UNIVERSITY OF THE PELOPONNESE
SCHOOL OF SOCIAL AND POLITICAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCES & INTERNATIONAL RELATIONS

Master of Arts in
“Global Risks and Analytics”

“Assessing Terrorist Cyber-Risks and the Potential Use of Terrorist Cyber-Threats in the Maritime Sector.”

Master’s Dissertation

Georgios **Gkousgkounis**

Defense Committee:

Assistant Professor, Efstathios Fakiolas
Assistant Professor, Ioannis Konstantopoulos
Associate Professor, Nikitas Koutsoukis

Final Version

Corinth, 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ

Πρόγραμμα μεταπτυχιακών Σπουδών
«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

«Αξιολόγηση Τρομοκρατικών Κυβερνό-κινδύνων και η εν Δυνάμει Χρήση Τρομοκρατικών Κυβερνο-απειλών στη Ναυτιλία.»

Μεταπτυχιακή Διπλωματική Εργασία

Γεώργιος **Γκουσγκούνης**

Τριμελής Επιτροπή:

Επίκουρος Καθηγητής, Ευστάθιος Φακιολάς
Επίκουρος Καθηγητής, Ιωάννης Κωνσταντόπουλος
Αναπληρωτής Καθηγητής, Νικήτας Κουτσούκης

Τελική Έκδοση

Κόρινθος, 2016

Φύλλο αξιολόγησης

Η διπλωματική εργασία με τίτλο «*Assessing Terrorist Cyber-Risks and the Potential Use of Terrorist Cyber-Threats in the Maritime Sector*» του Γεώργιου Γκουσγκούνη, αξιολογήθηκε από την τριμελή επιτροπή, τόσο ως προς την ποιότητα του κειμένου, όσο και ως προς την ποιότητα της προφορικής παρουσίασης και υπεράσπισης της διπλωματικής εργασίας ενώπιον ακροατηρίου.

Η διαδικασία αξιολόγησης της διπλωματικής εργασίας ολοκληρώθηκε την ………/………/……… με γενική επίδοση:

□ Καλώς

□ Λίαν Καλώς

□ Άριστα

Τα μέλη της τριμελούς επιτροπής:

1. Επίκουρος Καθηγητής, Ε. Φακιολάς
2. Επίκουρος Καθηγητής, Ι. Κωνσταντόπουλος
3. Αναπληρωτής Καθηγητής, Ν. Κουτσούκης

«Αξιολόγηση Τρομοκρατικών Κυβερνό-κινδύνων και η εν Δυνάμει Χρήση Τρομοκρατικών Κυβερνο-απειλών στη Ναυτιλία.»

Λέξεις Κλειδιά: Τρομοκρατία, Ναυτιλία, Πειρατεία, Ανάλυση Κινδύνου, Κυβερνο-Απειλές, Κυβερνό-κίνδυνοι

Περίληψη

Η 11η Σεπτεμβρίου 2001, έκανε εμφανές ότι οι τρομοκράτες έχουν την ικανότητα να χρησιμοποιήσουν μη συμβατικά μέσα προκειμένουν να πραγματοποιήσουν τις επιθέσεις τους. Η στρατηγική των τρομοκρατών άρχισε να αλλάζει και να στρέφεται προς οικονομικούς στόχους, ενώ ταυτόχρονα αποδείχτηκε ότι τα συνήθη μέσα μεταφοράς μπορούν να μεταμορφωθούν σε φονικά όπλα. Έπειτα από την 11η Σεπτεμβρίου 2001, έχουν αυξηθεί οι ανησυχίες στο ναυτιλιακό τομέα όσον αφορά στην πιθανότητα τρομοκρατικών πράξεων εναντίον πλοίων και λιμενικών εγκαταστάσεων με τη χρησιμοποίηση πλοίων ως όπλων σχεδόν με τον ίδιο τρόπο που τα αεροπλάνα χρησιμοποιήθηκαν ως όπλα. Υπήρξαν φόβοι ότι οι τρομοκράτες είναι πιθανό να χρησιμοποιήσουν τακτικές που χρησιμοποιούν οι πειρατές στη θάλασσα προκειμένου να εκτοξεύσουν επιτυχημένες επιθέσεις στη θάλασσα. Παρόλα αυτά, το να πραγματοποιήσει κάποιος επιθέσεις σε θαλάσσιο περιβάλλον παρουσιάζει πολλά προβλήματα. Για το λόγο αυτό, οι κύριες ανησυχίες των άμεσα ενδιαφερόμενων, έπειτα, στράφηκαν σε μια πιθανή τακτική συνεργασία μεταξύ πειρατείας και τρομοκρατίας. Ωστόσο, δεν υπάρχει κανένα στοιχείο που να καταδεικνύει την ύπαρξη μιας τέτοιας συμμαχίας ή τη μελλοντική της ύπαρξη, λόγω του γεγονότος ότι υπάρχει μια λεπτή διαχωριστική γραμμή μεταξύ τους. Συνεπώς, οι τρομοκράτες προσπαθούν να αναβαθμίσουν τις μεθόδους τους έτσι ώστε να πετύχουν τους στόχους τους ξεπερνώντας τα εμπόδια του θαλάσσιου περιβάλλοντος. Για αυτό το λόγο, οι τρομοκράτες προσαρμόζουν τις τακτικές τους, τον τρόπο λειτουργίας τους, ακόμα και τα οπλικά τους συστήματα και εκμεταλλεύονται την εξάρτηση του εμπορίου και των επικοινωνιών στα ηλεκτρονικά μέσα ούτως ώστε να εκπληρώσουν τις προσπάθειές τους. Πρόσφατα καταγεγραμμένες υποθέσεις επιτυχημένων κυβερνο-επιθέσεων απαιτούν την πλήρη προσοχή του τομέα της ναυτιλίας. Σκοπός της διπλωματικής εργασίας είναι να αναγνωρίσει τα κύρια προβλήματα στο ναυτιλιακό τομέα, να περιγράψει τις μεθόδους που χρησιμοποιούν οι τρομοκράτες για τους σκοπούς τους και να εκτελέσει μια ανάλυση κινδύνου χαρτογραφόντας τα δυνατά σενάρια απειλών που αφορούν κυβερνο-επιθέσεις σε πλοία και κρίσιμες ναυτιλιακές υποδομές.

