner and H Black *'Black's Law Dictionary'* (2004) 1601.
[211] C Soanes *'Paperback Oxford English Dictionary'* (2006) 855.
[212] World Health Organization 'World report on violence and health - Summary' (2002) 4.
[213] Deutsche Bundesregierung Inneres und Heimat (German Federal Government Ministry of the Interior and-Home Affairs) '*Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Gridorios Aggelidis, Renata Alt, weitere Abgeordnete und der Fraktion der FDP – Drucksache 19/7321'* (19 February 2019) 2.
[214] Garner and Black (note 210 above) 480.

become victims of an illegal act of detention. The last alternative that qualifies an act as piracy is depredation. The term 'depredation' means an act of plundering.[215] However, what is questionable is if an act of illegal detention or illegal depredation must also include a component of violence. There are three terms used parallel to each other in the definition: 'illegal violence', illegal detention', and 'illegal depredation'. If looking at the term violence in a wider sense, all illegal depredation and all illegal detention is also illegal violence but not all illegal violence is illegal depredation or illegal detention.[216] Illegal detention and illegal depredation do not overlap with illegal violence but are both parts of it.[217] For cyber piracy, this means that to be qualified as illegal detention or illegal depredation, the act must include a violent component. This component however is missing. Even in the case of an autonomous but manned ship, the people on board would not be violently taken hostage. In conclusion, the act of cyber piracy does not fulfil the first element of piracy.

Secondly, the act of piracy has to be 'committed for private ends'[218]. The private ends requirement is probably one of the most controversial discussed parts of the definition of the term piracy circling the demarcation between the words private and public.[219] The requirement has historical roots and comes from the time when some states employed pirates to use them against their enemy states.[220] Even though UNCLOS does not define the term it is now commonly recognised that an act cannot be treated as piracy in case of religious, political, or ethnic motivations.[221] The motivation of a cyber pirate to attack a ship does not differ from the motivation of a pirate. Both attacks could be committed because of several reasons ranging from the motivation to gain financial benefits to making political or ideological statements. The question of which motivations should be included to consider the attack to be committed for private ends is for both types of attacks equally difficult. The interpretation of the term private ends is a general legal question that is not bound to the action of cyber piracy only and is not deciding on the topic of the thesis.

[215] Garner and Black (note 210 above) 473.
[216] Logina (note 207 above) 13-14.
[217] Ibid 15.
[218] Article 101(a) of UNCLOS.
[219] A Honniball *'The "private ends" of international piracy: the necessity of legal clarity in relation to violent political activists'* International Crimes Database Brief 13 (October 2015) 4.
[220] Azubuike (note 94 above) 52. Compare chapter 2.1 of the thesis for background.
[221] Honniball (note 219 above) 3-5.

As a third element, piracy must be committed 'on the high seas[222] (…) outside the jurisdiction of a State'[223]. Article 101 of UNCLOS must be read in conjunction with Article 58(2) of UNCLOS, which states that 'Article 88 to 115 and other pertinent rules of international law apply to the exclusive economic zone in so far as they are not incompatible with this Part'.[224] Therefore, Article 101(a) of UNCLOS should be read to include a state's exclusive zone.[225] In conclusion, the high seas are the open waters that are not part of the territorial sea or the internal water of any state but include its exclusive zone and an act only qualifies as piracy when committed in this geographic scope. The act of cyber piracy could therefore only be considered an act of piracy if committed within the geographic scope of the high seas. A cyber pirate has two possible targets: The onboard ICT system of the ship at sea or the ICT system of the SCC on land. Depending on the target of the attack, the answers to the question of whether or not something is located on the high seas will be different. If the ship´s ICT system is attacked directly, the ship could be located within any of the maritime zones. The ship could either be located within the state´s internal waters, archipelagic waters, territorial waters, or on the high sea. The answer to the question of whether or not a ship is located on the high sea does not differ for unmanned and autonomous ships and those that are operating traditionally. For both types of ships, an attack does not qualify as an act of piracy if it takes place in any other maritime zone but on the high seas. This is because the type of propulsion has nothing to do with a ship's location. If the ship is located on the high seas during the attack of its system the attack would fulfil the geographic element. If the ship is located in the internal or territorial waters of a state the attack would not fulfil the element. Therefore, the question is not deciding on the topic of the thesis.[226] More problematic, however, is the attack on the ICT system of the SCC. The SCC is always located within the jurisdiction of a state on land and never on the high seas. If the attack on the SCC's system does not impact the ship at sea at all but only interferes with the shore system the attack cannot be considered to be taken place on the high seas. It must be considered as an attack within the jurisdiction of the state. However, if the attack on the ICT

[222] Article 101(a)(i) of UNCLOS.
[223] Article 101(a)(ii) of UNCLOS.
[224] International Maritime Organization *'Circular letter No. 3180 – Circular letter concerning information and guidance on elements of international law relating to piracy'* (17 May 2011) 4.
[225] Ibid.
[226] If the act takes place within a state´s internal waters, archipelagic waters, or territorial sea the question would be if this act could be qualified as armed robbery. The definition of armed robbery given by the IMO in Resolution A.1025(26) Paragraph 2.2 Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery against Ships reads as follows: '(a) any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or persons or property on board such a ship, within a State´s internal waters, archipelagic waters and territorial sea; (b) any act of inciting or of intentionally facilitating an act described above.' It only differs from the definition in UNCLOS in regards to the location the illegal act takes place but lines up with the other element of the definition. As a result, cyber piracy does not fulfil the requirements of armed robbery for the same reasons.

system of the SCC is only used to access or interfere with the onboard system of a ship that is currently operating on the high seas it could be arguable that the attack is still committed on the high seas. It does not seem reasonable to only look at the starting point of an attack but to look at the intended outcome. This point of view is also supported by the fact that sometimes it will be impossible to even investigate the starting point of an online attack.

Fourth and last, piracy must fulfil the 'two-ship' requirement. The act must be 'committed by the crew or the passenger of a private ship (…) and directed against a ship, (…) persons or property on board such a ship (…)'[227]. In other words, more than one vessel must be involved in the incident.[228] The act of cyber piracy could therefore only be considered as an act of piracy if the cyber pirate would be attacking the unmanned and autonomous ship as part of the crew or as a passenger from another ship. The term 'crew' is not defined in UNCLOS. In the Convention on Facilitation of International Maritime Traffic[229], however, it is stated clearly that a crew member must be on board a ship and that a person who is located on land cannot be considered on board. The term crew does not have any other meaning in the context of Article 101 of UNCLOS. The phrase *'of a private ship'* even clarifies that the person must be onboard a ship. For the same reason personnel working at the SCC of the ship, does not fall under the definition of a crew member. The term 'passenger' is also not defined in UNCLOS but, for example, in the Special Trade Passenger Agreement (STP) [230]. Rule 2(9) of the STP defines the term as follows: 'Passenger means every person other than: (a) the master and member of the crew or other persons employed or engaged in any capacity on board a ship on the business of that ship; and (b) a child under one year of age.' Generally speaking, this means a passenger is any person, who is travelling by ship but is not driving it or working on it. The closest to a passenger onboard a ship would be a visitor of the SCC or any other third-party present at the centre for any other reason than controlling, monitoring, or navigating a ship. However, according to the wording, such a person must also be on board a ship which is clarified by the phrase 'of a private ship'. In conclusion, crew members and passengers are only those people on board a ship. Of course, a cyber pirate can operate from a ship. He or she could be located anywhere in the world and this could very well also include a ship at sea. Depending on the technology that is used by the cyber pirate it might even be necessary to be close to the target. However,

[227] Article 101(a)(ii) of UNCLOS.
[228] International Law Commission Commentary on Article 39 United Nations (1956). Report of the International Law Commission Covering the Work of Its Eighth Session, 23 April to 4 July 1956. Commentary to the Articles Concerning the Law of the Sea, A/3159, 28.
[229] 591 UNTS 265. Adopted: 09.04.1965; EIF: 05.05.1967.
[230] 822 UNTS 311. Adopted: 6.10.1971; EIF; 02.01.1974.

when looking at how other types of hackers operate it could also be typical for a cyber pirate that he or she is not currently onboard a ship but is operating from anywhere in the world most likely from the land. Hackers normally only need an internet connection and do not have to be close by the target.[231] Being located on land would be more cost and time-efficient for the cyber pirate. In conclusion, a cyber pirate could be located anywhere including onboard another ship. The act of cyber pirates is therefore only excluded if the cyber pirate operates from the land.

Summarised, the act of cyber piracy does not fall under the definition of piracy in Article 101 of UNCLOS. It does not fulfil the element of 'violence'. The graphical requirement, the private-end requirement, and the two-ship requirement could or could not be fulfilled depending on the current location of the ship, the motivation of the cyber pirate, and whether or not the cyber pirate is onboard another ship.

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

Another international convention that deals with acts that threaten the safety of ships at sea is the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) which was drafted to cover a wider range of unlawful actions than just the ones mentioned by UNCLOS.[232] Article 3 of the SUA Convention reads as follows:

'1. Any person commits an offence if that person unlawfully and intentionally:

1. seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; or
2. performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; or
3. destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that 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

[231] Andronja, Brcko, Pavic, Greidanus (note 203 above).
[232] Compare, for example, Security Council of the United Nations *Resolution 579* (18 December 1985) UN Doc., S/RES/579 and Maritime Safety Committee of the IMO *MSC/Circ.443* (26 September 1986); J van Hauwaert *'The importance of the SUA Convention in the fight against violence at sea'* (2018) 1, 9, 14.

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; or

6. communicates information which he knows to be false, thereby endangering the safe navigation of a ship; or

7. injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f).

2. Any person also commits an offence if that person:

1. attempts to commit any of the offences set forth in paragraph 1; or

2. abets the commission of any of the offences set forth in paragraph 1 perpetrated by any person or is otherwise an accomplice of a person who commits such an offence;

3. 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 paragraph 1, subparagraphs (b), (c) and (e), if that threat is likely to endanger the safe navigation of the ship in question.'

As mentioned in the beginning, the scope of the SUA Convention is much larger than the scope provided in UNCLOS as the purpose of the SUA Convention was to broaden the narrow definition of the term 'piracy' and to make the Convention applicable to a larger number of different situations at sea.[233] Unlike Article 101 of UNCLOS, the SUA Convention is not limited to acts committed on the high seas only.[234] According to Article 4(1) of the SUA Convention, the Convention applies 'if a ship is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single State'. However, the ship must still operate in an international context and the Convention only applies to a ship that is operating in territorial waters of a state when it is scheduled to go on an international voyage.[235] It also does not apply if the ship operates in the territorial waters of only one state. Even though the SUA Convention´s scope regarding the location of a ship is much wider than the one in Article 101 of UNCLOS, the legal problems regarding an act of cyber piracy have one problem in common. As discussed above, a cyber pirate could have two possible targets: The onboard ICT system of the ship at sea or the ICT system of the SCC. If the ICT system of the ship itself is attacked while the ship is navigated through or from waters beyond the outer limit of the territorial sea of a single state the attack falls under the geographical scope of the SUA

[233] Hauwaert (note 232 above) 22.
[234] Ibid.
[235] Ibid.

Convention. However, problematic is the attack of the ICT system of the SCC on land in the case when the attack is only used to interfere with the ship at sea. The answer must be the same as given for the geographical scope under Article 101 of UNCLOS: it does not seem reasonable to only look at the starting point of an attack but to look at the intended outcome. If the SCC's ICT system is hacked only to interfere with the ship the attack itself must be understood as launched against the ship. Therefore, the answer whether or not the act of cyber piracy fulfils the first requirement depends only on where the unmanned and autonomous ship is located at the moment of the attack.

The SUA Convention is not limited to acts committed for private ends. According to Article 3 of the SUA Convention 'any person' that commits one of the mentioned offences, is an offender. The wording shows that the SUA Convention does not require any specific motives and also includes political, ethnic, religious, or ideological driven motivations. It is even arguable that any person that is acting on behalf of a government could be classified as an offender as the SUA Convention does not require any specific motivations at all.[236] Article 3 of the SUA Convention does not require specific motives on the part of the offender for acts to be qualified as offences. The only requirement is that the act must be committed 'unlawfully and intentionally'. As already discussed the motivation of a cyber pirate to attack a ship does not differ from the motivation of a pirate. Both attacks could be committed for several reasons. In conclusion, the element 'any person' includes a cyber pirate's motivations.

Article 3 of the SUA Convention provides a list of different possible offences. Some of them do not cover the act of cyber piracy. Article 3(2) of the SUA Convention concerns the performance of 'an act of violence against a person on board a ship'. As pointed out above, a cyber piracy attack cannot be qualified as an act of violence. Article 3(4) of the SUA Convention qualifies the placement of 'a device or substance which is likely to destroy that ship or cause damage to that ship' as an offence. Such an act also does not include any cyber-related activities as this sub-paragraph refers to any explosive devices such as bombs or dynamite or any flammable substance such as petrol.

[236] Some governments such as the Government of Kuwait and the Government of Saudi-Arabia wanted to include some wording that refers to illegal acts committed on behalf of governments. Compare IMO Doc. SUA/CONF/CW/WP.15 (3 March 1988) 1. The proposals were rejected by the Diplomatic Conference. Compare Hauwaert (note 232 above) 25. In conclusion the wording 'any person' can only mean that there is no difference on what behalf the offence is committed. Otherwise the law would exclude this particular motivation.

However, some of the offences described in Article 3 of the SUA Convention are more likely to be fulfilled in the case of an attack by a cyber pirate. Those offences can be divided into two groups. The first group includes those offences that describe an act that could include acts of cyber piracy. The second group contains those offences that describe a possible outcome of a cyber piracy attack. Article 3(1) of the SUA Convention and Article 3(6) of the SUA Convention belong to the first group. Article 3(1) of the SUA Convention speaks of the seizing or exercising of control over a ship by force or threat thereof or any other form of intimidation. The term 'exercises control over a ship' could also include the control over a ship by hacking into the ship's ICT system. However, the control must be gained by 'force or threat thereof or any other form of intimidation'. The use of words refers again to some sort of violent behaviour that excludes a cyber piracy attack for the above-mentioned reasons. Even though a cyber pirate could also threaten the authorities by, for example, telling them that he or she will destroy navigational communication of a vessel by hacking into its system, the control over a vessel would then not be caused by the attack itself but by the threat. Therefore, the act of cyber piracy does not fulfil the requirements of Article 3(1) of the SUA Convention.

Article 3(6) of the SUA Convention qualifies the communication of false information as an offence if it endangers the safe navigation of a ship. This could also include false information showing up on the onboard computer of a ship or SCC as a result of a cyber piracy attack. The above- mentioned cyber penetration test by Naval Dome showed that a cyber-attack may sometime not even be noticed by anyone. The hacked system may not report the attack but could display a perfectly normal and under control situation to the personnel. For example, the cyber pirate could send false information that the ship is on course. This could endanger the safe navigation of the ship. The ship would be controlled by a third party without the authorities knowing about it. The act of cyber piracy fulfils the requirements of Article 3(6) of the SUA Convention.

Article 3(3) of the SUA Convention belongs to the second group. This alternative concerns the destruction or damaging of a ship or its cargo which is likely to endanger the safe navigation of that ship. One result of a cyber piracy attack may be that the ship or its cargo could be destroyed or at least damaged. In such a case a cyber piracy attack does fulfil Article 3(3) of the SUA Convention as well.

Article 3(5) of the SUA Convention belongs to both groups. The first half of the sub-paragraph refers to the destruction or damage of maritime navigational facilities and therefore describes a result of an action. The second half concerns the interference with the operation and therefore describes an action. The first alternative could also be the result of cyber piracy attacks, for example, in the case that the ship is used as a weapon against port facilities. The second alternative describes the cyber-attack on the facility itself and could apply to the SCC which is a navigational facility. Article 3(5) of the SUA Convention is also applicable to cyber piracy attacks.

In conclusion, the SUA Convention with its broader and more flexible terms can be linked to the act of cyber piracy even though cyber threats were not common when the SUA Convention was adopted. However, the SUA Convention only covers specific results of an attack such as damages to the ship and cargo. Unfortunately, the first alternative of Article 3 of the SUA Convention does not include cyber piracy attacks as it refers only to any act of violence. Therefore, the SUA Convention lacks an overall definition of the term 'cyber piracy'.

3.2.3 German law

German law does not give any definition of the term 'piracy'. German courts use two different sections in the StGB combined to define piracy. Section 316c(1) number 1b of the StGB reads as follows: '(1) Whosoever 1. uses force or attacks a person's decision-making freedom or engages in the other practices in order to gain control of, or influence the navigation of (a) (…) (b) a ship employed in civil maritime traffic; or 2. (...) shall be liable to imprisonment of not less than five years. (…)' Section 239a(1) of the StGB states the following: '(1) Whosoever abducts or gains physical control of a person in order to exploit, for the purpose of blackmail (section 253), the victim's concern for his own welfare or the concern of a third person for the welfare of the victim, and whosoever for the purpose of blackmail exploits a person's situation thus caused by him shall be liable to imprisonment of not less than five years.' Section 316c(1) number 1 of the StGB contains three possible actions: The use of force, an attack on the freedom of decision of a person, or an engagement in other conduct to gain control over a ship or influence the navigation of a ship employed in civil maritime traffic. Section 239a(1) of the StGB contains only one action: The abduction or gain of physical control of a person to blackmail[237] by concerning the victim or a third party for the welfare of the victim. At first glance, the two first alternatives provided by section 316c(1) number 1 of the StGB line up with the definition

[237] The offence of blackmailing can be found in section 253 of the StGB.

of the term 'piracy' given in Article 101 of UNCLOS. Both share the characteristics of the use of some act of violence and have a ship as a reference point of the action. The difference between the two definitions is that in Article 101 of UNCLOS the use of force must be directed against another ship, person, or property on board this ship. Section 316c(1) number 1 of the StGB does not substantiate the point of reference to violence any further. Under German law, it is sufficient that any person or thing becomes a victim of violence, whether onboard or aboard a ship. However, the term 'force' refers to any physical activity to overcome the resistance that has been expected by the victim and is therefore comparable with the term 'violence' used in Article 101 of UNCLOS. The term 'attacks the freedom of decision' means any threat with a future action that will be unpleasant to the victim such as an act of violence. The threat must be used to gain control over the ship. Both alternatives only refer to physical actions. The act of cyber piracy is therefore not included. The same conclusion applies to section 239a(1) of the StGB. However, what is questionable is whether or not the third alternative could be relevant. According to section 316c(1) number 1 of the StGB whosoever 'engages in the other conduct in order to gain control of, or influence the navigation of a ship employed in civil maritime traffic' shall also be liable. This last alternative of the offence refers to any methodically calculated overall behaviour such as the influence of communication and navigation devices with, inter alia, technical and electronic instruments.[238] This includes, in particular, those manipulations that change the course of the ship by any sort of misleading or disruption.[239] An act of violence is not necessary. A cyber piracy attack on the onboard ICT system of an autonomous and unmanned ship that leads to the gain of control or any other influence over the navigation of a ship would therefore fulfil the requirements. In conclusion, the act of cyber piracy falls under the same law as piracy.

3.2.4 South African law

In South Africa, the term 'piracy' is defined in the Defence Act No. 42 of 2002. Section 24 of the Defence Act states the following:

'For the purpose of this Act, piracy is -

> (a) any illegal act of violence or detention, or any act of depredation, committed for private ends by the crew, including the Master, or passengers of a private ship or private aircraft, and directed -

[238] T Fischer *'Strafgesetzbuch und Nebengesetze'* (2020), § 316, 2.
[239] Ibid.

(i) on the high seas, against another ship or aircraft, or against persons or property on board such ships or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any state;

(b) any act of inciting or of intentionally facilitating an act contemplated in paragraph (a) or (b).'

This section defines the term 'piracy' by using almost the same wording as Article 101 of UNCLOS. The section also includes the element 'any illegal act of violence or detention, or any act of depredation'.[240] There is no reason for a different interpretation of the terms under the Defence Act. This means that to qualify as an act of piracy, the cyber piracy attack would have to include a component of violence which is not the case. This is why cyber piracy does not fall under the definition of section 24 of the Defence Act.

Even though section 24 of the Defence Act does not include cyber piracy, it might be helpful to take a look at sections 10 and 15 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act No. 33 of 2004[241] (POCDATARA). This act does not deal with the term 'piracy' but refers to the offence as related to hijacking a ship or endangering the safety of maritime navigation. Section 10 POCDATARA states the following:

'Any person who intentionally –

(a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation;

(b) performs any act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship;

(c) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship;

(d) 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 causes damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship;

(e) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if such acts are likely to endanger the safe navigation of a ship;

[240] Section 24(1)(a) of the Defence Act.
[241] Protection of Constitutional Democracy against Terrorist and Related Activities Act No. 33 of 2004.

(f) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safe navigation of a ship; or

(g) injures or kills a person, in connection with the commission of any of the acts set forth in paragraphs (a) to (f), is guilty of an offence relating to hijacking a ship or endangering the safety of maritime navigation.'

South African law almost uses the wording as Article 3 SUA Convention. Therefore, Section 10(a), (b), and (d) are for the same reasons not applicable as Article 3(1), (2), and (4) SUA Convention. Section 10(c), (e), and (f) of the Act applies for the same reasons as Article 3(3), (5), and (6) SUA Convention.

3.3 Cybercrime: Definition and Overlap to Cyber Piracy

3.3.1 European Convention on Cybercrimes

The European Convention on Cybercrime does not define the term 'cybercrime' or 'cyber-attack'. Chapter I of the Convention on Cybercrimes that deals with definitions does not provide any generalised definition of the term. Chapter II however includes specific offences. Title 1 under Chapter I of the Convention on Cybercrime deals with the offences against the confidentiality, integrity, and availability of computer data and systems. This includes illegal access[242], illegal interception[243], data interference[244], system interference[245], and misuse of devices[246]. The Convention on Cybercrimes demands that 'each party shall adopt legislative and other measures as may be necessary to establish a criminal offence under its domestic law'[247] for each offence. The Convention on Cybercrime itself does not define these offences further. Even though the act of cyber piracy is very likely to be included under the above offences it is necessary to take a look at the domestic law for a proper definition of the terms.

3.3.2 German law

In August 2007, German law incorporated the goals of the Convention on Cybercrime into national criminal law. Among the most significant changes are the extension of the criminal liability per section 202a of the StGB that now includes unauthorised access to data, the

[242] Article 2 of the Convention on Cybercrime.
[243] Article 3 of the Convention on Cybercrime.
[244] Article 4 of the Convention on Cybercrime.
[245] Article 5 of the Convention on Cybercrime.
[246] Article 6 of the Convention on Cybercrime.
[247] Compare Article 2-6 of the Convention on Cybercrime.

introduction of phishing as a criminal offence (section 202b of the StGB), and the criminalisation of acts preparatory to data espionage and phishing (section 202c of the StGB). The newly introduced section 303b(1) of the StGB reads as follows: 'Whosoever interferes with data processing operations which are of substantial importance to another by committing an offence under section 303a (1)'. Section 303(a)(1) of the StGB reads 'Whoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a(2)) incurs a penalty of imprisonment for a term not exceeding two years or a fine.' Section 202a(2) of the StGB defines data as 'only those which are stored or transmitted electronically, magnetically or otherwise in a manner which is not immediately perceptible'. Section 303(a)(1) of the STGB includes four different acts: deleting, suppressing, rendering, or altering data. Deleting includes the use of a computer virus that deletes data or overwrites it.[248] The suppression for data is given if the authorised person can temporarily not access data.[249] This can be done, for example, by changing passwords to lock out the entitled person.[250] Rendering data can be done by adding or partially deleting or changing data or changing the program code.[251] Altering data means changing it for example using viruses, worms, or software.[252] Any of these acts has to lead to interference with data processing according to section 303b of the StGB. If a cyber pirate would try to take control over a ship he or she would have to access its system. This would be done by manipulating data that controls the ship's navigation. In conclusion, section 303(a)(1) of the StGB includes cyber piracy.

3.3.3 South African law

South Africa regulates cybercrime in the Cybercrimes and Cybersecurity Bill. Part I of the Cybercrime and Cybersecurity Bill defines different cybercrimes including the unlawful access, unlawful interception of data, unlawful acts with respect of software or hardware tool, unlawful interference with data or computer program, the unlawful interference with a computer data storage medium or computer system, unlawful acquisition, the possession, the provision, the receipt or use of passwords, the access code or similar data or device as well as cyber fraud, cyber forgery and uttering, cyber extortion, aggravated offences, and theft of incorporeal property. Section 2 of the Cybercrimes and Cybersecurity Bill reads as follows:

[248] J Heidrich and S Tschoepe *'Rechtsprobleme der E-mail Filterung'* Multimedia und Recht (2004) 79.
[249] Ibid.
[250] Ibid.
[251] T Fischer *'Strafgesetzbuch mit Nebengesetzen'* (2020) § 303a 11; I Vassilaki and S Martens *'Computer und Internet-Strafrecht'* (2003) 47.
[252] Ibid.

‘(1) Any person who unlawfully and intentionally accesses –

(a) data;

(b) a computer program;

(c) a computer data storage medium; or

(d) a computer system, is guilty of an offence.

(2) For purposes of this section a person accesses –

(a) data when the person is in a position to –

(i) alter, modify or delete the data;

(ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(iii) obtain its output; or

(iv) otherwise use the data;

(b) a computer program when the person is in a position to –

(i) alter, modify or delete the computer program;

(ii) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(iii) cause a computer program to perform any function;

(iv) obtain its output; or

(v) otherwise use the computer program;

(c) a computer data storage medium when the person is in a position to –

i) access data as contemplated in paragraph (a) or access a computer program as contemplated in paragraph (b), stored on the computer data storage medium;

(ii) store data or a computer program on a computer data storage medium; or

(iii) otherwise use the computer data storage medium; or

(d) a computer system when the person is in a position to –

(i) use any resources of;

(ii) instruct; or

(iii) communicate with, a computer system.

(3) For purposes of subsection (1), the actions of a person, to the extent that such actions exceed his or her lawful authority to access data, a computer program, a computer data storage medium or a computer system, must be regarded as unlawful.’

Section 2(1) of the Cybercrimes and Cybersecurity Bill qualifies any intentional access to data, a computer program, a computer storage medium, or a computer system as an offence. In comparison to German law, South African law distinguishes between different accessible locations. If a cyber pirate wants to bring an autonomous ship under his control he or she will have to access its computer system. According to section 2(2)(d) of the Cybercrimes and Cybersecurity Bill, a person accessed a computer system when the person is in a position to (i) use any resources of, (ii) instruct, or (iii) communicate with a computer system. The cyber pirate will intend to instruct the computer system to change its route according to his or her plans. In conclusion, section 2(1) of the Cybercrimes and Cybersecurity Bill includes the act of cyber piracy.

3.4 Concluding Remarks

The act of cyber piracy is not an act of piracy as defined in Article 101 of UNCLOS because it is not an act of violence. As a consequence, numerous regulations under UNCLOS that describe what should be the proper reaction to acts of piracy also do not apply. Article 100 of UNCLOS, for example, sets out the 'Duty to cooperate in the repression of piracy'. Article 110 of UNCLOS allows States to exercises a right to visit ships suspected of being engaged in piracy. Both Articles play a critical role in the fight against piracy but cannot be applied to cyber piracy even though the motivations and objectives of both crimes are the same. However, the SUA Convention with its broader scope covers cyber piracy in some cases but misses an overall definition of the term. Under German law, a cyber pirate and a pirate both fulfil the elements of section 316c of the StGB. At first glance, this circumstance may give the impression that cyber piracy and piracy are subject to the same definition. However, this is questionable because the StGB does not speak of piracy or cyber-attacks at all but only criminalises the attack on maritime traffic. This open definition allows equal classification of a variety of different acts including piracy and cyber piracy. South African law defines the term piracy under section 24 of the Defence Act that is very similar to the one in Article 101 of UNCLOS and therefore excludes cyber piracy for the same reason. The act of cyber piracy can be defined under German and South African cyber-related law. German law distinguishes between the different ways of manipulating data. South African law distinguishes between the different access points. Both laws however include the act of cyber piracy. The European Convention of Cybercrime does not include any definitions.

4 DISCUSSION FROM AN INTERNATIONAL LAW PERSPECTIVE

4.1 International Legislation to Prevent Cyber Piracy

4.1.1 Introduction

The most effective way to minimise damage caused by cyber piracy is to establish sufficient measures and regulations to prevent it from the start. Because cyber piracy includes elements of two crimes of international concern, the best way to respond to the threat of cyber piracy is through international instruments. As cyber piracy is a crime that is new to the maritime world there is no international convention that deals with the topic exclusively. Some regulations however already concern cyber-attacks. The following chapter presents some international instruments that could help to prevent cyber piracy.

4.1.2 The International Ship and Port Facility Security Code

On 1 July 2004, the IMO published the International Ship and Port Facility Code (ISPS Code). This Code is an amendment to the Safety of Life at Sea Convention (SOLAS)[253] that entered into force under SOLAS Chapter XI-2. It presents security measures for preventing attacks on ships and port facilities and applies to ships engaged in international voyages. The ISPS Code is divided into two parts. Part A contains 19 sections dealing with mandatory provisions while Part B contains 19 sections of voluntary guidance on how to best comply with the mandatory requirements.[254] The objective of the ISPS Code according to section 1.2 of the ISPS Code is to establish an international framework that helps to detect and prevent security threats against ships and port facilities and to ensure maritime security on an international level by exchanging security-related information and by reacting with the change of security levels by having a plan in place.[255] To discover if the code addresses cyber piracy the following questions must be answered: Does the ISPS Code apply to unmanned and autonomous ships and does it cover the threats of cyber piracy?

The first focus will be on the question of whether or not the Code generally applies to unmanned and autonomous operations by analysing each section of Part A of the ISPS Code. Sections 1 to 4 of the ISPS Code include general information, definitions, the application, as well as the responsibilities of the contracting governments. According to section 3.1 of the ISPS Code, the

[253] 1184, 1185 UNTS 2. Adopted: 01.11.1974; EIF: 25.05.1980.
[254] Compare section 1.1 of the ISPS Code
[255] Compare the objectives set out in section 1 of the ISPS Code.

code applies to passenger ships, cargo ships, and mobile offshore drilling units as well as to port facilities serving such ships engaged on international voyages. The ISPS Code does not apply to warships, naval auxiliaries, or other ships owned or operated by a contracting government or used only on government non-commercial services according to section 3.3 of the ISPS Code. None of the mentioned sections exclude ships because of their specific manning or operating manners. Therefore, sections 1 to 4 of the ISPS Code apply to unmanned and autonomous ships.[256] Section 5 of the ISPS Code deals with the 'Declaration of Security'. Section 5.2., section 5.4.1, and section 5.4.2 of the ISPS Code require that the Declaration of Security shall be completed by the ship´s master or the ship's security officer. As discovered in chapter 2 of this thesis, a ship's master can only operate from onboard a ship. The remote-controller, the supervisor, or the pre-programmer of a ship are not considered masters of a ship. According to section 2.1.6 of the ISPS Code, a ship security officer is 'the person on board the ship, accountable to the master, designated by the company as responsible for the security of the ship, including implementation and maintenance of the ship security plan (...)'. A ship security officer is therefore a person that is operating on the ship and cannot be located onshore. Section 5 of the ISPS Code is, therefore, not applicable to unmanned ships as it is a requirement to have at least a master or a ship security officer onboard.[257] It would only apply to autonomous ships that are under the control of a bridge crew but not under the control of the SCC. Section 6 of the ISPS Code requires the company to ensure that the ship's security plan contains a clear statement emphasizing the ship´s master´s authority[258]. It also states that the company security officer, the ship´s master, and the ship security officer are given the necessary support to fulfil their duties and responsibilities.[259] In correspondence with section 5 of the ISPS Code, this section also speaks of personnel fulfilling their duties on board the ship and does not apply to unmanned operations. The same applies to section 7 of the ISPS Code which deals with the ship's security and requires that the performance of all ship security duties is ensured by the ship security officer who in correspondence with the port facility security officer shall liaise and coordinate the appropriate actions.[260] Section 8 of the ISPS Code deals with the ship's security assessment, section 9 of the ISPS Code with the ship's security plan, and section 10 of the ISPS Code with the records. All three sections do not speak of any personnel on board and

[256] S Ota *'Identification of IMO Regulations relating to Unmanned Operations of Maritime Autonomous Surface Ships - SOLAS Convention and Related Mandatory IMO Instruments' Papers* of National Maritime Research Institute, Volume 17, Issue 3, (2018) 267.
[257] Ibid.
[258] Compare section 6.1 of the ISPS Code.
[259] Compare section 6.2 of the ISPS Code.
[260] Ota (note 256 above).

are in general applicable to unmanned and autonomous ships. Section 11 of the ISPS Code also generally applies to unmanned and autonomous ships as it describes the obligation of a company security officer. However, the general application excludes section 11.2.10 of the ISPS Code. This section requires that a company security officer shall ensure effective communication and cooperation with the ship security officer. Therefore, it speaks of communication with personnel onboard the ship. Also, not applicable to unmanned operations are section 12 of the ISPS Code that deals with the ship's security officer himself and requires that an officer shall be designated on each ship[261] and section 14 of the ISPS Code that deals with port facility security and requires the ship security officer.[262] Section 13 of the ISPS Code deals with the training, the drills, and the exercises on ship security and generally applies to unmanned and autonomous ships. Sections 15 to 19 of the ISPS Code are applicable as they do not speak of any personnel on board a ship. In addition to the above-mentioned, Part B section 4.28 of the ISPS Code reads as follows:

> 'In establishing the minimum safe manning of a ship the Administration should take into account that the minimum safe manning provisions established by regulation V/143 only address the safe navigation of the ship. The Administration should also take into account any additional workload which may result from the implementation of the ship's security plan and ensure that the ship is sufficiently and effectively manned.'

This section makes it clear, that unmanned ships are generally do not fall under the scope of the ISPS Code. In conclusion, the ISPS Code requires that a ship´s master and/or a ship security officer are on board a ship.[263] Especially section 12 of the ISPS Code states very clearly that a ship security officer must be operating onboard each ship. Therefore, it does not address unmanned and autonomous operations.

To answer the second question of whether or not the ISPS Code covers the threat of cyber piracy it will first be necessary to examine the code's security scope. The ISPS Code generally speaks of security incidents and, therefore, includes cyber incidents as well as any other threat. Section 7 of the ISPS Code deals with the ship's security. Ships are required to apply incremental protective security measures according to the following levels: Security level 1 is according to section 2.1.9 of the ISPS Code the level for 'which minimum appropriate protective security

[261] Compare section 12.1 of the ISPS Code.
[262] Ota (note 256 above).
[263] Ota (note 256 above).

measures shall be maintained at all times'. Following section 2.1.10 of the ISPS Code security level 2 comes in force 'for a period of time as a result of a heightened risk of security incidents' and adds additional protective security measurements. Finally, security level 3 requires according to section 2.1.11 of the ISPS Code 'even further specific protective security measures for a limited period of time when a security incident is probable or imminent'. According to section 7.1 of the ISPS Code, 'a ship is required to act upon the security levels set by the Contracting Governments'. Section 7.2 of the ISPS Code sets out what activities should be carried out to identify security incidents and what preventative measures should be taken (security level 1). This should be done 'by ensuring the performance of all ship security duties; controlling access to the ship; controlling the embarkation of persons and their effects; monitoring restricted areas to ensure that only authorised persons have access; monitoring of deck areas and areas surrounding the ship; supervising the handling of cargo and ships stores; and ensuring that security communication is readily available.' According to section 9 of the ISPS Code, each ship must carry a ship security plan that should include the specific measurements for security levels 2 and 3 considering the guidance given in Part B of the ISPS Code.[264] Section 2.1.4 of the ISPS Code defines the ship security plan as a 'plan developed to ensure that application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units, and ship's stores within the port facility from the risk of a security incident'. According to section 9.4 of the ISPS Code, the plan shall address, at least, the following:

> '1. measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;
> 2. identification of the restricted areas and measures for the prevention of unauthorized access to them,
> 3. measures for the prevention of unauthorized access to the ship;
> 4. procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
> 5. procedures for responding to any security instructions Contracting Governments may give at security level 3;
> 6. procedures for evacuation in case of security threats or breaches of security;
> 7. duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

[264] Compare section 9.1 and section 9.4 of the ISPS Code.

8. procedures for auditing the security activities;
9. procedures for training, drills and exercises associated with the plan;
10. procedures for interfacing with port facility security activities;
11. procedures for the periodic review of the plan and for updating;
12. procedures for reporting security incidents;
13. identification of the ship security officer;
14. identification of the company security officer including 24-hour contact details;
15. procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
16. frequency for testing or calibration of any security equipment provided on board;
17. identification of the locations where the ship security alert system activation points are provided and
18. procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.'

Part B sections 8, 9, and 13 of the ISPS Code provide the relevant guidance on how to fulfil the mentioned ship security measurements. Section 8 of the ISPS Code deals with the security assessment which according to section 8.3 of the ISPS Code should address the following elements on board or within the ship: the physical security, the structural integrity, the personnel protection systems, the procedural policies, the radio and telecommunication systems, including computer systems and networks, and other areas that may if damaged or used for illicit observation, pose a risk to persons, property, or operations onboard the ship or within a port facility. Most of the listed activities address physical security but the code also mentions a ship's computer system and networks. This also includes any computer system of an autonomous ship and its pre-programmed or remote-controlled onboard network.

Therefore, the ISPS Code only superficially covers the threats of cyber piracy. The actions that are considered in the code are mainly of the physical type including physical access control, guards, patrols, and prevention of physical pirate attacks. The different facets of cyber-attacks in general and cyber piracy, in particular, are not addressed.
`

4.1.3 The International Safety Management Code

The International Safety Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code) is an international standard for the safe management of ships at sea as well as for the prevention of pollution. It was originally approved by the IMO in the year 1993 and was only made mandatory five years later.[265] Its objectives as set out in section 1.2 of the ISM Code are to 'ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, and to property'. The ISM Code is separated into two Parts. Part A deals with implementation and Part B with certification and verification. Chapter IX of SOLAS requires compliance with the ISM Code.[266] For the ISM Code, the same questions arise as for the ISPS Code: Does the Code apply to unmanned and autonomous ships and does it address the threat of cyber piracy?

Section 1 of the ISM Code includes general information such as definitions and objectives. According to section 1.3 of the ISM Code, the ISM Code applies to all ships meaning all commercial ships over 500 GT as the ISM Code is a chapter in SOLAS. This means it is generally applicable to unmanned and autonomous ships. In the following most sections of the ISM Code do not exclude unmanned and autonomous operations. The wording of some of the sections of the ISM Code specifically considers the personnel at the SCC. Section 2 of the ISM Code describes the safety and environmental protection policy. According to section 2.2 of the ISM Code, the company should ensure the protection policy both, ship-based and shore-based. The wording 'shore-based' explicitly includes personnel onshore and does, therefore, also cover SCC staff. The same applies to section 3 of the ISM Code where the Code refers to shore-based support. Other sections could be interpreted as optional. Section 4 of the ISM Code states the following:

> 'To ensure the safe operation of each ship and to provide a link between the Company and those on board, every Company, as appropriate, should designate a person ashore having direct access to the highest level of management.'

Even though this section speaks of people on board, it can be understood as *if* people are on board. The person ashore could also be a person at the SCC. Sections 7 to 13 of the ISM Code

[265] International Maritime Organisation *'ISM Code and Guidelines on Implementation of the ISM Code'* available at *http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx*, accessed 21 January 2021.
[266] Ibid.

do not speak of any personnel and generally apply to unmanned and autonomous ships. However, sections 5 and 6 of the ISM Code refer to the ship's master's authority and responsibility. According to section 5.1 of the ISM Code, the company should define and document the master's responsibilities. Additionally, section 6.2 of the ISM Code reads as follows:

> 'The Company should ensure that each ship is: 1. manned with qualified, certificated and medically fit seafarers in accordance with national and international requirements; and 2. appropriately manned in order to encompass all aspects of maintaining safe operation on board. Refer to the Principles of minimum safe manning, adopted by the Organization by Resolution A.1047(27).'

Even if the wording 'appropriately manned' could generally also include no manning in a case that may be appropriate, the current manning regulations consider a ship only appropriately manned if it has a certain number of people on board.[267] In conclusion, the ISM Code applies to unmanned operations with the exception of section 6.2 of the ISM Code that only applies if the current manning regulations will be changed.

The next step is to take a closer look at whether or not the risks of cyber piracy are addressed in the ISM Code. Section 2.1 of the ISM Code states that the company is responsible to establish a safety and environmental protection policy that describes how the objectives of the ISM Code shall be achieved. Section 1.2.2 of the ISM Code states that the safety-management objectives of the company should, inter alia 'provide for safe practices in ship operation and a safe working environment; assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards; and, continuously improve safety-management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection'. Section 1.2.3 of the ISM Code adds that the safety-management system should ensure 'compliance with mandatory rules and regulations; and that applicable codes, guidelines and standards recommended by the Organization, Administrations, classification societies and maritime industry organizations are taken into account'. According to section 1.1.4 of the ISM Code, Safety Management System means 'a structured and documented system enabling Company personnel to implement effectively the Company safety and environmental

[267] T Forster *'The Unmanned Ship Sets Sail - Is South Africa Prepared to Open the Ship Register?'* (2017) 22, 23; Compare Article 94(3)(b) of UNCLOS; Compare regulation 95(1) Merchant Shipping (Safe Manning, Training, and Certification) Regulations of 2013.

protection policy'. Overall, the ISM Code has a strong focus on physical security and therefore, does not cover cyber piracy as it predates much of its current concerns.[268]

4.1.4 The IMO Guidelines on Maritime Cyber Risk Management

In 2017, the International Maritime Organisation issued the Guidelines on Maritime Cyber Risk Management (in the following referred to as the Guidelines). As set out by the Organisation the Guidelines were drafted because of the 'urgent need to raise awareness on cyber risk threats and vulnerabilities'.[269] They provide 'high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities'.[270] The Guidelines are separated into a preamble followed by four sections. The first section stresses the necessity of risk management to safe and secure shipping operations and sets the goal of 'supporting safe and secure shipping'[271]. The term 'maritime cyber risk' is defined in section 1.1 of the Guidelines as 'a measure of the extent to which a technology asset is threatened by a potential circumstance of event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised'. Section 2 of the Guidelines focuses on background information and the application of the Guidelines. Section 2.1.1 of the Guidelines lists eight vulnerable systems: the bridge systems, the cargo handling, and management systems, the propulsion and machinery management and power control systems, the access control systems, the passenger servicing, and management systems, the passenger facing public networks, the administrative and crew welfare systems, and the communication systems. Section 2.2 of the Guidelines states that the Guidelines are primarily intended as a recommendation for all organizations in the shipping industry. Section 3 of the Guidelines deals with the elements of cyber risk management. Section 3.1 of the Guidelines defines the term cyber risk management 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'. Section 3.5 of the Guidelines then presents the following elements of cyber risk management:

---

[268] International Maritime Organisation *'Guidelines on Cyber Risk Management'* (5 July 2017) MSC-FAL.1/Circ.3; The Maritime Safety Committee adopted Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems to take cyber risk management into account in accordance with the objectives and requirements of the ISM Code.

[269] Compare Preamble section 1 of the Guidelines on Cyber Risk Management.

[270] Compare Preamble section 2 and Annex section 1.1 of the Guidelines on Cyber Risk Management.

[271] Compare Annex section 1.3 of the Guidelines on Cyber Risk Management.