Assessing Terrorist Cyber-Risks and the Potential Use of Terrorist Cyber-Threats in the Maritime Sector.

Keywords: Maritime Terrorism, Piracy, Cyber Threat, Risk Analysis

Abstract

September 11, 2001, made clear that terrorists have the ability to use unconventional means for their attacks. Terrorists' strategy started shifting towards economic targets and proved that ordinary means of transportation can be transformed into lethal weapons. Since September 11, 2001 worries have arisen within the maritime sector about the possibility for terrorist actions against ships, and port facilities by terrorists using ships as weapons approximately in the same way as airplanes were used as weapons. There have been fears that the terrorists might make use of piracy sea tactics to achieve successful attacks at sea. However, delivering attacks in the maritime environment presents many problems. The main worries for all the stakeholders then shifted to a potential tactical nexus between piracy and terrorism. Nevertheless, there is no evidence that pirates and terrorists have a collusion or that they will because there exists a very thin line between them. Consequently, terrorists are trying to advance their methods in order to achieve their goals by overcoming these barriers. Therefore, terrorists adjust their tactics, modus operandi and sometimes even their weapon systems and exploit the dependence of commerce and communication on electronic means so as to accomplish their efforts. Recent recorded cases of successful cyber-attacks require the sector's full attention. The aim of this dissertation is to identify the main problems in the maritime sector, describe the methods that terrorists use for their purposes and perform a risk analysis to map out potential threat scenarios that involve cyber-attacks to ships and critical maritime infrastructures.

Assessing Terrorist Cyber-Risks and the Potential Use of Terrorist Cyber-Threats in the Maritime Sector.

Preface

As behind every dissertation there is supervisor, my greatest regards go to Professor Eustathio Fakiola for his unfailing support throughout this process. Without his encouragement and belief in my topic, I would not have even pursuing this research. He has been a great adviser, always available to talk with me and share worthwhile ideas and comments, yet allowing me to work independently.

I must also acknowledge the support and help of my very good friends and colleagues, Michalis Michaletos and Grigoris Devetzis. Michalis and Grigoris, you and I began this journey together. Life has a way of bringing the right people together, at the right time, for the right reasons. I am so honored and truly grateful for your positive words of encouragement. You have been and will continue to be my true buddies and partners in the learning process and in life too.

Next, I would like to thank my friend and colleague Babis Theologis. Without his help the whole Master and especially the dissertation would be a catastrophe. He was there whenever I needed him and available to be in my place in order not to lose my classes. At least he traveled throughout Greece. I owe you my friend.

Finally, I would like to thank my family. So, mum, dad, Christina and Tasos a big part of this Master definitely belongs to you. Without your daily support this effort would not have been flourished.