‘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;

2. Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations;

3. Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner;

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;

5. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.’

Section 4 of the Guidelines provides a list of additional guidance and standards such as the BIMCO Guidelines on Cyber Security Onboard Ships and the ISO/IEC 27001 Standard on Information Technology. Both will be subject to the following sub-chapters. In conclusion, the Guidelines on Cyber Risk Management address the risks of cyber piracy and include unmanned and autonomous ships as well. However, it is problematic that the Guidelines are broad and do not go into details regarding the finer steps on how to deal with cyber piracy. Therefore, they are predominantly useful in raising awareness and are of good use in outlining the many vulnerable systems within maritime operations.

4.1.5 The Maritime Cyber Risk Management in Safety Management Systems

The Maritime Safety Committee (MSC), adopted Resolution MSC.428(98) - the Maritime Cyber Risk Management in Safety Management Systems (SMS). The Resolution encourages administrations, classification societies, shipowners and operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders to ensure that cyber risks are appropriately addressed in existing safety management systems as defined in the ISM Code no later than the first annual verification of the company's document of compliance after 1 January 2021.[272] This was done because of the ‘urgent need to raise awareness on cyber risk threats and vulnerabilities’[273]. This should be done by bearing the

[272] Compare section 2 ‘ENCOURAGES’ of the Maritime Cyber Risk Management in Safety Management Systems.

[273] Compare section ‘RECOGNIZING’ of the Maritime Cyber Risk Management in Safety Management Systems.

Guidelines on Maritime Cyber Risk Management in mind and including cyber risks in the SMS.[274] The SMS shows that the authorities concluded that the ISM Code currently does not cover cyber-related risks. To include the threat into the SMS is the right approach especially because it will become mandatory to do so by 2021. However, even though it will no longer be compulsory to include cyber risk management the regulatory framework on how to include cyber piracy is not yet fully developed as the resolution only refers to the above-mentioned IMO Guidelines.

4.1.6 The Guidelines on Cyber Security Onboard Ships

The Guidelines on Cyber Security Onboard Ships (in the following referred to as the Guidelines) were produced and supported by the Baltic and Maritime Council (BIMCO) together with the following leading shipping organisations CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI, and WORLD SHIPPING COUNCIL.[275] BIMCO has published the latest edition (version 3) of the Guidelines in December 2018. The Guidelines provide practical recommendations on maritime risk management covering both cyber security and cyber safety.[276] They are aligned with the IMO Resolution MSC.428(98) and the IMO Guidelines.[277] The document aims to offer guidance to shipping companies on how to maintain the security of their cyber systems[278] by identifying threats and vulnerabilities, assessing risk exposure, developing protection and detection measures, establishing contingency plans, and responding to and recovering from cyber security incidents.[279] Annex 4 of the Guidelines provides several important definitions of terms, for example, the terms cyber-attack, cyber incident, and cyber risk management. The Guidelines first present cyber threats by listing different possible groups of attackers, their motivations and objectives as well as different types and stages of cyber-attacks. This is followed by possible vulnerabilities. It also includes the response to and the recovery plan of a cyber-attack. Annex 1 of the Guidelines provides a summary of potentially vulnerable systems. This includes some very important systems of unmanned and autonomous ships as well. For example, it includes communication systems such as wireless networks and satellite communication equipment; bridge systems such as integrated navigation systems and positioning systems; propulsion and machinery management as well as power control systems such as power management and emergency response systems; access control

[274] Compare section 'RECALLING' of the Maritime Cyber Risk Management in Safety Management Systems.
[275] BIMCO *'Guidelines on Cyber Security Onboard Ships - Version 3'* (December 2018) frontpage.
[276] Ibid 1.
[277] Ibid 1.
[278] Ibid 1.
[279] Ibid 1.

systems such as electronic personnel-on-board systems.[280] Annex 2 of the Guidelines refers to cyber risk management and the SMS.[281] Stating that IMO Resolution MSC.428(98) gives instructions to include cyber risk management into the SMS the annex describes the terms 'identify', 'protect', 'detect', 'respond', and 'recovery' further.[282] To identify a cyber-related risk, the annex recommends implementing roles and responsibilities and, for example, cyber awareness training and IT personnel that understands the potential vulnerabilities.[283] To protect the ship's systems from cyber-attacks the annex suggests implementing risk control measures and developing contingency plans.[284] To detect potential risks, the annex provides a list of possible suspicious activities that should be included in the SMS such as unauthorised access to network infrastructure and suspicious network activity.[285] To respond to a cyber-attack the annex recommends developing and implementing activities and plans to provide resilience and to restore systems necessary to shipping operations.[286] For example, the company should be familiar with onboard IT and OT infrastructure and systems and should be able to maintain the software.[287] In the case of a cyber-attack, the company must be able to recover from it. The annex suggests, identifying measures to back-up and restore cyber systems that are necessary for shipping operations by, for example, checking back-up arrangements for critical systems.[288] Annex 3 of the Guidelines deals with onboard networks. The Guidelines recommend that newly built ships should plan the network layout and network control carefully.[289] Also, it is suggested to monitor data activity to detect any unauthorised data traffic and to implement protection measures in a way that maintains the integrity of the system at any time.[290] In conclusion, the Guidelines provide a wide range of different suggestions that can help to protect a shipping company from cyber-attacks and also from cyber piracy on autonomous ships. However, the Guidelines sometimes refer to personnel on board the ship which means that fully unmanned operations are not always considered.

Overall, even though the Guidelines refer to people on board a ship they are a significant step in the right direction. They are made for the maritime industry only and, therefore, highly

[280] Ibid 40
[281] Ibid 42.
[282] Ibid 42.
[283] Ibid 42.
[284] Ibid 43.
[285] Ibid 44.
[286] Ibid 45.
[287] Ibid 45.
[288] Ibid 45.
[289] Ibid 46.
[290] Ibid 46.

maritime specific. They do not only offer a list of potential threats and vulnerabilities but also present efficient ways to protect systems from cyber incidents. As a result, they cover the risks of cyber piracy very well. What is problematic, however, is that the Guidelines use the term 'cyber-attack'. The definition of this term lines up with the general definition of this term and does not include piracy. Even though the outcome of the attack could be the same as the one of a pirate the overall understanding of the term does not include the same consequences.

Therefore, it is submitted that the term cyber piracy should also be included and defined in the Guidelines. Unfortunately, the Guidelines only provide recommendations and are not mandatory. However, if developed further by adding risks and solutions for fully unmanned and autonomous ships and then used as the base for international regulations that are no longer obligatory to shipping companies, the Guidelines could have a significant impact on safeguarding the modern shipping industry.

4.1.7 The Information Security Management Standards

The Information Security Management Standards (ISO/IEC 27001 Standard on Information technology – Security techniques – Information security management systems – Requirements) (in the following referred to as the Standard) is an information security standard published jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC).[291] It is part of the ISO/IEC 27000 standard series (also known as the ISMS family of standards) that provides a globally recognised framework that lays out best-practice recommendations on information security management.[292] The Standard was first published in 2005 and its latest version is from 2013.[293] It provides requirements for establishing, implementing, maintaining, and continually improving an information security system.[294] The Standard covers all types of organisations, all sizes, and all industries such as banking, healthcare, and government. It lays out the design for an ISMS and can be used as the basis for formal compliance assessment by accredited certification auditors to certify an organisation. Certified compliance by a certification body is entirely optional and a list of mandatory

[291] International Organization for Standardization and the International Electrotechnical Commission *'ISO/IEC 27001 Information Security Management Standards on Information technology – Security techniques – Information security management systems – Requirements'* (June 2017).
[292] International Organization for Standardization and the International Electrotechnical Commission *'ISO/IEC 27001 Information Security Management'* available at *https://www.iso.org/isoiec-27001-information-security.html*, accessed 21 January 2021.
[293] Ibid.
[294] Ibid.

documentation is required to get the certification.[295] The certification auditors check the documentation and fit it for the purpose.[296] According to the ISO survey in the year 2018, there are about 31,000 ISO/EC 27001 organisations with valid certifications worldwide, most of them in East Asia and the Pacific, especially in Japan and China.[297] Even though the Standard comes highly recommended, it is neither compulsory nor available free of charge. If a company wishes to obtain the certification it will have to buy the service. Even though the IMO explicitly refers to the Standard on their website and their Guidelines as one possible way to protect the shipping industry from cyber-attacks, the Standard is not equally relevant as it is a private service and not an international regulation or guideline to secure the shipping industry. It is obligatory as well as costly to obtain a certification.

In conclusion, even though the threat of cyber piracy on unmanned and autonomous ships could be minimised by obtaining certification it would only protect the purchasing company and would not confront the threat in general.

4.2 International Jurisdiction in the Context of Cyber Piracy

4.2.1 Introduction

Both piracy and cybercrimes are typical transnational crimes that involve multiple jurisdictions.[298] In the case of an incident, it is not unusual that several countries are affected by it. As shown in chapter three of this thesis, cyber piracy includes elements of both piracy and cybecrimes, which turn it into a threat with enormous global consequences. The cyber pirates might be Polish citizens that acted from Russia, using an internet service in Italy. The victim may be an unmanned and autonomous container ship flying under the German flag, being in international waters at the time of the attack having Chinese and Korean goods on board that were meant for South African and Namibian buyers: A scenario with countless alternatives and variations. The circumstance that more than one country is affected by one cyber piracy attack leads to the question of which country would have jurisdiction over the enforcement and the prosecution in such a case. The term 'jurisdiction' refers to the authority of a state-granted by

[295] Ibid.
[296] Ibid.
[297] International Organization for Standardization and the International Electrotechnical Commission *'ISO Survey 2018 results – Number of certificates and sites per country and the number of sectors overall'* (2018).
[298] T Syring *'Candide, or Pessimism: Fighting Piracy and Transnational Crime in Uncharted Waters'* Interdisciplinary Political Studies Volume 2, No. 1 Special Issue (March 2012) 49; R McCusker *'Transnational organised cyber crime; Distinguishing threat from reality'* Crime Law and Social Change, Volume 46, Issue 4 (December 2006), 257.

law to affect persons, circumstances, and property in legal matters.[299] It is possible to differentiate between various principles of international jurisdiction. In the following, these different principles are presented and discussed with regard to piracy, cybercrime, and cyber piracy to find out if internationally the acts would be treated differently from one another and if this may lead to yet unsolved legal problems.

4.2.2 The principles of international jurisdiction

As mentioned above, jurisdiction describes the legal authority within a territory over both criminal and civil matters. International jurisdiction refers to the power of a state to be able to act in a legal matter.[300] It addressed questions of criminal law leaving civil jurisdiction to national control.[301] International law provides the following five different principles of jurisdiction: the principle of territoriality, the principle of nationality, the protective principle, the passive personality principle, and the principle of universal jurisdiction.[302]

The most fundamental principle and most common basis of jurisdiction is the principle of territoriality.[303] This principle also serves as the basic principle of jurisdiction in international law.[304] According to the territorial principle, a sovereign state has exclusive authority to exercise its criminal jurisdiction within its territory.[305] The principle also forbids a state to exercise its jurisdiction outside its borders, unless another principle, for example, the principle of nationality applies.[306]

The flag principle means that the flag state has jurisdiction over its ship.[307] The principle is closely related to the principle of territoriality but extends the application of domestic laws to aircraft and ships.[308] Ships and aircraft have the nationality of the states whose flag they fly or in which they are registered and are subject to its jurisdiction.[309] The flag state´s jurisdiction is

---

[299] D Helenios *'The If, How, and When of Criminal Jurisdiction – What is Criminal Jurisdiction Anyway?'* Bergen Journal of Criminal Law and Criminal Justice, Volume 3, Issue 1 (2015) 24.
[300] Ibid.
[301] Ibid.
[302] E Nyman *'Modern Piracy and International Law: Definitional Issues with the Law of the Sea'* (November 2011) 868.
[303] M Vagias and J Dugard *'The territorial jurisdiction of the International Criminal Court'* (2014) 13.
[304] Ibid.
[305] Ibid.
[306] M Gercke *'Understanding Cybercrime: Phenomena, Challenges and Legal Response'* (September 2012) 235.
[307] S Helmersen *'The sui generis nature of flag state jurisdiction'* Japanese Yearbook of International Law 58 (2015) 322.
[308] Gercke (note 306 above) 236; B Sage-Fuller *'The Precautionary Principle in Marine Environmental Law: With Special Reference to High Risk Vessels'* (2013) 36.
[309] Ibid.

exclusive on the high seas but not when the ship is located in the internal waters of another state.[310] The flag state may still have jurisdiction over ships when they are in foreign territorial waters and ports.[311] The most prominent example of the application of the flag principle is the *Lotus case*.[312] This case concerns a criminal trial at the Permanent Court of International Justice which was the result of the collision of a French and a Turkish ship in 1926 that caused the death of eight Turkish citizens.[313] The court ruled that Turkey had jurisdiction to try the French lieutenant. The case was the first to extend the principle of territoriality to cover cases at sea onboard a ship resulting in the flag principle.[314]

The principle of nationality permits a state to exercise jurisdiction in a criminal matter over any of its nationals accused of a criminal offence in another country.[315] This principle has the effect that the national could even be prosecuted for conduct that was committed in a country where the behavior was legal. When the behavior is illegal in both countries it is normally tried in the country the crime was committed. The principle is very useful especially on the high seas where the jurisdiction depends on the country the vessel is registered with as the flag state will most likely be chosen because of fiscal considerations.

The passive personality principle, also known as the passive nationality principle[316], allows states to claim jurisdiction over cases where a foreign national committed a crime abroad that affected their own citizens.[317] The principle deals with the crime's effect rather than where it occurred.[318] This principle appears in numerous international conventions such as the 1979 International Convention Against the Taking of Hostages[319], the 1984 Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment[320], and the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents[321]. Even though the principle is mostly used to prosecute terrorists, the leading case is the *Cutting's Case* where a U.S. citizen published a defamatory publication

[310] Ibid.
[311] D Guilfoyle 'Shipping Interdiction and the Law of the Sea' (2012) 16; D König *'Flag of Ships'* in Max Planck Encyclopaedia of Public International Law, 30-32.
[312] S.S. 'Lotus' France v Turkey, Judgement No 9, PCIJ Series A No. 10 (1927).
[313] M Vagias and J Dugard *'The territorial jurisdiction of the International Criminal Court'* (2014) 13.
[314] Helmersen (note 307 above) 324.
[315] Gercke (note 306 above) 237.
[316] S Sahu *'Passive Personality principle: An Overview'* (6 February 2015).
[317] Ibid.
[318] Ibid.
[319] 1316 UNTS 205. Adopted:17.12.1979; EIF: 03.06.1983.
[320] 1465 UNTS 85. Adopted: 10.12.1984; EIF: 27.06.1987.
[321] 1035 UNTS 167. Adopted:14.12.1973; EIF: 20.02.1977.

against a Mexican citizen in the U.S. state of Texas.[322] The offender was prosecuted under Mexican law. Another example with a maritime aspect is the Achille Lauro incident. In this case, a U.S. court prosecuted the leader of a terrorist group who hijacked a vessel in Egyptian waters and killed an American citizen.[323]

The protective principle, also known as the passive personality principle, can be found in numerous international conventions such as the Convention on the Safety of United Nations and Associated Personnel[324] and the hostages and aircraft-hijacking conventions. A state can refer to this principle if a crime was committed abroad by a non-citizen if the outcome of the case could be considered prejudicial for a national citizen.[325] The reason behind the principle is to ensure that national interests are protected by the state itself to the extent they find necessary without relying on another state.[326]

The fifth principle is the universality principle also called universal jurisdiction which allows for the assertion of jurisdiction in cases where the alleged crime may be prosecuted by all states because it is in the interest of the international community.[327] This principle originally applied to hold pirates and slave traders accountable for their crimes.[328] Today it is relevant concerning numerous serious crimes such as war crimes, crimes against the peace, and crimes against humanity. The principle can be found, for example, in the 1949 Geneva Convention Relative to the Treatment of Prisoners of War[329], the 1973 Convention on the Suppression and Punishment of the Crime of Apartheid[330], and the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment[331]. It can also be found in Article 105 of UNCLOS.

4.2.3 Jurisdiction regarding piracy

Given the nature of the crime, piracy *jure gentium* as defined in Article 101 of UNCLOS was the first crime in history that was recognised as being against international law and was reacted

[322] Department of State 'Report on Extraterritorial Crime and the Cutting Case' in Foreign Relations Law of the United States (1887) 751-867 (The Cutting Case Report).
[323] Klinghoffer v. SNC Archille Lauro, 759 F. Supp. 112 (S.D.N.Y. 1992) 23 July 1992.
[324] 2051 UNTS 363, (1995) 34 ILM 482. Adopted: 9.12.1994; EIF: 15.01.1999.
[325] Max Planck Encyclopaedias of International Law *'International Criminal Jurisdiction, Protective Principle'* (July 2007) 1.
[326] Ibid.
[327] X Philippe *'The principles of universal jurisdiction and complementarity'* International Review of the Red Cross 88, 862 (June 2006) 378.
[328] Ibid.
[329] 75 UNTS 85 (1950) Adopted: 12.08.1949, EIF: 21.10.1950.
[330] 1015 UNTS 243 (1974). EIF: 18.07.1976.
[331] 1465 UNTS 85 (1984). Adopted: 10 December 1984, EIF: 26.06.1987.

to with universal jurisdiction.[332] Article 105 of UNCLOS codifies universal jurisdiction and states:

> 'On the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. The courts of the State which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property, subject to the rights of third parties acting in good faith.'

This means that no jurisdictional link such as territoriality or nationality is needed between the state exercising jurisdiction and the pirate. Every state has jurisdiction over the person and the offence to legitimate its prosecution.[333] In addition to UNCLOS, the SUA Convention also covers jurisdiction on piracy.[334] Article 6 of the SUA asks the states to establish its jurisdiction if the offence is committed on board a ship flying its flag, if the offence is committed in the territory (or territorial waters) of the state, and if the offence is committed by a national of the state. Unlike UNCLOS, the SUA Convention demands a legal link such as nationality or territoriality to prosecute pirates. In conclusion, all five principles apply to piracy, universal jurisdiction being the only one with no specific link required.

4.2.4 Jurisdiction regarding cybercrimes

For cybercrimes, the principle of territoriality and the flag principle can be found in the European Convention on Cybercrime. Article 22 of the Convention on Cybercrime states:

> '1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
>
> a. on its territory; or
>
> b. on board a ship flying the flag of that Party; or
>
> c. on board an aircraft registered under the laws of that Party; (…)'.

---

[332] M. Cherif Bassiouni *'Universal jurisdiction for international crimes: historical perspectives and contemporary practice'* Virginia Journal of International Law, 42 (2001), 108-112.
[333] United Nations Conference on Trade and Development *'Maritime Piracy - Part II - An Overview of the International Legal Framework and of ultilateral Cooperation to Combat Piracy'* Studies in Transport Law and Policy 2014 No. 2 (2014) 18.
[334] Ibid.

The principle of territoriality is followed by the principle of nationality. Article 22 of the Convention on Cybercrime continues:

> 'd. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. (...).'

Besides the link to the nationality of the perpetrator, the principle of nationality can also be linked to the victim's nationality. The one principle that does not apply to cybercrimes is universal jurisdiction. This principle only applies to the above-mentioned crimes all of them including physical acts. However, given the global nature of the crime, a cybercrime treaty that establishes universal jurisdiction over cybercrimes could help deter and resolve those crimes. In addition to drafting an international cybercrime treaty, it could also be helpful in creating an agency comparable to the International Maritime Organisation. This cybercrime specific institution could ensure the security and safety of the internet dealing especially with international cybercrimes.

4.2.5 Jurisdiction regarding cyber piracy

At present, the term 'cyber piracy' is not used for cyber-attacks on vessels nor does any jurisprudence exist that states which international principle of jurisdiction would apply for such an act. Also, there is no international convention that only focuses on cyber-attacks on ships. Therefore, it cannot be said without a doubt how a court would decide. However, in most statutes and regulations cyber piracy is understood to be a normal cybercrime. Therefore, it would most likely apply to the same international principles of jurisdiction as a cyber-attack. This means that the principle of territoriality and the principle of nationality would be especially applicable. The principle of universal jurisdiction would not apply. As shown in chapter three of the thesis, the act of cyber piracy does not fall under the scope of UNCLOS. Therefore, the principle of universal jurisdiction as described in Article 105 of UNCLOS does also not apply to it. Even though the SUA Convention partly covers cyber piracy, section 6 of the SUA Convention is also only of limited use in this context, as it does not state universal jurisdiction. All of the above-mentioned leads to the question of whether or not the principles of jurisdiction that apply to cybercrimes are sufficient in the case of cyber piracy or if cyber piracy should be treated differently because of its similarities to piracy. The universal principle of jurisdiction

over piracy has a unique position in international law as it is an exception to all sovereignty-based principles. It allows a state to take legal action with absolutely no link to its territory or nationality.[335] Traditionally, this unique jurisdiction is a consequence of the fact that piracy is committed on the high seas, outside of anyone's jurisdiction. Historically, it can also be understood as a shortcut that allows a state to prosecute crimes involving nationals abroad as international law did not recognise a state's jurisdiction over offences that were committed against its nationals abroad. But even today, the universal principle plays a major role in international law. As the recent African Union and European Union joint report on universal jurisdiction stresses: 'Temporal, geographical, personal and subject-matter limitations on the jurisdiction of international criminal courts and tribunals mean that universal jurisdiction remains a vital element in the fight against impunity'.[336] For a very long time, piracy was considered to be the only crime with a global impact.[337] Today, cybercrimes, in general, pose legal challenges similar to piracy. The internet and the high seas are both international spaces that are shared globally. The consequences caused by criminal activity have similar effects. As shown in chapter 3 of the thesis, cyber piracy includes both of these elements. Because of its great international consequences resulting from these two elements and because of its unique resemblance to piracy with regard to its motivations and its outcome, it is submitted that universal jurisdiction should also apply for acts of cyber piracy. Chapter 6 of this thesis will discuss how to include this principle into the framework of cyber piracy.

4.3 International Court in the Context of Cyber Piracy

4.3.1 Introduction

In addition to adding the international jurisdiction on acts of cyber piracy to the legal framework, it is also necessary to take a closer look at where the crime should be prosecuted. In general, national courts have jurisdiction. For a long time, even serious international crimes such as war crimes and crimes against humanity could not be tried at an international tribunal.[338] However, this changed especially after the foundation of the United Nations in the year 1945 as a response to World War II.[339] The principal judicial institution of the United Nations is the

[335] Philippe (note 327 above).
[336] Council of the European Union *'The AU-EU Expert Report on the Principle of Univeral Jurisdction'* (16 April 2009) section 28.
[337] M Scharf *'The ICC's Jurisdiction over the Nationals of Non-Party States: A Critique of the U.S. Position'* (2001).
[338] Ibid.
[339] United Nations General Assembly *'Sixty-eighth session Agenda item 85 The rule of law at the national and international levels'* (19 August 2014) 6.

International Court of Justice (ICJ) based in Den Haag in the Netherlands.[340] The Court has contentious as well as advisory jurisdiction.[341] Following international law, it decides legal issues that are submitted to it by contracting states.[342] Such an international legal dispute can be defined as a disagreement on a question of law or fact, a conflict, or a clash of legal views or interests.[343] On the advisory side, the court recommends opinions on legal questions on request of the United Nation's organs or specialised organisations.[344]

Another body of international jurisdiction is the International Criminal Court (ICC) also based in the city of Den Haag.[345] Based on the legal foundation of the 1998 Rome Statute of International Criminal Court[346], the ICC tries individuals (not crimes committed by a state or organisation) for crimes such as war crimes, genocide, and crimes against humanity since 2003.[347] However, it is not the ICC's intention to replace national criminal courts and it only comes into effect if the national judicial system and its authorities are unwilling or unable to prosecute the crime.

The maritime sector also provides an example of international jurisdiction involving the United Nations: The International Tribunal for the Law of the Sea (ITLOS) based in Hamburg in Germany.[348] It was established in 1982 by the United Nations based on the Law of the Sea. Its relevant provision is Article 287 of UNCLOS.[349] The court has jurisdiction, subject to the provisions in Article 297 of UNCLOS and the declaration made under Article 298 of UNCLOS, for any jurisdiction relating to the interpretation or application of the Convention. Several multilateral conventions have already been concluded which confer jurisdiction on the court such as the 1995 Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks[350] in Article 30 and the 2007 Nairobi International Convention on the disposal of wrecks[351] in Article 15. Under the Law of the Sea, the court exercises compulsory jurisdiction in two categories of proceedings:

[340] Ibid 6.
[341] Ibid 6.
[342] Ibid 7.
[343] Ibid 8.
[344] Ibid 8.
[345] Compare Article 2 Rome Statute of the International Criminal Court.
[346] 2187 UNTS 3. Adopted: 17.07.1998; EIF: 01.07.2002.
[347] Compare Article 5 Rome Statute of the International Criminal Court.
[348] Compare Article 1 Annex VI. Statute of the International Tribunal for the Law of the Sea.
[349] B Turner *'The Statesman's Yearbook'* (2010) 49, 50.
[350] 2167 UNTS 3. Adopted: 11.08.1995; EIF: 11.12.2001.
[351] 55565 UNTS. Adopted: 18.05.2007; EIF; 14.04.2015.

Procedures relating to the immediate release of ships and crews and procedures for ordering provisional measures pending the formation of an arbitral tribunal.[352]

4.3.2 International Court for Piracy

Concerning piracy, none of the above-mentioned courts have jurisdiction.[353] Neither of the international courts in Den Haag nor the International Tribunal for the Law of the Sea, the latter being less of a criminal but more of a civil and administrative court, are competent in such matters.[354] The lack of an international court that tries pirates would not be problematic if it could be argued that national courts are sufficient to convict pirates.[355] However, this is rejected for various reasons.[356] First of all, most of the countries that are greatly affected by piracy, for example, in the Gulf of Guinea, lack the legal infrastructure meaning efficient court capacity and personnel to try pirates.[357] By trying to keep up with international standards, national cases could be declassified which could lead to a two-tier judicial system meaning that the national cases would not be treated with priority anymore. Even if the national legal infrastructure is efficient enough to take on piracy trials the outcome of each trial would differ enormously as the national legal frameworks differ in legal requirements and consequence. Another problem is that a lot of national courts are already under immense pressure to keep up with the national cases. Most countries, for example, Somalia, are already struggling with the enormous amount of legal proceedings because of their instability[358]

As a result of insufficient national piracy trials, various approaches are discussed. One idea is to establish a court that only deals with piracy under an international framework.[359] This court could be established as an international tribunal but also as a regional tribunal. Having jurisdiction within a specific geographical region such as high-risk areas including more than one country.[360] Alternatively, the establishment of a division that only deals with piracy at the International Tribunal for the Law of the Sea could help to exclusively try pirates.[361] Another approach

[352] Internationaler Seegerichtshof *'Der internationale Seegerichtshof'* (2016) 9.
[353] M O'Brien *'Where Security Meets Justice: Prosecuting Maritime Piracy in the International Criminal Court'* Asian Journal of International Law, Volume 4, Issue 1 (2014) 81-81.
[354] Ibid.
[355] Ibid 85-87.
[356] Ibid.
[357] A Osinowo *'Combating Piracy in the Gulf of Guinea'* (15 February 2015); W Burke-White *'Regionalisation of International Criminal Lan Enforcement: A Preliminary Exploration'* Texas International Law Journal, Volume 38 (2003) 734.
[358] O'Brien (note 353 above) 86.
[359] In Germany, for example, the former Minister of Defence Christian Schmidt requested to establish a United Nation Court that only deals with piracy.
[360] K Anele *'The Viability of Establishing an International Tribunal for maritime piracy'* 12.
[361] O'Brien (note 353 above).

is the introduction of a criminal jurisdictional court that assigns the jurisdiction to prosecute states in a binding manner. However, all the options, and especially the latter, may not be very practical regarding the immense logistics and funding required. Also, from a political perspective, states may not be interested to promote and achieve consensus on this topic. The establishment of regional courts could help countries in high-risk areas to reduce costs by dividing them between the contracting parties, to structure court proceedings and personnel, and to benefit from the collaborative learning process. On an international level, however, it would be beneficial to either establish a tribunal that only deals with piracy or to establish a special piracy chamber at the International Tribunal for the Law of Sea. [362] Both ideas have in common that the court would be maritime specific.

4.4.3 International Court for Cybercrime

Just like in the piracy cases, none of the above-mentioned international courts have jurisdiction for cybercrimes. The difference between piracy and cybercrime cases is, that the high-risk areas differ from one another. The risk of cyber-attacks increases with technical progress which makes highly developed nations a more vulnerable target. These countries are also more likely to have a sufficient jurisdictional system that makes it easier for them to try cybercrimes sufficiently. But the lack of jurisdictional development is not the only reason to establish an international court. The main reason to set up an international tribunal is the global effects that result from a crime. As discussed above, cybercrimes are the paradigm of cross-border offences. To respond to such a global crime in a sufficient and uniform manner it is necessary to establish a unified jurisdictional body that can help to prevent bypassing penalties. Cybercrimes could be prosecuted either at a specific chamber at the International Criminal Court of Justice or a court particularly established for cybercrimes.

4.3.4 International Court for Cyber Piracy

It is no surprise that there does not exit an international court for cyber piracy as there is neither an international court that tries piracy nor an international court for cybercrimes. However, because cyber piracy includes elements of piracy and cybercrimes, there is no doubt that the act of cyber piracy should also be tried at an international court. It it questionable if a maritime-related or a cybercrime-related court should have jurisdiction regarding cyber piracy. Chapter 6 will present some ideas on the topic.

[362] Ibid.

4.4 Conclusion

In the first part of this chapter under 4.1 it was found that throughout all the regulations, guidelines, and standards, the BIMCO Guidelines on Cyber Security Onboard Ships cover the risk of cyber piracy on unmanned and autonomous ships comprehensively. Unfortunately, the implementation of the Guidelines is entirely optional to the shipping industry. They also do not specifically cover unmanned and autonomous operations. The same applies to the IMO Guidelines on Maritime Cyber Risk Management which are also too basic to cover all the risks of cyber piracy. As the Guidelines are published by the IMO they at least raise awareness of cyber security incidents within the shipping industry. The Information Security Management Standards may be effective but their implementation is not compulsory and comes with a costly fee. Therefore, they are also not the right way to fight the risks of cyber piracy. The only regulations regarding cyber incidents that are compulsory to the shipping industry are the International Ship and Port Facility Security Code and the International Safety Management Code. Both codes, unfortunately, do not cover the risk of cyber piracy nor unmanned and autonomous operations. However, the codes would be the appropriate instruments to address the risks and threats identified. The Ships Security Plan and the Safety Management Manual may be the right document to include sufficient requirements to prevent and cyber piracy incidents for unmanned and autonomous operations. Chapter 6 of this thesis will present some ideas on how cyber piracy security could be incorporated.

In the second part of the chapter under 4.2, it was discovered that at present, the universal principle does not apply to acts of cyber piracy. This is because the act is mostly understood as a cybercrime and does not fall under the scope of UNCLOS. Chapter 4.3 of the thesis showed that cyber piracy is not yet be tried at an international court.

5 DISCUSSION FROM A DOMESTIC LAW PERSPECTIVE

5.1 Introduction

Besides a discussion from an international law perspective, it is also interesting to elaborate on the subject on a national level. This becomes especially interesting when comparing two different countries. Germany and South Africa are both known for international maritime trading. The city of Hamburg for example has the third biggest trading seaport in Europe. The Port of Durban is the largest shipping terminal in sub-Saharan Africa. Therefore, both countries have great potential to host unmanned and autonomous ships one day.

5.2 Germany

5.2.1 Preventive regulations

At present, German maritime-related legal framework is a hybrid of different pieces of law and its legislation can be found in many different statutes and provisions.[363] The legal area of maritime security law also has several legal foundations.[364] In the following, the most relevant statutes and regulations are presented to find out if they cover the risks of cyber piracy on unmanned and autonomous ships.

The first Act that comes to mind is the Schiffsicherheitsgesetz (SchSG). This Act determines the measures that have to be taken into consideration to comply with international regulations on ship safety and environmental protection at sea.[365] The SchSG applies according to section 1 of the SchSG to all sea-going vessels as well as to inland waterway transport vessels that are flying under the German flag. But even though section 1 of the SchSG does not exclude unmanned and autonomous ships the SchSG still refers to people working onboard the ship. Section 8 of the SchSG, for example, refers to the onboard crew and to sufficient manning of the ship which specifically excludes unmanned operations. Furthermore, the SchSG only refers to basic cyber-related measures such as ensuring a safe operation in general.[366] According to section 3 of the SchSG, any person who uses a ship at sea shall ensure that it is operated safely and, in particular, that the ship and its accessories are maintained in a way that ensures general safety and protects third parties from risks. In addition to that, section 7 of the SchSG states that the owner of the ship is responsible to fulfil the safety requirements of the ship's nautical

[363] H Schaps *'Das deutsche Seerecht, Kommentar und Materialsammlung'* (2019) 3-5.
[364] Ibid.
[365] Universität Hamburg *'Teil 3: Das Schifffahrtpolizeirecht'* (13.06.2014) 11.
[366] Ibid.

and technical equipment and systems, including radio equipment, accessories, and installations. This also includes the maintenance of onboard ship systems used to control the vessel from the land. But even though keeping those systems up to date and well maintained can lower the risks to become a victim of cyber piracy, the main focus of the SchSG does not lay on cyber risk security but physical safety. Cyber-related risks including cyber piracy are not discussed. Overall, the SchSG's scope does not include measures for cyber piracy on unmanned and autonomous vessels.

The second German regulation that has to be taken into consideration is the Schiffssicherheitsverordnung (SchSV). This Ordinance was passed based on the SchSG to further elaborate on some of the safety requirements.[367] The SchSV was passed to cover as many threats as possible and should therefore also include cybercrime-related issues.[368] It contains national implementations of the international regulations under SOLAS.[369] It deals with the safety precautions of ships, equipment, and crew. As the SchSV refers in section 1 to the SchSG's scope, the SchSV itself also only partly applies to unmanned and autonomous ships. Even though the SchSV does not set out any specific regulations regarding cyber piracy or cyber-security section 5 of the SchSV refers to the international safety standards of a ship. According to section 5(1) of the SchSV, all international regulations that are listed in sections A and C of the Annex must be applied as well. The Annex refers, inter alia, to the regulations under SOLAS Chapter II-1, II-2, and III. These chapters, however, do also not focus on cyber risks and do not apply to unmanned and autonomous operations. Overall, the SchSV does not cover cyber piracy attacks.

Another important ordinance is the Verordnung über die Sicherheit der Seefahrt der Bundesrepublik Deutschland (SeeFSichV). This Ordinance applies, according to section 1, to German maritime shipping and all German seagoing vessels. In the interest of maritime safety, it regulates the obligation to rescue at sea, the protocol in case of collision, and the reporting of significant events and wrecks.[370] Section 8 of the SeeFSichV states that the master or any other person in charge who is responsible for safety shall apply the regulations applicable to ship guidance systems adopted by the IMO which are mandatory for the specific type of the ship or its cargo. This does not apply if a particular system of navigation cannot be used for compelling reasons. Such reasons must be entered in the ship's logbook. The operator of the ship or any

[367] Compare section 1(1) of the SchSV.
[368] Universität Hamburg (note 365 above) 12.
[369] Compare section 5 of the SchSV.
[370] Compare, for example, sections 2 and 6 of the SeeFSichV.

other person in charge must also report all information to the competent authorities that are related to such systems.[371] The Federal Ministry of Transport and Digital Infrastructure publishes the information on the navigational systems in the maritime news (official publication for shipping of the Federal Office of Maritime Navigation and Hydrography). The term 'any other person in charge' also includes remote-controllers and supervisors operating an autonomous and unmanned vessel from the SCC. The wording was chosen to explicitly include these people in charge as the section itself refers to the IMO Guidelines on Maritime Cyber Risk Management. The IMO Guidelines are meant to raise awareness of cyber risks and present recommendations on how to react to a cyber-attack. Section 8 of the Ordinance turns recommended guidelines into mandatory regulations under German law. In conclusion, both unmanned and autonomous operations, as well as cyber-related risks and therefore cyber piracy, are considered under the scope of the SeeFSichV. However, even though section 8 of the SeeFSichV makes the IMO Guidelines mandatory, it cannot cover the risks of cyber piracy. As stated in chapter 4 of this thesis, the IMO Guidelines also do not cover the risk. They only mark one step in the right direction as they are predominantly useful to raise awareness and are of good use to outline the many vulnerable systems within maritime operations. Overall, the SeeFSichV applies to unmanned and autonomous operations and also addresses cyber-related risks. However, to respond to the risks of cyber piracy it would need to go into more detail.

The last important maritime-security-related act is the German Seesicherheits-Untersuchungs-Gesetz (SUG) which implements international investigation regulations and uniforms standards of reaction to maritime accidents.[372] Even though it also applies to unmanned and autonomous ships its scope only covers accidents at sea.[373] Cyber threats of any sort are not considered.

Besides the maritime-related regulations, Germany lately started to focus on regulations to prevent cybercrime in the Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BSIG) and the Verordnung zur Bestimmung kritischer Infrastrukturen (BSI-KritisV). Section 8 of the BSI-KritisV regulates the sector of transportation and commerce and includes the sectors aviation, maritime shipping, inland waterways, railroads, road transport, and logistic. For each of these sectors, specialists are working on regulating standards. So far, only the road transport standard has been published. For railroads and aviation, the regulations are in the

[371] Compare section 8 of the SeeFSichV.
[372] Compare section 1(1) of the SUG.
[373] C Gerlach *'Die Seesicherheitsuntersuchung - Die Untersuchung von Seeunfällen und die Einziehung von Berechtigungen nach dem Seesicherheitsuntersuchungsgesetz'* (2005) 12.

process of getting approved by the BSI. An official standard for maritime and inland waterway shipping does not yet exist. Letter c of Annex 7 Part 1 BSI-KritisV refers to maritime and inland waterway navigation and reads as follows:

'c) in the maritime and inland waterway navigation

aa) Facilities or systems used for the operation of federal waterways [means:] A facility or system used for the safe operation of a waterway according to section 1(4) number 1[374] Bundeswasserstraßengesetz (WaStrG - Federal Waterway Act) in the current version.

bb) Traffic management and control systems for maritime and inland waterway navigation [means:] District and traffic headquarters of the Federal waterways and shipping administration.

cc) Control centre of operators and transport companies in the maritime shipping sector [means:] A facility or system for the operational control of seagoing vessels according to a fixed timetable.

dd) Facilities or systems for the disposition of inland waterway navigation (freight transport only). An IT system for the disposition of the shipping space of the inland waterway navigation fleet.'[375]

According to the wording, onboard systems do not fall under the regulations. The focus lays on port facilities and other onshore located establishments. The draft bill and legal explanation by the German Federal Ministry of the Interior set out the objectives of the Ordinance and explain what was meant to be included.[376] The regulations under letter aa) include the facilities of all waterways; the regulations under letter bb) and cc) include facilities that are used to navigate traffic such as light and traffic signal systems, facilities for the control of variable traffic signs, as well as radar stations for both inland waterways and maritime operations; the regulations under letter dd) include control centres for communication facilities, traffic control centres, transport control centres including fleet telematics, applications for traffic management, vehicle

[374] Bundeswasserstraßengesetz BGBl. I S. 962 from 23 May 2007; no official English translation available; Section 1(4) of the WaStrG reads as follow 'Federal waterways also include: 1. The federally owned shipping facilities, especially locks, ship lifts, weirs, shelters, moorings and construction ports as well as federally owned dams, reservoirs, and other supply and relief facilities, 2. The federal waterfront plots, building yards, and workshops used for maintenance, 3. Federal facilities or water parts intended to maintain or restore continuity in dams built or operated by the federal waterways and shipping administration.'

[375] Unofficial translation from German into English.

[376] Bundesministerium des Inneren *'Referentenentwurf - Erste Verordnung zur Änderung der BSI-Kritisverordnung'* (23 February 2017).

management, and transport management, as well as facilities and systems for data exchange; the regulations under the letter ee) include control and management systems of shipping companies.[377] This means that the SCC on land but not the vessel at sea is included.

In conclusion, some of the German maritime-related regulations include unmanned and autonomous ships but none of them provide any prevention of cyber piracy. The only regulation that refers to onboard navigational systems is the Ordinance on the Safety of Maritime Navigation of the Federal Republic of Germany which refers to the IMO Guidelines on Maritime Cyber Risk Management. Overall, German maritime-related law will need to improve the regulations to raise awareness on the topic and to cover the risks of cyber piracy on unmanned and autonomous vessels. German cyber-related law shows great potential but excludes the navigational systems of the vessel itself. The regulations would have to be modified slightly to include unmanned and autonomous operations. The biggest issue, however, is that the IT security standards for the shipping sector are not yet drafted.

5.2.2 The criminal offence and its sentence

As shown in chapter 3 of the thesis, the act of cyber piracy could be prosecuted under both, section 316c(1) of the StGB and section 303b of the StGB. The expectable sentence of German criminal offences is regulated in the respective section itself. Section 316c of the StGB reads as follows:

'(1) Whosever
1. Uses force or attacks a person's decision-making freedom or engages in other practices in order to gain control over or influences the navigation of (a) An aircraft (…) (b) A ship deployed in civil maritime traffic or
2. uses firearms (…) Incurs a penalty of imprisonment for a term of at least five years. (…)
(2) In less serious cases, the penalty is imprisonment for a term of between one year and 10 years.
(3) If, by committing the offence, the offender at least recklessly causes another person's death, the penalty is imprisonment for life or imprisonment for a term of at least 10 years. (4) (…)'

Section 303b of the StGB reads as follows:

[377] Ibid 63.

‘(1) Whosoever interferes with data processing operations which are of substantial importance to another by

1. committing an offence under section 303a(1); or
2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier shall be liable to imprisonment not exceeding three years or a fine.

(2) If the data processing operation is of sustainable importance for another’s business, enterprise or an authority, the penalty is imprisonment for a term not exceeding five years or a fine.
(3) The attempt is punishable.
(4) In especially serious cases under subsection (2), the penalty is imprisonment for a term of between six months and ten years. An especially serious case typically occurs where the offender

1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage or
3. by committing the offence jeopardise the population’s supply with vital goods or services or the security of the Federal Republic of Germany.

(5) Section 202c applies accordingly to acts preparatory to an offence under subsection (1).’