List of Tables

List of Figures

List of Diagrams

Contents

1. Introduction

1.1 Background of the Problem

The years before 2001, when someone was talking about terrorism, referred to a rather traditionally concept of terrorism and terrorist attacks. Methods like car bombs, hijack events and political assassinations were the major terrorist forms of attacks until then. After 2001, new threats and scenarios came to the surface since items such as airplanes, trains or vessels could easily be turned against countries and people, as new, unrealized forms of terrorist attacks (Nincic, 2005, pp. 619-620). The atrocious 11 September attacks in New York and Washington, forced governments around the world to reconsider their vulnerabilities against terrorism and especially against these terrorist groups ready to sacrifice thousands of innocent lives in order to reach their goals. At first, and given the particular features of these air strikes, the initial attention was on the air transport system and its vulnerabilities. Afterward, since the maritime environment presents a unique opportunity for such kind of attacks, the focus turned to the vulnerabilities of the maritime domain (Raymond, 2006, p. 239).

Immediately after 11 September's attacks, in response to these catastrophic events, the international community identified the necessity of protecting the maritime transport sector against terrorism. IMO (International Maritime Organization) developed new requirements, after consultations with governments, government agencies, local administrations and shipping and port industries. On 1 July 2004 a new maritime security regulatory regime was adopted into the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, including the International Ship and Port Facility Security (ISPS) Code. The ISPS Code included detailed security requisites for port authorities, shipping organizations and governments, and meticulous instructions about how to meet these requisites (IMO, 2016).

Obviously, since the 11 September attacks the security has become tighter. Terrorists' operational field on land has been limited, which in turn has made the maritime sector more attractive for high profile attacks. Indeed, terrorists are able to recognize the importance of the maritime domain and to diagnose the vulnerabilities of maritime infrastructure which in conjunction with the fact that the maritime environment is a large unregulated area make the maritime domain an appealing target. In addition, the 11 September attacks indicated that ordinary means of transportation can be turned into lethal weapons of terror (Raymond, 2006, p. 241). That is why many analysts examine the possibility of a major terrorism event taking place at sea.

Due to the fact that maritime terrorism, as opposed to other violent illegal activities in the marine environment, has emerged recently and it concerns only the states in which it originates because of civil wars or wars of succession, the international naval community is still roughly unfamiliar with this threat (Raymond, 2006, p. 240).

According to the RAND Corporation's Terrorism Chronology Database and the RAND-MIPT Terrorism Incident Database, over the last three decades, maritime terrorism attacks has hardly surpassed 2% of all international terrorist events (Chalk, 2006, p. 21). However, some crucial maritime episodes have focused attention on terrorists' maritime capabilities and on what they can achieve at sea. Such major assaults are for example al-Qaeda's attacks on USS *Cole* warship in Aden harbor in 2000, on the oil tanker MV *Limburg* off Yemen in 2002 and the bombing of the "*SuperFerry 14*" passenger ferry in Manila by Philippine Islamist separatists in 2004. The consequences of this kind of assaults can be very serious, even if the probability to occur remains quite low (Murphy, 2007, p 7).

Furthermore, in those places where piracy is prevalent, deliberate or unwitting cooperation between piracy and terrorism can camouflage the preparations for terror assaults to look like ordinary piracy incidents. In this context terrorists might be able to undermine the world's seaborne trade in energy, raw materials and manufactured goods (Murphy, 2007, p. 7). Taking account of all the above, of the proliferation of nuclear technology and nuclear-WMD weapons and in combination with the terrorists' ability to move without restrictions at sea, establish an enormous threat among the interconnected industrial economies. The following quote from a jihadist website along with what was said above making it essential to develop and maintain response strategies: "*It becomes necessary to develop the battle to include the sea, and as the Mujahidin have managed to form martyr brigades on the ground, the sea remains the next strategic step toward ruling the world and restoring the Islamic Caliphate*". (Agnihotri, 2012, p. 19)

On the one hand, governments have taken countermeasures to discover and eradicate terrorist groups and additionally have designed adequate defenses and security barriers to prevent attacks. On the other hand, terrorists try to continually advance their methods in order to survive and succeed by overcoming the governmental defenses and barriers. Therefore, it is critical for the terrorists to be one step ahead of the counterterrorism, adjust their tactics, modus operandi and sometimes even their weapon systems (Hoffman, 1998). Is more than certain that there would be some sophisticated terrorist groups which will find a way to accomplish their efforts.

Given the above, the erosion of the conventional form of terrorism is imminent. The new generation of terrorists cannot absorb the methods and the assault techniques as it has been known, into training camps. Virtual attacks, involving anonymous cyber assaults are becoming increasingly appealing, especially nowadays as our society becomes more and more dependent on electronic means of commerce and communication (Hoffman, 2002, p. 313).

We have now moved into the Information Age which has brought huge benefits but also has introduced new problems, such as our dependence on computer systems that raises the threat of being hacked (Hansen & Rahman, 2014, p. 2). As technology continues to develop, maritime activity started to increasingly relies on information technology (IT) and ICT systems, taking solutions that offer high functionality in order to optimize maritime operations. From navigation to propulsion and from freight management to traffic control communications, information technology (IT), operational technology (OT) and ICT systems are increasingly used to enable essential maritime operations by being networked together and more frequently being connected to the worldwide web (ENISA, 2011, pp. 1-3).

The maritime domain is not impervious to the capacity of modern digital communications and computing to be disruptive (Fitton, Prince, Lacy, & Germond, 2015, p. 1). Many services supported by ICT systems (databases or systems hosting sensitive information), may be affected by the vulnerabilities created by the security gaps in these systems while increasing use of new, advanced communications technologies increases the threat level. Both cargo tracking and identification are increasingly exposed to cyber-security incidents resulting from cyber-attacks or systems failures (XL Group, 2013, pp. 5-6).

Furthermore, the sustainable use of the internet brings the major risk of unauthorized access or malicious attacks to ships' systems and networks. Not to mention risks also occur from personnel having access to the systems onboard (installing malware via removable media etc.) (BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO, 2016, p. 1).

Inadequate cyber-security is rather a new threat compared with traditional risks. Notwithstanding, cyber-threats are considering to be a huge subject for the shipping industry as concern as the future, since it is not improbable that a cyber-attack could result in a disaster. In 2011 the European Network and Information Security Agency (ENISA) released a report titled "Analysis of Cyber Security Aspects in the Maritime Sector", realized that "the awareness on cyber-security needs and challenges in the maritime sector is currently low to non-existent" (p. 1), but little if any improvement made since then. Maritime environment is considered vulnerable to cyber-attacks and the cyber-threats from hackers are intensified as crews becoming smaller, vessels becoming larger and larger and more dependable on automation (Allianz, 2015, p. 30).

Consequently, cyber-security in the maritime industry is a major issue, due to a lack of security awareness or accountability. In order to gain the advantages of modern technology those operating in the maritime sector must also become aware and cultivate strategies to handle the unavoidable security subjects that modern computing systems bring with them (Fitton, Prince, Lacy, & Germond, 2015, pp. 1-3). With the potential for sensitive customer data leaks via systems like ECDIS, AIS, RFID and GPS, it is important that security procedures and processes are available so that operators know how to identify a possible security threat or have been skilled to respond when a cyber-attack is in process (ESC, 2015, p. 5). Related personnel should have training in distinguishing the typical modus operandi of cyber-attacks too (BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO, 2016, p. 1). Recent cyber-risk incidents such as in 2011 when drug smugglers gained remote access to Port of Antwerp's terminal systems, in 2012 when a criminal syndicate penetrated cargo systems operated by Australian Customs and Border Protection or in 2013 when the World Fuel Services fell victim to an online bunkering scam with estimated loss almost $18m, demonstrate a clear frame of action. The perpetrators active in the maritime domain and in particular maritime pirates, are mostly interested in financial gain, attending to gain access and extract financial profit from their targets (ESC, 2015, p. 5). However, maritime terrorism refers to "any illegal act directed against ships, their passengers, cargo or crew, or against sea ports with the intent of directly or indirectly influencing a government of group of individuals" (Menefee, 1986). Therefore, accessing and extracting sensitive information or intellectual property can also help pirates or terrorist groups whose incentive is to use the sector to benefit from it. Thus it is imperative the need for these risks to be carefully assessed, measured and analyzed (ESC, 2015).

1.2 Scope and Significance of the Study

This study seeks to investigate the extent of the threat posed by maritime terrorism either to vessels and shipping or to commercial and passengers' ports or even rigs. After we discuss about maritime terrorism and the distinction that exists between piracy and maritime terrorism, we shall focus, in particular, on the threat from the terrorist groups that use cyber vulnerabilities of the maritime sector in order to achieve their goals. It tries to identify the inherent weaknesses present in the maritime transport industry concerning cyber security and assess terrorist cyber-risks and the potential use of terrorist cyber-threats in the maritime sector. This will help us achieve a holistic view of key cyber-security challenges in the maritime domain, including the main ICT risks. (See about Maritime Piracy in Appendix A)

There is a huge gap in maritime cyber-security for the following reasons. At first, there are quite a few verified incidents-attacks that have taken place so far. Secondly, as maritime cyber-security awareness is at present time low, to non-existent and due to the high ICT complexity, it is primary challenge to ensure sufficient maritime cyber-security. Also, it is a fact that all the current maritime regulations and policies do not consider cyber-security aspects of security and safety but only physical aspects of them, or there is no regulatory pressure to report cyber-incidents yet. Moreover, the professionals in the maritime domain are not sufficiently aware of potential damage from cyber-threats.

Most of cyber-experts are not totally understand maritime cyber-threats because they have little experience in maritime domain as most of them are not experts at all as concern as maritime, hence they need to deduce from their experience in other domains and there is a need to learn by engaging with maritime professionals.