To find out which criminal charges would be brought by a prosecutor, it is necessary to first discover how the two criminal offences are connected. German law uses the word ‘Konkurenz’[378], meaning competition of the law. Competition means the investigation of the criminal regulations for which the accused can be charged and if necessary convicted, as well as the determination of the criminal regulations that are used in the sentencing.[379] The different principles of legal competition are regulated in section 52 of the StGB and the following sections. German law differentiates between echte (real) and unechte (false) competition.[380] The real competition can be found in sections 52 and 53 of the StGB and deals with the question of how many acts are committed by the offender. The law distinguishes between the principle of Tateinheit (unity of offences)[381] and Tatmehrheit (the principle of joinder of offences)[382]. The

[378] D Kienapfel *‘Strafrecht, Allgemeiner Teil: Mit Einführung in programmierter Form‘ (*2015) 582.
[379] Ibid.
[380] Ibid.
[381] B Heinrich *‘Strafrecht – Allgemeiner Teil’* (2019) 619.
[382] Ibid 620.

principle of unity of offences, also called Idealkonkurrenz (ideal competition),[383] applies according to section 52 of the StGB when the same act violates more than one criminal statute or the same criminal statute more than once.[384] This means that several violations of criminal law are carried out by the same act that can stand side by side without displacing each.[385] In this case, only one penalty is imposed which is according to the statute the one that provides the most severe penalty.[386] The principle of joinder of offences applies according to section 53 of the StGB when a person has committed several offences. In this case, an aggregate sentence is imposed according to section 54 and 55 of the StGB, if all offences are to be adjudicated at the same time, and when the person has incurred more than one sentence of imprisonment or more than one fine.[387]

The false competition describes the relationship between statutes.[388] German criminal law distinguishes mainly between three different principles of false competition. The first one is called the principle of specialty and follows the principle *lex speciales derogate legi generali*.[389] If one provision contains all the elements of another and also describes another aspect of the criminal conduct, it supersedes the other provision.[390] The second one is the principle of subsidiarity.[391] This principle refers to the suppression of a more general regulation by a more specific one.[392] The last one is the principle of consumption.[393] In this case, the unlawful content of one statute is consumed by another. In conclusion, the principles are the key to the sentence of the court and are therefore of high importance.[394]

The act of cyber piracy violates more than one criminal statute. Section 316c of the StGB and section 303b of the StGB are of equal rank and none of the principles of false competition apply. A cyber pirate attack would, therefore, be prosecuted as an attack on maritime traffic according to section 316c of the StGB in conjunction with computer sabotage according to section 303b of the StGB. Because the principle of unity applies, only the most severe is imposed. In this

[383] V Erb *'Überlegungen zu einer Neuordnung der Konkurrenzen'* Zeitschrift für die gesamte Strafwissenschaft, Volume 117, Issue 2 (2005), 38.
[384] Compare sections 52(1) and (2) of the StGB.
[385] Geppert *'Grundzüge der Konkurrenzlehre'* Jura 2000, 598 ff., 651 ff.;
[386] Ibid.
[387] Compare section 53(2) of the StGB and sections 54 and 55 of the StGB.
[388] Kienapfel (note 378 above).
[389] Kienapfel (note 378 above) 583.
[390] G Seher *'Zur strafrechtlichen Konkurrenzlehre - Dogmatische Strukturen und Grundfälle'* Juristische Schulung (2004) 392 ff., 482 ff.
[391] Ibid.
[392] Ibid.
[393] Ibid.
[394] Ibid.

case, section 316(c)1 of the StGB states the stricter penalty with imprisonment of not less than five years.[395] Whenever the law states that a sentence should not be *less* than a certain number of years it means that the sentence could range up to imprisonment for life (15 years). A cyber pirate would therefore face a sentence between five and 15 years. The court's decision is guided by aspects such as the seriousness of the crime and the motive of it, the criminal record of the offender and his personality, and his living conditions.

5.2.3 The national implementation of international jurisdiction regarding cyber piracy

As found in chapter 4 of this thesis, according to international law, universal jurisdiction applies to all acts of piracy and therefore enables the prosecution of the act by all states without any other legal link such as the place where the crime is committed or the nationality of the offender or victim. As Germany and South Africa are both parties to UNCLOS universal jurisdiction also applies on their national level. For cybercrimes however, the principle of universal jurisdiction does not apply. For any cyber-related offence, a legal link is necessary for a country to have jurisdiction. Because internationally, cyber piracy is mostly understood as a cybercrime and not so much as one of piracy, the universal jurisdiction does also not apply for acts committed by cyber pirates. Keeping the above in mind, this section takes a closer look at the national implementation of the international principles of jurisdiction into German and South African domestic law to find out how the issue is treated on a national level.

The principles of jurisdiction in German criminal law can be found in sections 3 to 7 and section 9 of the StGB. These sections only regulate the question if an act can be prosecuted under German law, but do not deny the possibility that the same act can also be subject to foreign jurisdiction according to their principles of jurisdiction.[396] The basic principle of German jurisdiction is the worldwide prevailing principle of territoriality which connects jurisdiction to the place where the crime was committed. Sections 3 and 9 of the StGB are expressions of this principle. According to section 3 of the StGB, German criminal law applies to offences

[395] The section reads as follows: '(1) Whosoever 1. uses force or attacks the freedom of decision of a person or engages in the other conduct in order to gain control of, or influence the navigation of(a) (…) (b) a ship employed in civil maritime traffic; or 2. shall be liable to imprisonment of not less than five years. (…) (2) In less serious cases, the penalty is imprisonment for a term of between one year and 10 years. (3) If, by committing the offence, the offender at least recklessly causes another person's death, the penalty is imprisonment for life or imprisonment for a term of at least 10 years.'

[396] H Kühne *'Strafprozessrecht - Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts'* (2015) 21.

committed on German territory. Resulting from section 9 of the StGB is the so-called principle of ubiquity.[397] This section reads as follows:

> '(1) An offence is deemed to have been committed at every place where the offender acted or, in the case of an omission, was required to act or in which the result, if it is an element of the offence, occurs or was to have occurred as envisaged by the offender.
> (2) Acts of participation are not only committed at the place where the offence was committed, but also at every place where the participant acted or, in the case of an omission, was required to act or where, as envisaged by the participant, the offence was to have been committed. If the participant to an offence committed abroad acted within the territory of the Federal Republic of Germany, German criminal law applies to the participation even if the act is not a criminal offence according to the law of the place of its commission.'

Furthermore, according to section 4 of the StGB, German criminal law applies when the offence is committed on a ship or an aircraft that is entitled to fly the federal flag or to carry the national insignia of the Federal Republic of Germany (flag principle). Section 5 of the StGB deals with offences committed abroad with specific domestic connections and states that regardless of which law is applicable at the place where the offence was committed, German criminal law also applies to some offences committed abroad. This includes, for example, crimes such as offences against life,[398] physical integrity,[399] and personal liberty.[400] Section 6 of the StGB covers offences committed abroad against internationally protected legal interests and is, therefore, an expression of the universal jurisdiction. According to this section, German criminal law also applies regardless of which law is applicable at the place where a crime was committed for several offences committed abroad. In general, Germany applies universal jurisdiction over genocide, crimes against humanity, and war crimes.[401] Section 6 number 3 of the StGB also includes 'attacks on air and maritime traffic (section 316c)'. Germany also claims universal jurisdiction for one cybercrime: child pornography according to section 6 number 6 of the StGB.[402] The principle of passive nationality which allows states, in limited cases, to claim

[397] Ibid.
[398] Compare section 5 number 9 of the StGB.
[399] Compare section 5 number 9a of the StGB.
[400] Compare section 5 number 6 of the StGB.
[401] Compare section 1 of the Völkerstrafgesetzbuch (VStGB - German International Criminal Code) BGBl. I S. 3150 from 26 June 2002.
[402] Another European country that prosecutes child pornography applying universal jurisdiction is Belgium.

jurisdiction to try a foreign national for offences committed abroad that affects its citizens is codified in section 7 of the StGB. Section 7 of the StGB reads as follows:

> '(1) German criminal law shall apply to offences committed abroad against a German, if the act is a criminal offence at the locality of its commission or if that locality is not subject to any criminal jurisdiction.'

For piracy, the implementation of the international principles of jurisdiction leads to German prosecution whenever the offender or the victim is a German national or the offence was committed on German territory.[403] Because German law also codifies the universality principle, German prosecution on piracy is also possible with no legal link. For cybercrimes, the German implementation of international jurisdiction leads to the following: According to section 9 of the StGB, the place of the commission of the offence can be the place where the offence was committed. Usually, even for crimes committed online the determination of the place of action is not problematic. If the offender himself is located in Germany and uses another person as a tool to commit the crime abroad for him, the place where the crime was committed is both Germany and the location abroad.[404] Besides the place where the offence was committed, section 9 of the StGB also speaks of the place where the offence's result occurs. If, for example, computer viruses are sent from abroad that lead to data manipulation in Germany according to section 303a of the StGB, the place of the result of the action is Germany.[405] The universal principle does not apply to cybercrimes with the exception of online child pornography according to section 6(6) of the StGB. For acts of cyber piracy, section 9 of the StGB leads to the same result. The place of action is the location from where the cyber pirate launches his or her attack. The place of the result can be any vessel the cyber piracy attack was launched against which can be understood as part of the German territory according to the flag principle. However, because cyber piracy and piracy can both be prosecuted as attacks on maritime traffic according to section 316c of the StGB the universal principle also applies to cyber piracy under German law. Section 6 number 3 of the StGB refers to all crimes that fall under section 316c StGB and does not speak of piracy only.

[403] The offence is committed on German territory when the ship is located in German territorial waters. Unlike UNCLOS the German national law according to section 316c of the StGB is not limited to offences committed on the high sea.
[404] Bundesgerichtshof Zeitschrift für Wirtschafts- und Steuerstrafrecht (1991) 135; Oberlandesgericht Schleswig Zeitschrift für Wirtschafts- und Steuerstrafrecht (1998) 31.
[405] K Malek and A Popp *'Strafsachen im Internet'* (2015) 17.

5.2.4 Law enforcement

German law does not state clearly if the national power to combat piracy under Article 105 of UNCLOS lays with the coastguard of the Federal Police or the National Defence Force (Bundeswehr) or with both. The problem is that in some cases the two authorities' areas of competence overlap which makes it difficult to make a clear and exclusive attribution to the police or the military.[406] Partly, the fight against piracy is primarily seen as a police task. According to section 6 sentence 1 Bundespolizeigesetzbuch (BPolG - Federal Police Act[407]) it is the Federal Police's objective without prejudice to the competence of other authorises or armed forces to take measures at sea outside the territorial waters of Germany if international law authorises it. The constitutional basis for the Bundeswehr's efforts to combat piracy is found in Article 24 section 2 of the Grundgesetz (GG – German Constitution[408]). Others believe that law enforcement against piracy is a National Defence Force's job.[409] Even though German legislation does not state clearly which authorities are in charge the Deutsche Bundestag states that both the Federal Police and the German Maritime Defence Force should jointly combat piracy.[410] For the combat of cybercrimes, the Bundeskriminalamt (BKA – Federal Criminal Police Office) in correspondence with the Landeskriminalämtern (LKA - Federal State Criminal Police Offices) are responsible in Germany.[411] The BKA is part of the Federal Ministry of the Interior and coordinates the crime in cooperation with the police forces of the German Federal States.[412] According to the KritisV, the BKA is in charge of setting up central defence facilities against cybercrime and internet attacks and is working closely together with organisations related to cybercrime (for example the Federal Association of IT Security TeleTrust and the German Competence Centre against Cyber Crime (G4C).[413] Since July 2016, the BKA has also been working on a new organisational structure that considers the challenges posed by international terrorism, organised crime and cybercrime, rapid technological development, and demographic

---

[406] J Waak '*Pirateriebekämpfung durch deutsche staatliche Stellen – Zu den Befugnissen der deutschen Marine, der deutschen Polizei und des Bundesnachrichtendienstes'* (2018) 229.
[407] Bundespolizeigesetz BGBl. I S. 2978, 2979 from 19 October 1994; no official English translation available.
[408] Grundgesetz für die Bundesrepublik Deutschland from 23 May 1949; official English translation available *https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html*, accessed on 21 January 2021.
[409] Waak (note 410 above) 70.
[410] Deutscher Bundestag Wissenschaftliche Dienste *'Zur Bekämpfung von Piraterie – Völkerrecht, Staatsrecht, Strafrecht'* (29 June 2009) 3.
[411] Compare section 1 and section 5 of the Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG – Act on the Federal Criminal Police Office and the Cooperation of the Federal Government and Federal State Governments in Criminal Police Matters) BGBl. I S. 1354 from 1 June 2017; no official English translation available.
[412] Compare sections 1 and 2 of the BKAG.
[413] Bundeskriminalamt *'Cybercrime'* available at *https://www.bka.de/DE/KarriereBeruf/ArbeitenBeimBKA/Einblicke/Cybercrime/cybercrime_node.html*, accessed on 21 January 2021.

change.[414] In doing so, the BKA relies on close cooperation with Interpol and Europol.[415] In order to strengthen the fight against cybercrime, the BKA has set up the Cybercrime (CC) department on April 1, 2020.[416] The new IT law also now regulates the competence of the many offences explicitly. Thus, the BKA now responsible for the law enforcement of the offences according to section 202a-202c of the StGB (preparation and execution of the spying and interception of electronic data), 263a of the StGB (computer fraud), and 303a of the StGB (data modification) of the StGB and all computer sabotage offences.[417] In conclusion, acts of piracy and cybercrimes are responded to by different law enforcement authorities.

5.2.5 The court's jurisdiction

The next question is, which court has the exclusive jurisdictional competence in a cyber piracy case. German criminal law distinguishes between regional, objective, and functional jurisdictional competence of a court.[418] Within the framework of the regional jurisdiction, it is clarified which court and where is responsible for the hearing of the case.[419] In general, this is according to section 7 of the Strafprozessordnung (StPO - German Code of Criminal Procedure[420]), the court in which district the offence was committed ('venue shall be deemed to be established in the court in whose district the offence was committed'[421]). In addition to this general regulation, section 10(1) of the StPO reads as follows 'If the offence was committed outside the territorial scope of this statute on a ship authorised to fly the federal flag, the competent court shall be the court whose district the ship's home port is located or the port within the territorial scope of this statute first reached by the ship after commission of the offence'. In addition to that, section 10a of the StPO states 'if nor venue is established for an offence committed at sea outside the territorial scope of this statute, the venue shall be Hamburg, the competent local court shall be Hamburg Local Court'. For the *Taipan Case,* for example, this meant that the trial was held in the city of Hamburg because it is the container ship's homeport.

The objective competence of German courts describes their scope of legal duties.[422] German criminal courts are differentiated into the local courts, the regional courts, the higher regional

[414] Ibid.
[415] Ibid.
[416] Compare section 3 of the BKAG.
[417] Compare section 5(5) of the BKAG.
[418] C Roxin, G Arzt, K Tiedermann *'Einfühung in das Strafrecht und Strafprozessrecht'* (2006) 114.
[419] Ibid.
[420] Strafprozessordnung BGBl. I S. 1074, 1319 from 7 April 1987; English translation available *https://www.gesetze-im-internet.de/englisch_stpo/index.html*, accessed on 21 January 2021.
[421] Compare section 7(1) of the StPO.
[422] Roxin (note 418 above).

courts, the Federal Supreme Court, and the Constitutional Court. Their objective competence at first instance is generally varying according to the expectable sentence of an offence. Following section 24 I of the Gerichtsverfassungsgesetz (GVG – German Courts Constitution Act[423]) the district court has jurisdiction if the expectation of punishment does not exceed four years' imprisonment or if the regional or the higher regional court is not entitled to the sentence in exceptional cases regardless of the extent of the sentence. The Regional Courts has competence in cases with an expectable sentence above four years' imprisonment or in exceptional cases.[424] The Higher Regional Court only has competence in the exceptional cases described in section 120 I, II of the GVG. The Federal Supreme Court has no legal competence in the first instance and deals with appeals only.[425] The Constitutional Court only decides on constitutional matters.[426] For the prosecution of cyber piracy, the expectable sentence depends on its outcome. According to section 316c(1) of the StGB criminals that fulfil any act described in section 316c of the StGB face a penalty of imprisonment for a term of at least five years. Therefore, in most cases, the regional courts would have objective competence.

The functional competence of a court describes the composition of the court meaning how many judges are attending the hearing.[427] For example, at the local courts, only one judge attends the hearing if the expectable sentence will be less than two years of imprisonment.[428] If the criminal offence is expected to be given a sentence above two years and under four years three judges attend the hearing (one judge and two lay judges).[429] For the regional courts, German law distinguishes between the criminal divisions and the criminal divisions with lay judges.[430] According to section 76(1) of the GVG, the criminal divisions are composed of three judges and two lay judges. Unlike the criminal division with lay judges, the criminal division can be reduced to a small criminal division that only includes one judge and two lay judges.[431] In general, the small criminal divisions have jurisdiction over all offences prosecuted at the regional courts[432] except for those serious criminal offences listed in section 74(2) which are all crimes that are resulting in death. A cyber piracy attack would in most cases not result in the loss of life

[423] Gerichtsverfassungsgesetz BGBl. I S. 1077 from 9 May 1975; English translation available at *https://www.gesetze-im-internet.de/englisch_gvg/index.html*, accessed on 21 January 2021.
[424] Compare section 74 of the GVG.
[425] Compare section 135 of the GVG.
[426] Compare Article 93(1) of the GG.
[427] Roxin (note 418 above).
[428] Compare section 25 of the GVG.
[429] Compare section 28 of the GVG.
[430] Compare section 76(1) of the GVG.
[431] Compare section 76 of the GVG.
[432] Compare section 74(1) of the GVG.

especially when the target operates unmanned. Therefore, the criminal division of the high court would have the jurisdiction. However, because a serious case of cyber piracy would hold various legal problems and would also lead to great media coverage the criminal division would most likely work with all five judges. In conclusion, the full criminal division of the regional court at the ship's homeport (most likely to be Hamburg) would have the jurisdiction in case of cyber piracy.

5.3 South Africa

5.3.1 Preventive regulations

In South Africa, the maritime security law is predominantly regulated in the Merchant Shipping (Maritime Security) Regulations (MSR)[433]. The purpose of the MSR according to section 2 of the MSR is 'to safeguard against unlawful interference with maritime transport'[434] by establishing 'a regulatory framework centred around the development of security plan for ships and maritime transport'[435] to meet the 'obligations under Chapter XI-2 of the Safety Convention and the ISPS Code'[436]. Section 4 of the MSR provides a list of ships and places that are excluded from the scope of the regulations. Excluded are, for example, warships and other vessels owned or operated by an organ of a state that is used for non-commercial activities.[437] Generally, unmanned and autonomous ships are not excluded as they are not listed under section 4 of the MSR. However, the regulations speak of the master in multiple sections, for example, in section 12 of the MSR, section 105 of the MSR, and section 111 of the MSR. Therefore, the MSR does not consider unmanned operations. However, when it comes to maritime security, South African law has got more potential than German domestic law. Section 5 of the MSR describes the term of unlawful interference with maritime transport and reads as follows:

'(1) Any of the following done without lawful authority is an unlawful interference with maritime transport:

(a) committing an act, or causing any interference or damage, that puts the safe operation of a port, or the safety of any person or property at the port, at risk;

(b) taking control of a ship by force, or threat of force, or any other form of intimidation;

(c) destroying a ship that is being used for maritime transport;

[433] Merchant Shipping (Maritime Security) Regulations of 2004.
[434] Compare section 2(1) of the MSR.
[435] Compare section 2(2) of the MSR.
[436] Compare section 2(4)(a) of the MSR.
[437] Compare section 4 of the MSR.

(d) causing damage to a ship that is being used for maritime transport that puts the safety of the ship, or any person or property on board or off the ship, at risk;
(e) doing on board a ship that is being used for maritime transport anything that puts the safety of the ship, or any person or property on board or off the ship, at risk;
(f) placing, or causing to be placed, on board a ship that is being used for maritime transport anything that puts the safety of the ship, or any person or property on board or off the ship, at risk;
(g) putting the safety of a ship at risk by interfering with, damaging or destroying navigational aids, communication systems or security systems;
(h) putting the safety of a ship at risk by communicating false information.'

To meet the obligations of the ISPS Code, the regulations describe the different security levels and security plans.[438] The security levels apply according to section 22 of the MSR to security regulated ports as well as to areas within such a port and to South African regulated ships, maritime industry participant as well as to their operators. The security plan must set out the security measures that have to be implemented by the participant for the security levels.[439] Section 62 of the MSR sets out the content of the ship's security plan. Besides setting out the security levels it must, for example, include a security assessment for the ship which according to section 62(2)(b) of the MSR must address the matters required by Annex 2. Part 1 of Annex 2 defines the ship's and port's security personnel in a similar manner as the ISPS Code. It speaks of port security officers and the ship security officer (SSO). According to section 6 of the Annex, the ship operator must 'designate the master, or a crew member, of the ship as security officer'. The duties of the SSO also include maintaining the ship security plan for the ship.[440] However, the Annex also mentions other shore-based personnel which is defined as 'in relation to a South African regulated ship, means persons (other than the master and crew) employed by the ship operator for the ship'[441]. Part 3 of the Annex outlines the maritime security plans. Section 61 of the Annex describes which matters must be addressed in the ship's security plan. This includes, for example, a range of physical security measures such as measures to prevent unauthorised carriage or possession of weapons on board the ship, the identification of on-board security zones, and the measurements to prevent unauthorised access to these zones or the ship

[438] Compare especially Part 2 *'Maritime Security Levels and Security Directions'* for example sections 16, 21, and 22 of the MSR.
[439] Compare section 44 of the MSR.
[440] Compare section 6(3)(a) Annex 2 of the MSR.
[441] Compare section 8 Annex 2 of the MSR and section 1 Annex 2 of the MSR.

in general and procedures for evacuation of the ship.[442] Other measurements speak of procedures to respond to security threats or breaches of security and of procedures for reporting maritime transport security incidents and other occurrences that threaten the security of the ship.[443] Section 69 of the Annex lists the onboard systems that have to be described in the security plan. This includes information external and internal communications systems, surveillance, identification, monitoring and reporting systems, tracking and positional systems, and security alert systems. In conclusion, South African maritime-related law shows a of potential in this matter. It is orientated on the ISPS Code and outlines different security levels and the security plan. Unfortunately, it focuses mainly on the physical security of the ship. Onboard systems that are used for autonomous operation are not taken into consideration to a full extend. Also, the Act still speaks of personnel onboard the ship. The threat of cyber piracy on unmanned and autonomous vessels is therefore not covered.