This study will be the first of its kind in Greece, as a risk-based approach and an assessment of maritime specific terrorist cyber-risks while simultaneously will identify the potential use of terrorist cyber-threats in the maritime sector as well as of all critical assets within this sector. This might help in the future both states and maritime companies to undertake targeted maritime sector awareness, raising campaigns and cyber-security training of shipping companies, port authorities, national cyber-security offices, etc.

1.3 Method and Limitations of the Study

In order to conduct this research, we used a qualitative approach which means that we gathered data in order to identify reasons, tendencies and deeper motives. Secondary data collected by current bibliography are used for a "sense making" analysis or understanding a phenomenon, rather than predicting or explaining. A creative and investigative mindset is needed for qualitative analysis, based on an ethically enlightened and participant-in-context attitude, and a set of analytic strategies. At the end a risk framework for analysis was used to analyze the individual threats and risks from terrorist groups. Risk analysis can be divided in two key components, risk assessment, and risk management. Kaplan and Garrick (1981), posed three fundamental questions that constitute the risk assessment process. The first was "What can go wrong?", the second was "What is the likelihood?" and the last one "What are the consequences?". To answer these questions, we have chosen a part of the Risk Filtering, Ranking, and Management method (RFRM) developed by Haimes, Kaplan, and Lambert (2002).

Unfortunately, the maritime theater characterized by opacity and the transparency is quite low. Many cyber events in the maritime industry had remained undetected or under-reported and also businesses that have potentially fallen victim to cyber-attacks did not want to reveal them in public as companies may fear appearing to have allowed confidential information to be compromised. All the above in combination with the fact that the writer is not an expert as concern as maritime domain introduce some limitations to the current study.

2 Maritime Terrorism

This chapter evaluates the potential threats of maritime terrorism. We begin by giving some definitions about maritime terrorism, citing a series of major maritime terrorist events, discussing the significance of the after 9/11 era for maritime terrorism and listing the potential methods and different uses of the vessels as weapons for the terrorist groups. We then briefly analyzing the factors underscoring the current concern and the reasons that might motivate terrorists to undertake operations in a marine environment. Afterwards, we examine the main problems experienced by terrorist organizations that have operated at sea and conclude why cyber threats constitute a major source of concern about the future of maritime terrorism. Finally, we discuss the link that connects piracy and maritime terrorism and also the distinction between them.

2.1 Definitions

In a comparison with piracy and other violent activities, maritime terrorism is a more recent and contemporary phenomenon (Raymond, 2006, p. 240). In recent decades, was observed a rapid increase in acts of terrorism on land. It seems certain that they would eventually be extended to the maritime theater. Maritime terrorism has emerged as a horrifying threat in the world, with a target group that includes both civilian and naval vessels (Hong & Ng, 2010, p. 3). Hence, the intelligence analysts, law enforcement officials, and policymakers progressively have increased their concerns in recent years about possibility of terrorist actors undertaking attacks in the maritime domain (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006, p. 9). However, there is an objective difficulty to define precisely maritime terrorism, and even the United Nations has not been able to provide the international community with an acceptable and binding definition for terrorism (Nelson, 2012, p. 16).

The US Department of Defence defines terrorism as “unlawful use or threatened use or force of violence against people or property to coerce or intimidate governments or societies, often to achieve political, religious or ideological objectives“ (US Department of Defence, 2010), while Ranstorp and Wilkinson describe terrorism as

> … the systematic use of coercive intimidation usually, though not exclusively, to service political ends. It is used to create and exploit a climate of fear among a wider group than the immediate victims of the violence, often to publicize a cause, as well as to coerce a target into acceding to terrorist aims (Ranstorp & Wilkinson, 2005, p. 1).

Maritime terrorism is nothing else but terrorism that eventuates at sea, on inland water as lakes, canals, rivers, watercourses, inlets, and bays, or against places that are in contact with water such as ports and coastal infrastructure (Murphy, 2008, p.185) The sea environment in just one of the many areas where terrorists undertake their attacks.

Herbert-Burns in an attempt to define maritime terrorism characterizes it as “the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change, in the maritime domain” (Herbert-Burns, 2004, p. 31).

As was said above the international community has not agreed to adopt an international definition. Utilizing Articles 3 and 4 of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), some legal scholars have made an attempt for an international definition. According to their definition maritime terrorism is any attempt or threat to seize control of a ship by force; to damage or destroy a ship or its cargo; to injure or kill a person on board a ship; or to endanger in any way the safe navigation of a ship that moves from the territorial waters of one State into those of another State or into international waters (Joubert, 2013, p. 113).

The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group, in February 2002, offered an extensive definition for the types of events that comprise maritime terrorism, as follows:

> the undertaking of terrorist acts and activities (1) within the maritime environment, (2) using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, (3) against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities (CSCAP, 2001, p. 15).

Despite the broadness of this definition, the maritime environment has not historically been a major domain of terrorist activity. According to the RAND Terrorism Database, over the last 30 years, seaborne strikes have constituted only 2% of all international maritime episodes. This definition does not clarify what exactly terrorism is, or what precisely type of maritime attacks does include, but under it there is plenty of room for many forms of potential attack scenarios.

For many years, it was common for many national authorities to characterize terrorist events in the maritime environment as piracy, even though these acts do not fulfill fundamental criteria to be characterized as that. The real reason behind this was that until then there was no specific international rule to handle terrorist attacks. So, in order to punish the attackers, they treated every episode as a case of piracy (Jesus, 2003, p. 387). Untill 1990, maritime terrorism has not yet been an international problem although piracy and armed robberies against ships. That explains partially, the absence of accurate international rules on terrorism. Therefore, maritime terrorism had not been the object of a well-established set of international rules, nor has it been a long-lasting and binding practice (Ronzitti, 1990). The internationally community decided to set some specific rules, appropriate for terrorism at sea, through the adoption of the 1988 SUA Convention, only after the serious terrorism incident, in 1985, to the passenger liner *Achille Lauro*. The SUA 1988 is the first international legal instrument on a specific legal regime covering sea terrorist acts (Hong & Ng, 2010, p. 4).

2.2 Major Events

The most prominent incident that for the vast majority first brought in the front maritime terrorism was the hijack of the cruise ship, the *Achille Lauro* by Palestinian terrorists, in the Mediterranean in 1985 and in particular in Egyptian territorial waters. Terrorists took over the ship and held hostages the crew and passengers. They demanded the freedom of a group of Palestinian prisoners from Israel or else they threatened with death the hostages. One hostage was shot and thrown into the sea. Terrorists secured a deal with Egypt in order to surrender the ship. Through US military intervention, which was not party to the deal the terrorists were captured by forcing the commercial jetliner carrying the hijackers to land in Italy (Bohn, 2004, pp. 1-20).

The next maritime terrorist attack that attracted much attention and publicity happened 15 years after the Achille Lauro, in October 2000 and it was a suicide attack on the USS Cole in Aden harbour, by al-Qaeda operatives, killing 17 people, another 39 were injured and nearly succeeded in sinking the warship. Two terrorists using a small dinghy full of explosives, penetrated the security of one of the most advanced warships in the world and came into direct contact with the American navy destroyer. Only two years later a French owned crude oil tanker called MV *Limburg* was hit by a small craft, in a similar way by al-Qaeda (Chalk, 2002, p. 10; Benjamin & Simon, 2003, p. 323-324).

Another high-profile terrorist attack and the deadliest one was against a Philippine ferry, the *SuperFerry 14*, in February 2004 which suffered a bombing attack and a huge explosion which in turn killed more than 100 people (63 immediately, 717 jumped into the sea and among them 53 died) (Raymond, 2006, p. 240; Murphy, 2007, p. 46).

Appendix B catalogs some of the higher-profile and publicized maritime terrorist incidents from 1961 to 2004, while Image 1 shows the global concentration and intensity of terrorist attacks from 1970 to 2015.