South African cyber-related law is addressed in the Cybercrimes and Cybersecurity Bill. As shown in chapter 3 of this thesis, the Cybercrimes and Cybersecurity Bill's scope also includes cyber piracy onboard unmanned and autonomous ships. The Bill's main objective is to deal with cyber-offences and impose penalties on such crimes, to regulate jurisdiction and investigations, and to provide proof of cyber-related incidents.[444] Overall, the Bill focuses on measures regarding the prosecution of cybercrimes. However, it does not present preventive or risk management provisions on how to obviate cyber piracy from occurring. In conclusion, the South African Cybercrimes and Cybersecurity Bill does not offer prevention for cyber piracy attacks on unmanned and autonomous ships.

5.3.2 The criminal offence and its sentence

In South Africa, the court's decision is guided by the sentencing principles known as 'triad of Zinn'.[445] The three general guides that lead to the development of the sentence are the seriousness of the offence committed, the personal circumstances of the offender, and the public interest in this matter.[446] Besides the triad of Zinn, South Africa enacted minimum sentences for certain serious offences such as murder, rape, smuggling of ammunition, and theft.[447] For the offences relating to hijacking a ship or endangering safety of maritime navigation as defined in

[442] Compare section 61(a), (b), (c), and (f) Annex 2 of the MSR.
[443] Compare section 61(d) and (j) Annex 2 of the MSR.
[444] Compare Preamble of the Cybercrimes and Cybersecurity Bill.
[445] S v. Zinn 1969 (2) SA 537, 540.
[446] Ibid.
[447] Section 51 of the Criminal Law Amendment Act No. 105 of 1997.

section 10 of the POCDATARA, section 18(1) of the POCDATARA describes penalties and reads as follows:

'any person who is convicted of an offence referred to in section 10 is liable (i) in the case of a sentence to be imposed by a High Court, to a fine or to imprisonment for a period up to imprisonment for life; (ii) in the case of a sentence to be imposed by a regional court, to a fine or to imprisonment for a period not exceeding 18 years; (iii) in case of a sentence to be imposed by a magistrate's court, to a fine or to imprisonment for a period not exceeding five years.'

Because certain acts of cyber piracy fall under the definition of the offence according to section 10 POCDATARA the sentence for such crimes could be anything ranging between a fine or imprisonment for life. If cyber piracy would fall under the definition of the term 'piracy' under section 24 of the Defence Act the sentence according to section 24(3) of the Defence Act could include 'a fine or to imprisonment for any period including life imprisonment'. For the sentencing of the crime it does not make a difference that cyber piracy does not qualify as piracy under section 24 of the Defence Act but only as an offence relating to hijacking a ship and endangering the safety of maritime navigation as for both crimes the offender could be sentenced to a penalty of imprisonment for life.

The sentencing for cybercrimes is dealt with in chapter 2, part V of the Cybercrimes and Cybersecurity Bill and can be found in section 19 of the Cybercrimes and Cybersecurity Bill and reads as follows:

'(1) Any person who contravenes the provisions of section 2(1), 3(3) or 7(2) is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment.
(2) Any person who contravenes the provisions of section 3(1) or (2), 4(1), 5(1), 6(1) or 7(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment.
(3) Any person who contravenes the provisions of section 11(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 15 years or to both a fine and such imprisonment.
(4) A court which convicts a person of an offence in terms of section 8, 9(1) or (2), 10 or 11(2) may, where a penalty is not prescribed in respect of that offence by any other law, impose a

sentence, as provided for in section 276 of the Criminal Procedure Act, 1977, which that court considers appropriate and which is within that court's penal jurisdiction.

(5) A court which imposes any sentence in terms of this section, or where a person is convicted of the offence of theft that was committed or facilitated by electronic means, must, without excluding other relevant factors, consider as aggravating factors—

(a) the fact that the offence was committed by electronic means;

(b) the extent of the prejudice and loss suffered by the complainant or other person as a result of the commission of such an offence;

(c) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or

(d) the fact that the offence was committed in concert with one or more persons.

(6) If a person is convicted of any offence provided for in section 2(1), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2), a court which imposes any sentence in terms of those sections where the offence was committed—

(a) by a person; or

(b) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed, must, unless substantial and compelling circumstances justifying the imposition of another sentence impose, with or without a fine, a period of direct imprisonment which may not be suspended as contemplated in section 297(4) of the Criminal Procedure Act, 1977.

(7) Any person who contravenes the provisions of section 14, 15 or 16 is liable on conviction to a fine or to imprisonment of a period not exceeding three years or to both a fine and such imprisonment.'

Because cyber piracy falls under the scope of the Cybercrimes and Cybersecurity Bill the sentence for the crime could range from a fine up to 15 years' imprisonment. In conclusion, the sentence for cyber piracy depends on various factors and cannot be generalised. First of all, a minimum sentence could be imposed by the court if the outcome of the crime would fulfil one of the above-mentioned offences such as murder or theft. Section 19 of the Cybercrimes and Cybersecurity Bill offers a wide range of penalties depending on the offence. The sentence can be anything between a fine and imprisonment of up to 15 years. Even though section 19 of the Cybercrimes and Cybersecurity Bill limits the imprisonment to a relatively low number of years

of imprisonment, section 18 of the POCDATRA provides for imprisonment of up to 18 years or imprisonment for life depending on the court. For the act of cyber piracy the sentence could therefore be as low as a fine or as high as imprisonment for life depending on its seriousness.

5.3.3 The national implementation of international jurisdiction regarding cyber piracy

South African legislation on the application of the principles of international jurisdiction is not defined in a single Act only but can be found in the respective specific legislation. Chapter 3 Part 1 of the POCDATARA deals with the jurisdiction in respect of the offences committed under this Act. Section 15 of the POCDATARA states:

'(1) A court of the Republic has jurisdiction in respect of any specified offence as defined in paragraph (a) of the definition of 'specified offence', if-

(a) the accused was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic; or

(b) the offence was committed

(i) in the territory of the Republic;

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed;

(iii) by a citizen of the Republic or a person ordinarily resident in the Republic; against the Republic, a citizen of the Republic or a person ordinarily resident in the Republic;

(iv) against the Republic, a citizen of the Republic or a person ordinarily resident in the Republic (…)

(vii) when during its commission, a national of the Republic is seized, threatened, injured or killed (…)

(c) the evidence reveals any other basis recognised by law.'

The section codifies the principle of territoriality[448] and the flag principle[449] and gives a South African court the jurisdiction if the offender committed a crime on South African territory including its territorial waters. It also includes the principle of nationality[450] and the passive

[448] Compare section 15(1)(b)(i) of the POCDATARA.
[449] Compare section 15(1)(b)(ii) of the POCDATARA.
[450] Compare section 15(1)(b)(iii) of the POCDATARA.

personality[451] principle. Besides the principles that require a legal link sub-section '(c)' could be understood to include universal jurisdiction as it states that 'a court of the Republic has jurisdiction in respect of every specified offence (…) if the evidence reveals any other basis recognised by law'.[452] Section 15(1)(c) of the POCDATARA could be interpreted so that the principle of universal jurisdiction is seen as a 'basic recognised by law' applies in cases where it is recognised by any law already. This interpretation would lead to the application of the universal principle for cyber piracy if it would be qualified as piracy or any other crime that is reacted to with universal jurisdiction. This is however not the case as cyber piracy is not considered as an act of piracy but rather an act of cybercrime. If cyber piracy would fall under the definition of piracy under section 24 of the Defence Act the relevant provision would be section 29 of the Defence Act. In conclusion, cyber piracy prosecution would require a legal link. Unlike German law, section 15(1)(c) of the POCDATARA does not link universal jurisdiction to section 10 of the POCDATARA in general but only to those offences that are already recognised by law to be prosecuted in a certain way.

For cybercrimes, chapter 3 of the Cybercrimes and Cybersecurity Bill deals with jurisdiction. Section 24 of the Cybercrimes and Cybersecurity Bill reads as follows:

'(1) A court in the Republic trying an offence has jurisdiction where –

(a) an offence in terms of Part I or Part II of Chapter 2 was committed –

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed. (…)

(b) an offence in terms of Part I or Part II of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is citizen of the Republic or ordinarily resident in the Republic;

(c) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is—

(i) a company, incorporated or registered as such under any law, in the Republic; or

(ii) any body of persons, corporate or unincorporated, in the Republic;

[451] Compare section 15(1)(b)(iv) of the POCDATARA.
[452] Compare section 15(1)(c) of the POCDATARA.

(d) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against—

(i) a restricted computer system contemplated in section 11(1)(b); or

(ii) a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or

(e) any act in preparation of an offence in terms of Part I or Part II of Chapter 2, or any action necessary to commit the offence took place—

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed.

(2) If the act alleged to constitute an offence in terms of Part I or Part II of Chapter 2 was committed outside the Republic, a court of the Republic, regardless of whether or not the act constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged—

(a) is a citizen of the Republic or ordinarily resident in the Republic;

(b) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;

(c) is a company, incorporated or registered as such under any law, in the Republic; or

(d) any body of persons, corporate or unincorporated, in the Republic.

(3) Any act alleged to constitute an offence in terms of Part I or Part II of Chapter 2 and which was committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act constitutes an offence or not at the place of its commission, deemed also to have been committed in the Republic if that—

(a) person is found to be in South Africa; and

(b) person is for one or other reason not extradited to, or by South Africa, or if there is no application to extradite that person.

(4) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted.

(5) (a) A prosecution in terms of subsections (2) and (3)—

(i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and

(ii) must commence before a court designated by the National Director of Public Prosecutions.

(b) A copy of the written permission and designation must be served on the accused and the original thereof must be handed in at the court in which the proceedings are to commence.

(6) The National Commissioner and the National Head of the Directorate, respectively, in consultation with the National Director of Public Prosecutions must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act regarding the investigation of offences that was committed outside the Republic.'

Therefore, section 24(1) the Cybercrimes and Cybersecurity Bill describes the principle of territoriality[453] and the flag principle[454]. Section 23(b) of the Bill includes the principle of nationality. Section 24(c) of the Bill includes companies that are registered in South Africa. The principle of universal jurisdiction does not apply as it is not mentioned in the section. This means that cybercrimes and also cyber piracy attacks need a legal link that connects the committed crime to South African prosecution.

5.3.4 Law enforcement

The law enforcement outside of South African territorial waters and for piracy is included in chapter 4 of the Defence Act 42 of 2002.[455] According to section 22 of the Defence Act, the use of a warship owned by the defence force can be used to enforce any provision of South African law at sea in internal waters[456] and territorial waters,[457] and outside the territorial waters against foreign ships only if international law permits it[458]. In addition to that, section 25(1) Defence Act states that 'an officer of the Defence Force may seize a ship or aircraft, and the property on board, and arrest any person on board, in accordance with Article 105 and 107 of UNCLOS'. According to section 25(3) Defence Act, the South African National Defence Force is entitled to bring the offenders back to the South African mainland to face prosecution in a South African court. In the case of piracy, the National Defence Force, therefore, enforces the law. Law

[453] Compare section 24(1)(i) of the Cybercrimes and Cybersecurity Bill.
[454] Compare section 24(a)(ii) of the Cybercrimes and Cybersecurity Bill.
[455] Defence Act No. 42 of 2002.
[456] Compare section 22(2)(a) Defence Act.
[457] Compare section 22(2)(b) of the Defence Act.
[458] Compare section 22(3)(b) of the Defence Act.

enforcement including the power to investigate, search, access and seize regarding cybercrimes is regulated in chapter 4 of the Cybercrimes and Cybersecurity Bill. In general, any police official can execute the powers and investigate the case following the Criminal Procedure Act 51 of 1977.[459] This means the South African Police Service (SAPS) enforces cyber-related law.

5.3.5 The court's jurisdiction

In South Africa, criminal courts are differentiated into the Magistrates' Courts, the High Court, the Supreme Court of Appeal, and the Constitutional Court.[460] Chapter 8 of the Constitution of South Africa[461] deals with the courts and the administration of justice and establishes the structure of the judicial system. For the Magistrate' Courts, South African law differentiates between the Regional Magistrates' Courts which only deal with criminal cases, and District Magistrates' Court which deal with both criminal and civil matters. The latter can hear offences that are less serious involving all crimes excluding rape, murder, and treason[462] and can impose fines up to ZAR 120,000.00 and imprisonment of up to three years. The Regional Courts deal with more serious crimes including the above-mentioned ones expect treason[463] and can impose fines up to ZAR 600,000.00 and can sentence up to 15 years in prison. The High Court hears appeals from the magistrates' courts and acts as the court of the first instance for cases where the sentencing exceeds the lower court's jurisdiction.[464] It has jurisdiction in its area over all persons residing or present in that area. The Supreme Court of Appeal only hears appeals from the High Court and has no first instance jurisdiction and its proceedings must ordinarily be presided over by five judges.[465] Cyber piracy would be tried at a Regional Court because of the seriousness of the crime. Only in less severe cases, a District Court would exercise jurisdiction.

5.4 Concluding Remarks

In the first part of the chapter it was discovered that neither German nor South African maritime-related law addresses the risks of cyber piracy on unmanned and autonomous ships to a full extant. The South African MSR, however, shows more potential than German legislation. German cyber-related law excludes onboard systems completely and only focuses on land-based facilities which means the SCC but not the vessel itself would be covered. However,

[459] Compare section 27 of the Cybercrimes and Cybersecurity Bill.
[460] Compare Article 166 of the Constitution of South African.
[461] Constitution of the Republic of South Africa of 4 February 1997.
[462] Compare section 89(1) of the Magistrates' Court Act No 32 of 1944.
[463] Compare section 89(2) of the Magistrates' Court Act.
[464] Compare section 21 of the Superior Court Act No. 10 of 2013.
[465] Compare section 13 of the Superior Court Act.

German law could easily be modified to include onboard IT systems as well. The problem is that the IT standards for the shipping sector do not exist. South African legislation focuses only on the prosecutorial measures that come into effect after the cyber piracy attack has already been launched against the vessel but lacks sufficient preventive measures. Overall, both German and South African maritime- and cyber-related legislation is currently not responding to cyber piracy on unmanned and autonomous ships in a preventive way.

In Germany cyber piracy is tried as a combination of maritime- and cyber-related offences. This leads to the appliance of the principle of universal jurisdiction. South African law, however, requires a legal link between the offence and the prosecution. For both countries, it is not clear which authorities would be in charge to enforce the law as the authorities for piracy and cyber-crimes law enforcement differ.

6 CONCLUSIONS

6.1 New Definitions

In chapter 2.3 of this thesis, we took a closer look at the definitions of the terms ‘autonomous’, ‘unmanned’, ‘ship’, and ‘master’. We discovered that the terms ‘unmanned’ and ‘autonomous’ are already defined. We also discovered that an unmanned and autonomous ship fulfils the requirements of the definitions used for the term ‘ship’ under multiple regulations. The term ‘master’, however, does not cover any people operating a ship from land and therefore does not include a remote-controller, a supervisor, or a pre-programmer at the SCC. In chapter three of this thesis, we took a look at the term ‘cyber piracy’. We discovered, that the act does not fall under the scope of UNCLOS and that the SUA Convention only applies partly but is missing an overall definition of the term. The next sub-chapters will present a possible definition of the terms ‘unmanned’ and ‘autonomous’, on the term ‘ship’ and ‘master, and the term ‘cyber piracy’.

6.1.1 The terms ‘unmanned’ and ‘autonomous’

Even though the terms ‘unmanned’ and ‘autonomous’ are already defined it would be helpful for future codification of the terms to draft a compressed definition. The following definitions are just one example of how to define the terms. The definitions will have to be continuously updated following the technological progress in the shipping industry. In the future, it may become necessary, for example, to divide the different degrees into further sub-degrees.

‘Unmanned’ means that there is no human presence on board the ship to perform or supervise the operation of a vessel. A periodically unmanned ship is designed to operate without a crew on board for a limited defined period of time. A continuously unmanned ship is designed to operate without a crew on board at any time.

‘Autonomous’ means that a vessel can perform a set of defined operations with no or reduced attention from a ship bridge crew or shore control centre crew. Autonomy degrees are as follows: remote-controlled, automatic, independent, and fully independent vessels. Remote-controlled vessels are continuously under the control of human authority (remote-controller). Automatic vessels complete certain operations without any human interference but can be supervised at any time by human authority (supervisor). Independent vessels are automatic vessels that are pre-programmed to solve a variety of occurring problems on their own but can be

supervised at any time (pre-programmer and supervisor). Fully independent vessels operated completely on their own with no human supervision what so ever (pre-programmer).

6.1.2 The term 'ship'

Even though unmanned and autonomous ships fall under the definition of the term 'ship' it could still be helpful to update current definitions to explicitly include unmanned and autonomous ships. In doing so the international shipping industry will become more aware of the new technology and the clarification could prevent wrong interpretation in the future. The following two definitions include the two elements that were discovered to be mostly included in any definition of the term 'ship': navigation by water and the transportation purpose. Other additions such as the weight of the ship can be made if necessary in a certain case that requires it. A short definition of the term ship could read as follows: 'Ship' means any vessel used as means of transportation by sea regardless of its navigation type and its manning level. A longer but also more clarifying definition could be as follows: 'Ship' means a vessel of any type whatsoever operating at sea and includes any degree of autonomous operating vessels, unmanned vessels, hydrofoil boats, air-cushion vehicles, (…) that is used for the transport of goods, passengers, or both.

6.1.3 The term 'master'

As shown above, the terms 'master' only applies to any person working onboard the vessel. The shore remote-controller and the supervisor at the SCC or the pre-programmer of a vessel cannot be considered as masters of a ship. The traditional master plays a central role and has to fulfil a wide range of duties. But because he or she is currently understood to be on board a ship, many legal regulations do not apply to unmanned and autonomous ships. Some of the master's duties could – maybe slightly modified - also be met by the master on land which means the same regulations could apply for both. For this reason, the current definition of the term 'master' would have to be updated to include the person in charge on land. Therefore, it will be necessary to define the terms 'shore control centre', 'remote-controller', 'supervisor', and 'pre-programmer' to include them in the legal frameworks. A master's main duty is to navigate the ship. But other than that, he or she also has to fulfil a wide range of other duties that are not related to the navigation of a ship. As navigating an unmanned and autonomous ship will be a very technical job the training will differ immensely from a traditional master's training. Therefore, it would be easier to split the master's duties into navigational and non-navigational duties. The navigational duties will be fulfilled by the remote-controller, the

supervisor, or the re-programmer of the ship. The non-navigational duties will be fulfilled by another person. For the purpose of this thesis, this person will be called the duty. Together they fulfil the duties of a traditional master. Also, it will be necessary to include a definition of the crew at the SCC which for the purpose of this thesis will be called the centre crew (CC). The following definitions are one example of how to legally fill the terms:

'Shore Control Centre' means the land-based facility from where a shipowner monitors and controls an autonomous vessel of any degree on the water.

'Duty' means the person in charge of any decision at the shore control centre other than navigational ones.

'Remote-controller' means any person at a shore control centre that is in charge to navigate a remote-controlled ship.

'Supervisor' means any person at the shore control centre that is in charge to overlook the journey of an automatic or independent ship and can interfere at any time.

'Pre-programmer' means any person that programs the computer system of an autonomous ship prior to its journey for the ship to navigate itself independent or fully independent.

'Centre Crew' means all personnel working at the shore control centre supporting the remote-controller, the supervisor, the pre-programmer, and the duty in fulfilling their responsibilities.

The above-mentioned definitions could be used for any new legislation that is specifically drafted for autonomous ships. Whenever common ships and autonomous ships are addressed by the same legislation the old definitions could also be modified. For the term 'crew' a modified definition could, for example, be: 'Crew' means all personnel working onboard a ship or at a shore control centre.

6.1.4 The term 'cyber piracy'

A definition of the term 'cyber piracy' meaning a cyber-attack on an unmanned and autonomous ship does not exist. Before drafting a definition of the term 'cyber piracy' one important question arises: In which legislation should such a definition be included? Both elements of cyber

piracy, piracy and cybercrime, are international threats that are not a problem to one state only but spread across all borders. Therefore, cyber piracy should also be addressed internationally. One can even say that cyber piracy is even more universal than piracy or cybercrime alone as it consists not only of one international but both border crossing elements. The only way to respond to such a threat is to include it in international legislation. As shown above, cyber piracy and piracy have a lot in common and cyber piracy could be considered as a modern type of piracy. In my opinion, it should therefore be included in a maritime specific law. However, including cyber piracy into UNCLOS would not be very convenient. The practicalities of an amendment to UNCLOS are very complex.[466] A very complicated amendment procedure, which has never been invoked before makes it difficult to include cyber piracy.[467] Also, it is unlikely that a conference with all the state parties will be convened to adopt a change like this.[468] However, on the theoretical side of things, it is still very interesting to draft a definition of cyber piracy in the manor of Article 101 of UNCLOS to show its resemblance to piracy.