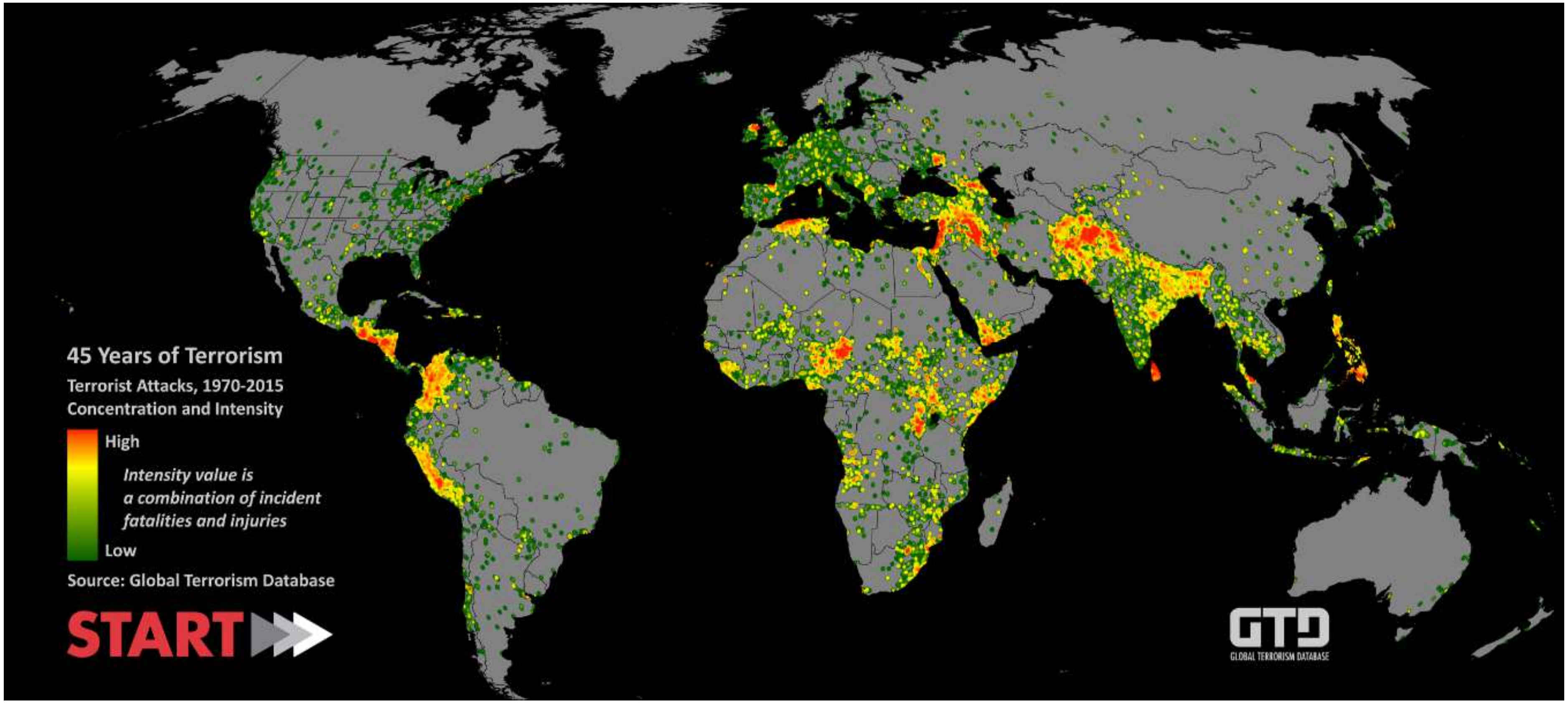

45 Years of Terrorism
Terrorist Attacks, 1970-2015
Concentration and Intensity
High
Intensity value is
a combination of incident
fatalities and injuries
Low
Source: Global Terrorism Database
START
GTD
GLOBAL TERRORISM DATABASE

Figure 1 Concentration and Intensity of Terrorist Attacks, 1970-2015 (Source: Global Terrorist Database)

2.3 The Significance of 11 September for Maritime Terrorism

In the aftermath of September 11, 2001 the world's perception of terrorism has changed significantly and new facts came to light. The enormous simultaneous suicide attacks on the Twin Towers, the Pentagon and a field in rural Pennsylvania was without precedent. Significant characteristics of the attack such as its sheer scale, its ambitious scope and dimensions, its impressive coordination and synchronization but also undeviating dedication and determination of the terrorists who voluntarily offered themselves to be killed, overshadow anything previously seen in terrorism (Hoffman, 2002, p.1-2; Raymond, 2006, p.241).

The terrorist attacks against the US demonstrated that the internationally community is liable to being attacked since terrorism is not limited just to one specific region of the world. The use of commercial airliners as their weapon of choice for high impact, catastrophic strikes, in order to deliver these barbarities made clear that terrorists have the ability to use unconventional means to take advantage of potential weakness in a state's security (Nelson, 2012, p. 20). The attacks revealed the potential fragility of the transportation systems, which could possibly lead to a breakdown of the global trade system (Ng & Gujar, 2008), made clear that terrorists' strategy started to alter towards economic targets and proved that ordinary means of transportation can be transformed into lethal weapons (Raymond, 2006, p. 241). The maritime realm is one area that rises serious concerns because its ungoverned, its ports and facilities are difficult to secure and is to a high degree open to attacks (Murphy, 2008, p.198). The advent of September 11, 2001 rose worries within the maritime domain concerning the possibility for terrorist actions against ships, port facilities by using ships as weapons approximately in the same way that airplanes were used as weapons (Hong & Ng, 2010, p. 1). Undoubtedly, terrorists successfully attacked the US when only two men using a small craft placed a shape charge against the hull of the USS Cole while refueling at a Yemini port, and succeed to kill 17 US service members and injuring 39 more (Murphy, 2008, 196).