The definition of cyber piracy should start with the description of the act itself. As stated above, cyber piracy is not an act of violence but could be described as any unauthorised act or illegal influence initiated in or through cyber space using a computer or any other electronic device. It must also be considered that the device could be used from anywhere in the world or could as well be part of the SCC or the ship itself. The first part of the definition could read as follows: *Cyber piracy is any illegal or unauthorised act or influence initiated in or through cyber space from any computer, or similar technological device, including those of the SCC itself or connected to such a centre, committed from anywhere in the world.*

Secondly, the definition must state for what ends the act would be committed. Piracy must be committed for private ends. As stated in chapter 3, this aspect is very controversial but only plays a subordinate role for this thesis. As shown above, the better arguments support that the term private ends should only exclude any activities that are lacking in state sanctioning. To clarify that the term should not exclude political, religious, and ethnic motivated attacks but

[466] V Surbun *'Piracy Jure Gentium in Territorial Seas: A Perspective from the East African Seaboard'* (2017) 294.
[467] Ibid.
[468] Ibid.

only those that are being committed by a state or on its official behalf, the definition could slightly be modified as follows: *committed for ends not taken on behalf of a State*.[469]

For the third part of the definition, it is particularly important to identify the different potential groups of people who might be involved in a cyber-attack of a ship and could, therefore, be defined as cyber pirates. First of all, those people must be taken into consideration that are directly involved in the control of the ship. This would be, depending on the degree of autonomy, the remote-controller, the supervisor, or the pre-programmer of the ship. Besides, any person that was somehow involved in the production of the IT system's software belongs to this group as well. Those people could already have manipulated the software of the ship against the will of the ship owner during the programming process to intervene unauthorised at any time. Another potential group is the one who is neither directly nor indirectly involved in the control of the ship but who has been granted authorised access to the SCC or the ship itself. This includes all employees in the broadest sense such as mechanics and office staff as well as visitors to the ship and the SCC. The last group of people that has to be taken into consideration is the one who has no legal access to the ship or the premises of the SCC. This includes persons who illegally gain access to the vessel or the SCC to manipulate the software on-site and as well as those people who hack and manipulate the software from anywhere in the world via the internet using their technical device. Taking all this into consideration, the next part of the definition of cyber piracy could be as follows: *Any act (…) committed by any person that has authorised access to the SCC of a private ship or the ship itself, any person that was included into the process of programming the software of such ship, or any third party.*

The next step is to identify the potential targets of a cyber piracy attack and include them in the definition. Access to the ship's system could be gained through two different interventions. The cyber pirate could hack into either the ship's or the SCC's computer system. The original definition of piracy states that the act must be committed outside of the jurisdiction of any State (Article 101(1)(a)(ii) of UNCLOS 'against a ship, aircraft, persons or property in a place outside the jurisdiction of any State'*).* The definition excludes acts that are taking place in the territorial waters of a state. This is because a state has exclusive sovereignty over its territory. Therefore, this aspect should also be part of the definition of cyber piracy. This leads to the question of whether or not the attack on the SCC's system should become part of the definition as it is

[469] If a phrase like this would be included into the definition of the term cyber piracy under UNCLOS, the definition of piracy in Article 101 of UNCLOS would also have to changed accordantly. Otherwise the difference between the two definition would lead more controversial discussion.

located on land and within a state's territory and its jurisdiction. However, as shown above, the hacking of the system of the SCC affects not mainly the control centre but the ship itself. Because of this, the definition should not focus on the location of the cyber piracy attack if its outcome only affects the ship's system. In this case, the interpretation of the situation depends on where the ship is located at the moment of the attack. If the ship is located outside the jurisdiction of a state it does not matter which system got originally hacked to control the ship. The act must be detected against a computer system or part of such a system of a ship outside of the jurisdiction of any state or the SCC. Taking all of this into consideration, the next part of the definition could sound like this: *Any act (...) against a computer system of a ship or SCC if the attack is only used to affect the ship's system, or part of such systems when the ship is located outside of the jurisdiction of any State.*

The last part of the definition must state the objective of the cyber piracy attack. The first aim of an attack could be to endanger or injure the life or physical integrity of another person. This aim could be fulfilled if the ship would be used as a weapon. The ship could be directed unrestrained into a port facility or coastal region or could be controlled for the purpose to collide with another ship. Another objective could be to harm the ship owner´s property. It could either be the ship itself that the cyber pirate is interested in or just the cargo of the ship. To reach that goal the ship could be taken to a foreign port or into 'safe waters' so the ship's cargo can be offloaded. Another scenario could be that the attacker wants to deliberately damage the ship´s owners' business or contracting partners. The goal could then be to damage or sink the ship or its cargo or simply abandon the course of the ship for a while. The latter could be done so the owner would suffer financial penalties due to delivery delays. Lastly, the attack could simply be designed to obtain personal information stored on the software or to falsify or delete such information to either harm the owner of the ship or to gain benefits. Because the goals of a pirate and a cyber pirate are similar the last part of the definition practically lines up with the original definition provided by Article 101 of UNCLOS and could sound as follows: *The act must be committed (...) to harm people or property or to compromise the confidentiality, integrity or availability of the ship, its computer system or the information stored on it.*

The subparagraphs (b) and (c) of the definition of piracy can be adopted as they are: *Cyber Piracy is any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making is a pirate ship and any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).*

Putting the pieces together the full definition of the term cyber piracy would sound as follows:
Cyber piracy consists of any of the following acts:
(a) Cyber piracy is any illegal or unauthorised act or influence initiated in or through cyber space from any computer, or similar technological device, including those of a the SCC itself or connected to such a centre, committed from anywhere in the world for private ends not taken on behalf of a State, by any person that has either authorized access to an SCC of a private ship or the ship itself, or any person that was included into the process of programming the software of such ship, any visitor or any third party and directed:
(i) against a computer system of a ship or the shore control centre itself, or part of such systems, when the ship is located outside of the jurisdiction of any State;
(ii) to harm people or property or to compromise the confidentiality, integrity or availability of the ship, its computer system or the information stored on it
(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making is a pirate ship or aircraft;
(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

An option to include cyber piracy in an international Convention could be to modify the SUA Convention. Even though the Convention does not exclude cyber piracy completely, it is still lacking an overall definition of the term. The act does not fall under the scope of Article 3 (1) of the SUA (*1. 'Any person commits an offence if that person unlawfully and intentionally seizes or exercises control over a ship by force or threat thereof or any other form of intimidation')* which provides the overall definition for any act that threatens the safety of ships at sea. For the SUA Convention, it would be more practical to include the definition of cyber piracy directly into Article 3 as the scope of the Convention is already much broader and Article 3 includes many different alternatives already. The general definition of cyber piracy could be directly included in Article 3 (1) of the Convention. Also, Article 3 (5) of the SUA could be added to clearly include the SCC. The definition in Article 3 of the SUA Convention could be modified as follows:
'1. Any person commits an offence if that person unlawfully and intentionally
1. seizes or exercises control over a ship by force or threat thereof or any other form of intimidation or through the cyber space; or (...)

5. destroys or seriously damages maritime navigational facilities including any SCC or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship; (...).'

6.2 Regulations to Prevent Cyber Piracy

In chapter 4.1 of this thesis, we took a closer look at maritime-related and cyber-related regulations and guidelines that are currently in place to help prevent cyber piracy on an international level. Chapter 5.2.1 and 5.3.1 dealt with national preventive regulations. We discovered that the international compulsory law does not prevent cyber piracy on unmanned and autonomous ships to a full extent. Nationally, German cyber-related law showed more potential than South African law to prevent cyber-attacks in general but excluded cyber piracy. South African maritime-related law showed more potential than German law in this area as it is orientated on the ISPS Code. The following sub-chapter presents some ideas on how improve preventive measures into both international and national legislation further.

6.2.1 International regulations

As laid out in chapter 4 of this thesis, the International Safety Management Code and the International Ship and Port Facility Security Code would be the right place to include preventive regulations concerning cyber piracy on unmanned and autonomous ships. Especially the ship's security plan that is mandatory according to the ISPS Code and the safety management manual which is mandatory according to the ISM Code could be used to include measurements to prevent cyber piracy incidents on unmanned and autonomous ships. Especially the ISPS Code could be the preferable legislative ground to include preventive measures in this matter. So far, the ISPS Code requires that a ship´s master and/or a ship security officer are on board a ship. Therefore, those regulations that address the master and the ship security officer must be changed to include the remote-controller, the supervisor, and the pre-programmer as well as the duty or other onshore personnel. After making the ISPS Code applicable to unmanned and autonomous operations, the regulations must then be modified to prevent cyber piracy. As stated above, this should be done by including preventive measures into the ship security plan and cyber piracy specific regulations into the ISPS Code.

The first step of prevention is to raise awareness on the topic and to educate personnel. This can be done by enforcing awareness training for the involved staff members. This especially includes the SCC personnel and the ship owner. It can also include other port facility personnel

and traditional staff such as masters and crew of manned operations. The awareness training should give an overview of unmanned and autonomous ships and their onboard technology, the possible targets and vulnerabilities of such ships, the potential cyber pirate groups including their motivations and objectives, and the general cyber security risks and controls. The awareness training should be mandatory to those who work closely with unmanned and autonomous operations and obligatory to those working in the general maritime shipping sector and should be held annually hosted by the ship owner. In addition to the cyber security training, the ship owner should also run cyber security practice drills. This could be done similar to the Naval Dome cyber security test and would help to find out if the cyber systems are sufficiently secured and if the SCC personnel would react according to the cyber security plan. The drill can discover gaps to prepare and improve the plan in case of a real cyber incident.

The next step would be to make it mandatory for every ship that uses onboard information systems and especially for unmanned and autonomous vessels, to have a cyber security officer (CSO) that only deals with matters regarding cyber security. The CSO would also have to attend mandatory training that deals in detail with the ship's and SCC's information technology and its sufficient security. The personal details of the responsible CSO and his or her training certificate would have to be included in or attached to the ship security plan.

The ship security plan in general should have one section that is dedicated to cyber security. To implement appropriate measures for every ship, it would be helpful to include a vulnerability rating system. For example, this rating system could have three vulnerability levels with level one being the lowest and level three being the highest vulnerability level. Each level would then be bound to different security measures. To set the level for a ship, numerous aspects would have to be taken into consideration. The first thing that should impact the setting of the vulnerability level should be the degree of autonomy and whether or not the ship will operate unmanned. The higher the degree of autonomy the more vulnerable the ship will become to cyber piracy. The next aspect that should have an impact on the vulnerability level should be the type of the ship. As shown above, a cargo ship's vulnerability should be considered higher than the one of a fishing vessel.[470] Other factors that should be considered when setting the level are the intended route of the ship, the ship's cargo, but also the flag state of the vessel, and the ship's

[470] This would be in the unlikely event that a fishing vessel would even be unmanned and autonomous in the future. Due to changing weather, wind, currant, and fish movement conditions it would almost be impossible or at least not sufficient to operate unmanned and autonomous.

owner. Every vulnerability level should then lead to different cyber security measures. Higher vulnerability levels set out stricter cyber security demands.

After stating the level of vulnerability, it should be mandatory for every level to include a list with all onboard technology and its description in the ship security plan. The list should then be followed by a risk analysis of the information technology systems. The most important step would be to secure information technology through sufficient software that protects the systems from cyber incidents. Such software would have to be updated and maintained to secure up to date protection. Also, the most important information systems should be separated from each other in a way to secure that in case of a cyber incident the systems will not be taken down all at the same time. Technology that is used for the navigation of the ship and its communication with the SCC should also have back-up systems that can be accessed separately.

Another very important objective would be to state who will be allowed to have physical access to both, the ship and the SCC. Different areas of the ship and the SCC could have different authorisation levels which means only very few people would, for example, be allowed near vulnerable areas such as the control room at the SCC. But not only physical access should be limited. Besides, network access control would have to be established to control the access to the wireless networks that are used onboard and at the SCC. Other measures would have to include a policy for the use of removable storage media such as USB sticks, external drives, CDs, and DVDs. All of these devices could be used to interfere with the onboard technology and could contain computer viruses and other malware.

In addition to cyber piracy prevention, the ship security plan must also include an appropriate management procedure plan to deal with a cyber pirate attack and its outcome in case the preventive measures have failed. This plan should include at least three different stages: the detection of an incident, the response to it, and the recovery from it. It must be clear how SCC personnel would have to respond to a cyber piracy attack and who would be in charge to make decisions. Also, the incident would have to be reported to the authorities as soon as possible. The last thing to keep in mind is that the ship security plan should always be updated according to the development of the technology.

6.2.2 National regulations

Even though cyber piracy is a global and cross-border threat and should therefore be primarily addressed on an international level, it is also important to respond to it through national legislation. For German legislation, the Verordnung über die Sicherheit de Seefahrt der Bundesrepublik Deutschland could be the right place to include regulation to prevent cyber piracy on unmanned and autonomous ships. This ordinance already includes some cyber security measures and could easily be expanded to include cyber piracy as well. For South African legislation, it could be helpful to include preventive measures against cyber piracy on unmanned and autonomous ships into the MSR as the regulations refer to all security measures onboard ships and at the ports. Because the act still uses the terms 'master' and 'crew' when refereeing to ship's personnel the regulations would have to be slightly modified to include unmanned operations as well. Therefore, the above-defined terms of the SCC personnel would have to be included. Also, the scope of the preventive measures would have to be widened to include cyber threats as well. The measures that would have to be implemented into German and South African law are the same that are already described above for the international implementation. On a national level, however, the legislation could go into more detail with regard to, for example, the content of the cyber security training for the CSO and other personnel, the performance of the security practice drill, the outline of the cyber security certificate. However, the setting of the vulnerability level and the measures that are bound to it should follow equal international standards to ensure the same grade of cyber security.

6.3 International Jurisdiction

As shown in chapter 4.2 of this thesis, in an international context cybercrimes and piracy are not treated the same way with regard to international jurisdiction. Because cyber piracy is believed to be more an act of cybercrime and not so much an act of piracy it also leads to a different judgement. Piracy is a crime that is dealt with using universal jurisdiction while cybercrimes are not. Because of the understanding of cyber piracy being a cybercrime, it is also not subject to universal jurisdiction. However, it is already arguable that cybercrimes, in general, should be subject to universal jurisdiction. The internet poses similar legal challenges to the world's oceans: both, the World-Wide-Web and the international waters of the sea are shared globally. In the future, cybercrimes could lead to disastrous outcomes because the world relies more and more on information technology. Depending on the target a cyber-attack could affect not only individuals or businesses but also an entire province or country and could have a cross-border impact. It could, for example, affect supply chains for essential goods and interrupt public

access to the media coverage. Therefore, it should be in the interest of the international community to be able to prosecute these crimes universally. At the moment, however, only serious global crimes against bodily integrity allow for the assertation of universal jurisdiction. Cyber piracy has a very unique position in the field of cybercrimes as it can have a similar outcome to an act of piracy. There are two possible options on how to include universal jurisdiction to cyber piracy into the international legal framework. The first one is to add the act of cyber piracy to UNCLOS. This way the universal jurisdiction codified in Article 105 of UNCLOS would apply to both kinds of piracy. However, as mentioned above, an amendment to UNCLOS is highly unlikely. The other would be to draft an international cybercrime treaty that establishes universal jurisdiction over all cybercrimes. This would then include cyber piracy as well. However, the practicalities of these suggestions are also very complicated as universal jurisdiction could entail the encroachment of another state's sovereignty where cyber-attacks are land-based. For cyber piracy however, the land-based attacks are not problematic as universal jurisdiction would only apply if the ship at sea would be under attack.

6.4 International Court

As discussed in chapter 4.3 of this thesis, in addition to international and national legal improvement, it could also be very helpful to establish an international court to prosecute cyber piracy. The first option would be to try cases of cyber piracy at the same international court that would have to be established to prosecutes piracy. As presented in the chapter such an international court has not yet been established but could either be an independent court that only deals with piracy or a chamber at the International Tribunal for the Law at Sea that specialises in piracy cases. The advantage of trying cyber piracy and piracy at the same court would be that both crimes would be prosecuted in a unified manner that considers that cyber piracy is just a modern version of piracy that leads to the same outcome. The court would also be specialised in maritime legislation which means it would be able to take all the specific aspects of maritime law into account. However, the disadvantage of this option is that the court may lack expertise concerning cyber-related legislation. Another possibility would be to prosecute cyber piracy at a court that mainly deals with cybercrimes. Such an international court does not yet exist. However, the establishment of such a court also seems to become a necessity considering the increase of international cybercrimes. The advantage of this option would be that the court would have the cybercrime-related expertise. The disadvantage, however, would be that the legal assessment of cyber piracy cases would most likely be lacking maritime specification. The crime would be treated similarly to any other cybercrime and it would not be considered that cyber

piracy could be seen as a modern version of piracy. The last alternative would be to establish a court that specialises in cyber piracy crimes only. This way the court could be specialised in both areas of law. However, even though cyber piracy is a serious threat to the maritime industry there are not enough cases yet to justify the establishment of a court that only deals with the threat. Because this thesis argues that when assessing the act of cyber piracy, the focus of reprehensibility lays on the outcome of the crime, establishing an international court dealing with both piracy and cyber piracy would be the preferred option. Even though the attack itself can be seen as a normal cybercrime the outcome of the crime and its impact on its victim is very similar to piracy. Especially when adding cyber piracy to UNCLOS, presenting it as an equal threat as piracy it would only be logical when trying cyber pirates in the same court as pirates.

Bibliography

1. International Conventions and Legislation

1.1 United Nations

1982 United Nations Convention on the Law of the Sea, 1833 UNTS 3, (1982) 21 ILM 1261. Adopted: 10.12.1982; EIF: 16.11.1994.

1988 United Nations Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1678 UNTS 221, 27 ILM 668. Adopted: 01.03.1988; EIF: 01.03.1992.

1986 United Nations Conference Convention on Conditions for Registration of Ships, 26 ILM 1229. Adopted: 07.02.1986.

1973 United Nations Convention for the Prevention of Pollution from Ships, as modified by the Protocol of 1978, 1340 UNTS 61. Adopted 1973; EIF: 2.11.1973.

1949 Geneva Convention Relative to the Treatment of Prisoners of War, 75 UNTS 85. Adopted: 12.08.1949, EIF: 21.10.1950

1979 United Nations International Convention against the Taking of Hostages, 1316 UNTS 205. Adopted:17.12.1979; EIF: 03.06.1983.

1984 United Nations Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, 1465 UNTS 85. Adopted: 10 December 1984, EIF: 26.06.1987.

1973 United Nations Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, 1035 UNTS 167. Adopted:14.12.1973; EIF: 20.02.1977.

1958 United Nations Geneva Convention on the High Seas, 450 UNTS 11, 13 UST 2312. Adopted: 29.04.1958; EIF: 30.09.1962.

1974 United Nations *International Convention on the Suppression and Punishment of the Crime of Apartheid,* 1015 UNTS 243 (1974). EIF: 18.07.1976.

1998 Rome Statute of International Criminal Court, 2187 UNTS 3. Adopted: 17.07.1998; EIF: 01.07.2002.

1995 Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks, 2167 UNTS 3. Adopted: 11.08.1995; EIF:11.12.2001.

1994 United Nations Convention on the Safety of United Nations and Associated Personnel, 2051 UNTS 363, (1995) 34 ILM 482. Adopted: 9.12.1994; EIF: 15.01.1999.

1924 International Convention for the Unification of Certain Rules of Law relating to Bills of Lading and Protocol of Signature. 1412 UNTS. Adopted: 21.12.1979; EIF:14.02.1984.

2. International Maritime Organisation

Convention on Facilitation of International Maritime Traffic, 591 UNTS 265. Adopted: 09.04.1965; EIF: 05.05.1967.

1973 International Management Code for Safe Operation and for Pollution Prevention, 1340 UNTS 61. Adopted 1973; EIF: 2.11.1973.

Convention on the International Regulations for Preventing Collisions at Sea, 1050 UNTS 16. Adopted: 20.10.1972; EIF: 15.07.1977.

Special Trade Passenger Agreement, 822 UNTS 311. Adopted: 6.10.1971; EIF: 02.01.1974.

International Ship and Port Facility Code, Adopted: 01.07.2004

Convention for the Safety of Life at Sea, 1184, 1185 UNTS 2. Adopted: 01.11.1974; EIF: 25.05.1980.

International Safety Management Code for the Safe Operation of Ships and for Pollution Prevention, 1993.

Guidelines Maritime on Cyber Risk Management' MSC-FAL.1/Circ.3; Issued: 05.07.2017.

Nairobi International Convention on the Removal of Wrecks, 55565 UNTS. Adopted: 18.05.2007; EIF: 14.04.2015.

Maritime Cyber Risk Management in Safety Management Systems Resolution MSC.428(98), Adopted: 16.06.2017.

3. Other Conventions

2014 African Union Convention on Cyberspace Security and Personal Data Protection, Adopted: 27.06.2014.

2001 Convention on Cybercrime of the Council of Europe, ETS No 185. Adopted: 23.11.2001; EIF: 01.07.2004.

2. German Legislation

Bundespolizeigesetz BGBl. I S. 2978, 2979 from 19 October 1994.

Bundeswasserstraßengesetz BGBl. I S. 962 from 23 May 2007.

Gerichtsverfassungsgesetz BGBl. I S. 1077 from 9 May 1975.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik BGBl. I S. 2821 from 14 August 2009.

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten BGBl. I S. 1354 from 1 June 2017.

Grundgesetz für die Bundesrepublik Deutschland from 23 May 1949.

Schiffsbesatzungsverordnung BGBl. I S. 2575 from 1981.

Schiffsicherheitsgesetz BGBl. I S. 2860 from 9 September 1998.

Schiffssicherheitsverordnung BGBl. I S. 3013, 3023 from 18 September 1998.

Seearbeitsgesetz BGBl. I S. 868 from 2013.

Strafgesetzbuch BGBl. S. 3322 from 1998.

Strafprozessordnung BGBl. I S. 1074, 1319 from 7 April 1987.

Verordnung über die Sicherheit der Seefahrt der Bundesrepublik Deutschland BGBl. I S. 1417 from 27 July 1993.

Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz BGBl. I S. 958 from 22 April 2016.

Völkerstrafgesetzbuch BGBl. I S. 3150 from 26 June 2002.

3. South African legislation

Criminal Law Amendment Act No. 105 of 1997.

Constitution of the Republic of South Africa of 4 February 1997.

Cybercrimes and Cybersecurity Bill B6 of 2017.

Defence Act No. 42 of 2002.

Electronic Communication and Transactions Act No. 25 of 2002.

Merchant Shipping Act No. 57 of 1951.

Merchant Shipping (Maritime Security) Regulations of 2004 published under section 356 of the Merchant Shipping Act No. 57 of 1951.

Merchant Shipping (Safe Manning, Training, and Certification) Regulations of 2013.

Protection of Constitutional Democracy against Terrorist and Related Activities Act No. 33 of 2004.

Ship Registration Act No. 58 of 1998.

4. Court decisions

4.1 Germany

Bundesgerichtshof *BGH 1951, Az.: I ZR 84/51, NJW 1952, 1135* (14 December 1951).

Landgericht Osnabrück *10 KLs - 710 Js 21274/13 - 31/13* (17 April 2014).

Landgericht Hamburg 6*03 KLs 17/10* (19 October 2012).

4.2 South Africa

S v. Zinn 1969 (2) SA 537, 540.

4.3 Other Countries

U.S. Court of Appeals for the Ninth Circuit *'The Institute of Cetacean Research v. Sea Shepherd Conservation Society*' Case No. 12-35266 (25 February 2013).

The Case of the S.S. Lotus (France v. Turkey) PCIJ Se. A, No. 10 (1927).

Cutting Case (Mexico v. the U.S.A) 1887.

Klinghoffer v. SNC Archille Lauro, 759 F. Supp. 112 (S.D.N.Y. 1992) 23 July 1992.

5. Reports

Council of the European Union *'The AU-EU Expert Report on the Principle of Universal Jurisdiction'* (16 April 2009).

International Organization for Standardization and the International Electrotechnical Commission *'ISO Survey 2018 results – Number of certificates and sites per country and the number of sectors overall'* (2018).

UITP Advancing Public Transport *'Statistics Brief - World Report on Metro Automation - July 2016'* (July 2016).

Verizon *'2019 Data Breach Investigations Report'* (2019).

World Health Organization 'World report on violence and health - Summary' (2002)

6. Articles

Andrej Andronja, Tanja Brcko, Ivica Pavic, and Harm Greidanus '*Assessing Cyber Challenges of Maritime Navigation'* Journal of Marine Science and Engineering Volume 8, Issue 10 (3 October 2020), 6-8.

A Lilington *'Listen to the people'* (April 2018) *The global seafarer*.

Arron Honniball *'The "private ends" of international piracy: the necessity of legal clarity in relation to violent political activists'* International Crimes Database Brief 13 (October 2015).

Christopher D Chen *'Computer Crime and Computer Fraud and Abuse Act of 1987'* Computer Law Journal, Volume 10, Issue 1 (1990), 71-86.

Dan Helenios *'The If, How, and When of Criminal Jurisdiction – What is Criminal Jurisdiction Anyway?'* Bergen Journal of Criminal Law and Criminal Justice, Volume 3, Issue 1 (2015) 22-47.

Douglas R. Burgess *'Hostis Humnni Generi: Piracy, Terrorism and a New International Law'* University Miami International & Comparative Law Review, Volume 13, Issue 2 (2006), 293-341.

Elizabeth Nyman *'Modern Piracy and International Law: Definitional Issues with the Law of the Sea'* Geographical Compass, Volume 5, Issue 11 (November 2011) 863-874.

Erik Barrios *'Casting A Wider Net: Addressing the Maritime Piracy Problem in Southeast Asia'* Boston College International & Comparative Law Review, Volume 28, issue 1 (2005), 149-163.

Eric Van Hooydonk *'The law of unmanned merchant shipping – an exploration'* Journal of International Maritime Law, Volume 20, Issue 6 (2014), 403-423.

Filip Koscielecki *'Autonomous shipping – Revolution by evolution'* Legal Briefing (July 2019) 3-7.

Florian Ilordanoaia *'Master of the Ship, Manager and Instructor'* Management and Marketing Journal, University of Craiova, Faculty of Economics and Business Administration, Volume 0(S1) (2010) 133-155.

Gerhard Seher *'Zur strafrechtlichen Konkurrenzlehre - Dogmatische Strukturen und Grundfälle'* Juristische Schulung (2004) 392 ff., 482 ff.

Guilia Berlusconi *'History of Piracy'* Encyclopaedia of Transnational Crime and Justice (2014) 301-3903.

Johannes Xingan Li *'Cybercrime and Legal Countermeasures: A Historical Analysis'* International Journal of Criminal Justice Sciences – Official Journal of the South Asian Society of Criminology and Victimology, Volume 12, Issue 2 (2017), 197-207.

Jörg Heidrich and Sven Tschoepe 'Rechtsprobleme der E-mail Filterung' Multimedia und Recht (2004), 75-79.

Mayank Suri 'Autonomous vessels as ships – the definition conundrum' IOP Conference Series: Materials Science and Engendering, Volume 929 (2020), 1-11.

Melanie O'Brien *'Where Security Meets Justice: Prosecuting Maritime Piracy in the International Criminal Court'* Asian Journal of International Law, Volume 4, Issue 1 (2014) 81-102.

Michael J. Kelly *'The Pre-History of Piracy as a Crime & Its Definitional Odyssey'* Case Western Reserve Journal of International Law, Volume 46, Issue 1 (2013), 25-42.

Michael P Dierks *'Computer Network Abuse'* Harvard Journal of Law and Technology, Volume 6, Issue 2 (1993) 307-342.

M Cherif Bassiouni *'Universal jurisdiction for international crimes: historical perspectives and contemporary practice'* Virginia Journal of International Law 42 (2001).

Proshanto K Mukherjee *'The SUA Convention 2005: a critical evaluation of its effectiveness in suppressing maritime criminal acts'* Journal of International Maritime Law, Volume 12, Issue (2006), 170-191.

Quoc Tien Le *'A short review: the situation of piracy in the world and proposed solutions for prevention'* International Journal of Mechanical Engineering and Technology, Volume 10, Issue 1, (January 2019) 261-276.

Rob McCusker *'Transnational organised cyber crime; Distinguishing threat from reality'* Crime Law and Social Change, Volume 46, Issue 4 (December 2006), 257-273.

Sanjana Sahu *'Passive Personality principle: An Overview'* (6 February 2015).

Sean T. Pribyl, Alan M. Weigel *'Autonomous Vessels: How an Emerging Disruptive Technology Is Poised to Impact the Maritime Industry Much Sooner than Anticipated'* RAIL: The Journal of Robotics, Artificial Intelligence & Law, Vol. 1, Issue 1 (January-February 2018), 17-25.

Susumu Ota *'Identification of IMO Regulations relating to Unmanned Operations of Maritime Autonomous Surface Ships - SOLAS Convention and Related Mandatory IMO Instruments'* Papers of National Maritime Research Institute, Volume 17, Issue 3, (2018) 227-276.

Tom Syring *'Candide, or Pessimism: Fighting Piracy and Transnational Crime in Uncharted Waters'* Interdisciplinary Political Studies Volume 2, No. 1 Special Issue (March 2012) 48-58.

Volker Erb *'Überlegungen zu einer Neuordnung der Konkurrenzen'* Zeitschrift für die gesamte Strafwissenschaft, Volume 117, Issue 2 (2005), 37ff.

William W Burke-White *'Regionalisation of International Criminal Lan Enforcement: A Preliminary Exploration'* Texas International Law Journal, Volume 38 (2003) 729 ff.

Xavier Philippe *'The principles of universal jurisdiction and complementarity'* International Review of the Red Cross 88, 862 (June 2006).

Xingan Li 'A review of Motivations of Illegal Cyber Activities' Kriminologija & Socijalna Integracija, Volume 25, Issue 1 (February 2017), 110-126.

7. Papers and Guidelines

Adeniyi Adejimi Osinowo *'Combating Piracy in the Gulf of Guinea'* (15 February 2015).

Advanced Autonomous Waterborne Application Initiative *'Remote and Autonomous Ships - The next steps'* (2016).

Angela Nelson '*The legal Obligations of Ship Masters and Seaplane Pilots'* (February 2003).

Baltic and International Maritime Council *'Guidelines on Cyber Security Onboard Ships – Version 3'* (2018).

Hui-Min Huang *'Autonomy Levels for Unmanned Systems (ALFUS) Framework Volume I; Terminology Version 2.0'* (October 2008).

International Organisation for Standardisation and the International Electrotechnical Commission *'ISO/IEC 27001 Information Security Management Standards on Information technology – Security techniques – Information security management systems – Requirements'* (June 2017).

International Maritime Organization *'Circular letter No. 3180 – Circular letter concerning information and guidance on elements of international law relating to piracy'* (17 May 2011)

Internationaler Seegerichtshof *'Der internationale Seegerichtshof'* (2016).

Maritime Unmanned Navigation through Intelligence in Networks *'Research in maritime autonomous systems project results and technology potentials'* (2019).

Michael Scharf '*The ICC's Jurisdiction over the Nationals of Non-Party States: A Critique of the U.S. Position'* (2001).

Norwegian Forum for Autonomous Ships '*Definition for Autonomous Merchant Ships* (10 October 2017).

Peter Beaumont and Stephen Wolthusen *'Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts'* ISG MSc Information Security thesis series (2017).

Robert Rylander and Yemao Man *'Autonomous safety in vessels - an international overview and trends within the transport sector'* (2016) *Lighthouse Reports* 37.

Shipbuilding, Machinery and Marine Technology (SMM) *'SMM insights 2017'* (2017).

United Nations Conference on Trade and Development *'Maritime Policy - Part II - An Overview of the International Legal Framework and of Multilateral Cooperation to Combat Piracy - Studies in Transport Law and Policy - 2014 no. 2'* (2014).

Ulrich Sieber *'Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission'* (1998).

9. Thesis

Anete Logina *'The international law related to maritime security: an analysis of its effectiveness in combating piracy and armed robbery against ships'* (2009).

Elizabeth Nyman '*Modern Piracy and International Law: Definitional Issues with the Law of the Sea;* (November 2011).

Kalu Anele *'The Viability of Establishing an International Tribunal for maritime piracy'*.

Jan van Hauwaert *'The importance of the SUA Convention in the fight against violence at sea'* (2018).

Jenna Ahokas *'The Finnish Maritime Sector Inside the Cybersecurity Hurricane'* (11 November 2018).

Marcus Toremar *'The legal position of the ship master'* (2000).

Tom Forster *'The Unmanned Ship Sets Sail - Is South Africa Prepared to Open the Ship Register?'* (2017).

Vishal Surbun *'Piracy Jure Gentium in Territorial Seas: A Perspective from the East African Seaboard'* (2017).

10. Books

August Bequai *'White-Collar Crime: A 20th Century Crisis'* (1978).

Anthony M. Townsend *'Ghost Road - Beyond the Driverless Car'* (2020).

Barry Turner '*The Statesman's Yearbook'* (2011).

Benedicte Sage-Fuller *'The Precautionary Principle in Marine Environmental Law: With Special Reference to High Risk Vessels'* (2013).

Bernd Heinrich *'Strafrecht – Allgemeiner Teil'* (2019).

Carlos G. Soares *'Progress in Maritime Technology and Engineering'* (2018).

Claus Roxin, Gunther Arzt and Klaus Tiedermann *'Einfühung in das Strafrecht und Strafprozessrecht'* (2006).

Cristian Gerlach *'Die Seesicherheitsuntersuchung - Die Untersuchung von Seeunfällen und die Einziehung von Berechtigungen nach dem Seesicherheitsuntersuchungsgesetz'* (2005).

David Hambling '*WE ROBOT: The robots that already rule our world'* (2016).

David Hamilton *'Technology, Mn and the Environment'* (1973).

Diethelm Kienapfel *'Strafrecht, Allgemeiner Teil: Mit Einführung in programmierter Form' (*2015).

Donn B. Parker *'Computer Crime: Criminal Justice Resources Manual'* (1989).

Donald R Rothwell and Tim Stephens *'The International Law of the Sea'* (2010).

Hans-Heiner Kühne *'Strafprozessrecht - Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts'* (2015).

Hans-Jürgen Schaps *'Das deutsche Seerecht, Kommentar und Materialsammlung'* (2019).

Huadong Guo *'Manual of Digital Earth'* (2020).

Irini Vassilaki and Silke Martens *'Computer und Internet-Strafrecht'* (2003).

Johann Waak '*Pirateriebekämpfung durch deutsche staatliche Stellen – Zu den Befugnissen der deutschen Marine, der deutschen Polizei und des Bundesnachrichtendienstes'* (2018).

Jeff Kosseff *'Cybersecurity Law'* (2019).

Katie Hafner and Matthew Loyn *'Where Wizards Stay up Late: The Origins of the Internet'* (1998).

Klaus Malek and Andreas Popp *'Strafsachen im Internet'* (2015).

Kevin Desmond *'Electric Boats and Ships – A History'* (2017).

Marco Gercke *'Understanding Cybercrime: Phenomena, Challenges and Legal Response'* (September 2012).

Thomas Fischer *'Strafgesetzbuch und Nebengesetze'* (2020).

Vincent Mosco *'The Digital Sublime: Myth, Power, and Cyberspace'* (2005).

11. Governmental Publication

Bundesministerium des Inneren *'Referentenentwurf – Erste Verordnung zur Änderung der BSI-Kritisverordnung'* (23 February 2017).

Deutsche Bundesregierung Inneres und Heimat '*Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Gridorios Aggelidis, Renata Alt, weitere Abgeordnete und der Fraktion der FDP – Drucksache 19/7321'* (19 February 2019).

Deutscher Bundestag Wissenschaftliche Dienste *'Zur Bekämpfung von Piraterie – Völkerrecht, Staatsrecht, Strafrecht'* (29 June 2009).

USA Congressional Research Service *'Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress'* (30 March 2020).

USA National Research Council, Division on Engineering and Physical Sciences, Naval Studies Board, Committee on Autonomous Vehicles in Support of Naval Operations *'Autonomous Vehicles in Support of Nava Operations'* (2005).

12. Online Publications

Ajay Menon *'Bridge of a Ship - Design And Layout'* Naval Architectures (May 2020) available *at https://www. marineinsight.com/naval-architecture/bridge-of-a-ship-design-and-layout/*, accessed on 21 January 2021.

'Antwerp incident highlights maritime IT security risk' (21 October 2013) *Seatrade Maritime News* available at *https://www.seatrade-maritime.com/news/europe/antwerp-incident-highlights-maritime-it-security-risk/*, accessed on 21 January 2021.

'Austal falls victim to cyber-attack' (2 November 2018) available at *https://worldmaritimenews.com/archives/263840/austal-falls-victim-to-cyber-attack/*, accessed on 21 January 2021.

Boeing *'Echo Voyager Overview'* available at *https://www.boeing.com/defense/autonomous-systems/echo-voyager/index.page*, accessed on 21 January 2021.

Bundesamt für Sicherheit der Informationstechnik *'Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz-BSIG)'* available at *https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html*, accessed on 21 January 2021.

Bundeskriminalamt *'Cybercrime'* available at *https://www.bka.de/DE/Karriere-Beruf/ArbeitenBeimBKA/Einblicke/Cybercrime/cybercrime_node.html*, accessed on 30 May 2020.

Chris Baraniuk *'How hackers are targeting the shipping industry'* (18 August 2017) *BBC News* available at *https://www.bbc.com/news/technology-40685821*, accessed on 21 January 2021.

'Clarksons Falls Victim to Cyber Security Breach' (29 November 2017) available at *https://worldmaritimenews.com/archives/236548/clarksons-falls-victim-to-cyber-security-breach/*, accessed on 21 January 2021.

'COSCO Shipping Lines Falls Victim to Cyber Attack' (25 July 2018) available at *https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/*, accessed on 21 January 2021.

'COSCO Shipping Lines back to Normal after Cyber Attack' (30 July 2018) available at *https://worldmaritimenews.com/archives/257916/cosco-shipping-lines-back-to-normal-after-cyber-attack/*, accessed on 21 January 2021.

Daniel Herder *'Erster Piraten-Prozess in der Hansestadt seit 400 Jahren'* (05 June 2010) *Hamburger Abendblatt* available at *https://www.abendblatt.de/hamburg/article108540468/Erster-Piraten-Prozess-in-der-Hansestadt-seit-400-Jahren.html*, accessed on 21 January 2021.

Edward Robertson *'MSC Melody attacked by pirates'* (27 April 2009) *Travel Weekly* available at *http://www.travelweekly.co.uk/articles/30833/msc-melody-attacked-by-pirates*, accessed on 30 May 2020.

International Maritime Organisation *'IMO Takes First Steps to Address Autonomous Ships'* available at *https://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx*, accessed on 21 January 2021.

International Maritime Organisation *'Cyber Security'* available at *http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx*, accessed on 21 January 2021.

International Maritime Organisation *'ISM Code and Guidelines on Implementation of the ISM Code'* available at *http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx*, accessed 30 May 2020.

International Maritime Organisation *'Maritime cyber risk'* available at *http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cybersecurity.aspx*, accessed on 30 May 2020.

International Organization for Standardization and the International Electrotechnical Commission *'ISO/IEC 27001 Information Security Management'* available at *https://www.iso.org/isoiec-27001-information-security.html*, accessed 30 May 2020.

'In Depth: Unmanned Ships - Are We There Yet?' (14 March 2018) available at https*://worldmaritimenews.com/archives/247204/interview-unmanned-ships-are-we-there-yet/*, accessed on 30 May 2020.

Jordan Novet *'Shipping company Maersk says June cyberattack could cost it up to $300 million'* (16 August 2017) *CNBC* available at *https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html*, accessed on 21 January 2021.

Jill Leovy '*Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks'* (17 August 2017) *Los Angeles Times* available at *https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html*, accessed on 30 May 2020.

Lee Mathews *'NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million'* (16 August 2017) *Forbes* available at *https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#72efd764f9ae*, accessed on 21 January 2021.

Mike Schuler *'Rolls-Royce Reveals Vision of Shore-Control Centres for Unmanned Cargo Ships'* (22 March 2016) *gCaptain* available at *https://gcaptain.com/rolls-royce-reveals-details-on-shore-based-control-rooms-for-operation-of-unmanned-cargo-ships/*, accessed on 21 January 2021.

Mike Schuler *'Clarkson Plc Reveals Details of 2017 Cyber Security Incident'* (31 July 2018) *gCaptain* available at *https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/*, accessed on 21 January 2021.

Maritime Unmanned Navigation through Intelligence in Networks *'The MUNIN Consortium'* (2016) available at *http://www.unmanned-ship.org/munin/partner/*, accessed on 21 January 2021.

'Norway Provides Grant for Construction of Yara Birkeland' (29 September 2017) available at *https://worldmaritimenews.com/archives/231229/norway-provides-grant-for-construction-of-yara-birkeland/*, accessed on 21 January 2021.

Oberlandesgericht Hamburg *'Poolführung im Strafverfahren gegen 10 Somalier wegen Angriffs auf den Seeverkehr und erpresserischen Menschenraubs'* Official press release (19 November 2019) available at *https://justiz.hamburg.de/pressemitteilungen/2639402/pressemeldung-2010-11-19/*, accessed on 21 January 2021.

Oberlandesgericht Hamburg *'Landgericht Hamburg entscheidet über Eröffnung des Hauptverfahrens gegen zehn somalische Angeklagte – Verhandlungsbeginn am 22. November 2010'* Official press release (29 October 2010) available at *https://justiz.hamburg.de/pressemitteilungen/2601882/pressemeldung-2010-10-29/*, accessed on 21 January 2021.

ONE SEA '*Test Area'* (2017) available at *https://www.oneseaecosystem.net/test-area/*, accessed on 21 January 2021.

ONE SEA '*Roadmap'* (2017) available at *https://www.oneseaecosystem.net/roadmap/*, accessed on 21 January 2021.

ONE SEA '*Advisory Board'* (2017) available *at https://www.oneseaecosystem.net/about/advisory-board/*, accessed on 21 January 2021.

'Pirates Attack Cruise Ship' (5 November 2005) *CBS NEWS* available at *https://www.cbsnews.com/news/pirates-attack-cruise-ship*/, accessed on 30 May 2020.

Stadt Nürnberg *'Echtes Pionierstück: Nürnbergs automatische U-Bahn'* available at *https://www.nuernberg.de/internet/digitales_nuernberg/automatische_ubahn_nuernberg.html*, accessed on 21 January 2021.

Vincent Wee *'Naval Dome exposes vessel vulnerabilities to cyber-attack'* (22 December 2017) *Seatrade Maritime News* available at *https://www.seatrade-maritime.com/news/asia/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack/*, accessed on 21 January 2021.

Waymo LLC *'Our Journey'* available at *https://waymo.com/journey*/, accessed on 21 January 2021.

Yara '*Yara selects Norwegian shipbuilder VARD for zero-emission vessel Yara Birkeland'* available at *https://www.yara.com/corporate-releases/yara-selects-norwegian-shipbuilder-vard-for-zero-emission-vessel-yara-birkeland/*, accessed on 21 January 2021.

'Yara Birkeland Autonomous Container Vessel' available at *https://www.ship-technology.com/projects/yara-birkeland-autonomous-container-vessel/*, accessed on 21 January 2021.

13. Encyclopaedias and dictionaries

Bryan Garner and Henry Black 'Black's Law Dictionary' (2004).

Catherine Soanes *'Paperback Oxford English Dictionary'* (2006).

Online Etymology Dictionary *'pirate'* available at *https://www.etymonline.com/search?q=Pirate*, accessed on 21 January 2021.

Online Etymology Dictionary *'cybernetics'* available at *https://www.etymonline.com/word/cybernetics*, accessed on 21 January 2021.

'International Criminal Jurisdiction, Protective Principle' (July 2007).

UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

Mrs Emily Simon (219095768)
School Of Law
Howard College

Dear Mrs Emily Simon,

Protocol reference number: 00004536
Project title: Unmanned and autonomous Container Ships and Cyber Piracy: An Analysis of international and national regulatory measures

Exemption from Ethics Review

In response to your application received on 22 October 2019, your school has indicated that the protocol has been granted **EXEMPTION FROM ETHICS REVIEW.**

Any alteration/s to the exempted research protocol, e.g., Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through an amendment/modification prior to its implementation. The original exemption number must be cited.

For any changes that could result in potential risk, an ethics application including the proposed amendments must be submitted to the relevant UKZN Research Ethics Committee. The original exemption number must be cited.

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.

I take this opportunity of wishing you everything of the best with your study.

Yours sincerely,

[redacted]

Mr Simphiwe Peaceful Phungula
Academic Leader Research
School Of Law