2.4 Weapons and Tools

Even though September 11 grew our concerns, until now terrorists have ignored to exploit maritime targets. That should not be surprising considering that many terrorist organizations have neither been located near to coastal regions nor acquired the means needed to extend their physical reach beyond their territory. Even for those that did have a geographic proximity, there are several issues associated with executing sea strikes that have worked to offset some of the tactical advantages of the maritime environment (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006, p. 10).

Most people have in mind that ships can be attacked anywhere they sail. But most terrorists do not have the appropriate capabilities and are, therefore, unlikely to proceed to attacks on ships a long distance from the shore (Murphy, 2007, p.50). Terrorists who performing at sea are obligated to have mariner skills, access to appropriate assault and transport vehicles, the ability to carry out and sustain operations from a waterborne environment, and familiarity with certain specific abilities. Due to the fact that terrorists have limited resources, such options excluded from being available to most groups (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006, p. 10). Obviously, not many terrorists have both the tendency and the capabilities to attack at sea because delivering such attacks depends on a certain degree of familiarity with the sea

(Herbert - Burns, Bateman, & Lehr, 2009, p. 55). Within this limitation, however, there are a number of ways in which attacks may be launched:

Small boats: Small rigid-hulled recreational craft or inflatable boat, which are inexpensive, difficult to detect, highly maneuverable and often very fast or can accelerate rapidly. They form the most serious maritime terrorist threat because of the fact that are usually the equivalent of a car bomb or are armed with waterborne improvised explosive devices (IEDs) (Chalk, 2006, p.28; Murphy, 2007, p.50-51).

Naval mines: They can be placed quickly and secretly in large amounts but at the same time are time consuming and expensive to remove. They are unnoticeable and highly effective and can evoke extensive damages and perhaps if they be planted in a busy port they potentially imposing substantial costs. In addition, they could be supplement or alternative to IEDs and the upgrade of old and cheap mines can make them more effective, even enable them to select specific ship profiles (Truver, 2007; Murphy, 2007, p.52).

Divers and "human torpedoes": Terrorist use of divers first came to public attention by reports of revealed plans of terrorist groups. These reports were very rare and not reliable with most analysts having doubts or reservations about their extent. Some terrorist groups that initially use divers offensively failed because at the beginning they used normal open-circuit diving equipment and air bubbles gave them away. Therefore, they supplied their weaponry with "re-breather" kits that enabled divers to breathe using recirculated air (Apps, 2006). In addition, terrorist groups invested in acquiring swimmer delivery vehicles, small semi-submersible craft for guiding divers to their targets as "human-torpedoes" or "suicide-scooters" (Murphy, 2006, p.9; Murphy, 2007, p.52-53).

Submarines: A submarine introduce a greater threat in the weaponry of terrorists. More dangerous than a diver, due to the fact that skilled attackers can operate over a long way from their base, more accurate and with larger explosive cargo than a diver could ever accomplish, even if he had a swimmer delivery vehicle. However, terrorist groups do not have neither the capabilities to operate a submarine nor the resources to purchase one, unless they are state sponsored (Murphy, 2007, p.53). Criminal gangs, usually drug-smugglers, gave terrorist groups another option by building and operating simple submarines, confirming that it is well within the abilities of non-state actors (Sinai, 2004, p. 53).

Missiles: The general agreement until now has been that terrorist groups are not capable of buying, maintaining and operating such weapons as missiles and even more, states would not allow them to use such sophisticated weapon systems. But many attacks that were identified as missile hits make this issue controversial. While the consensus still broadly holds many insist that terrorist groups have everything or many of what a state has (Murphy, 2007, p.54).

Other weaponry: Except the above means that are used by terrorists as weapons, there are more weapons that are relatively cheap, widely available and do not demand specific capabilities. Such weapons are (1) anti-tank guided weapons, (2) rocket-propelled grenades (RPGs), (3) heavy machine guns, (4) mortars, (5) Katyusha-style rockets and (6) man-portable Air Defense Systems (MANPADS) (Murphy, 2007, p.54-55).

2.5 The Uses of Ships in Terrorism

If we see things from the terrorist operational perspective, these “impressive”, sheer scale, simultaneous attacks are comparatively uncommon (Hoffman, 2002, p.304). These successful assaults on US, could help us draw important elements, even though terrorists prefer far smaller scale operations and conventional means of attack, and then relocate these features to the maritime realm so as to see how they might be reproduced at sea.

The terrorists involved in 11 September, exploited the inherent characteristics of aircraft to turn them into controlled weapons without any form of modification. Both the Twin Towers and the Pentagon were iconic symbols of US. In addition, the Twin Towers were an economic target and when they were destroyed, imposed a serious cost on US economy. Moreover, they were a mass casualty target.

Having in mind these elements, the possibilities for terrorism at sea can be decomposed into four broad categories: (1) ships as iconic targets, (2) ships-offshore installations as economic targets, (3) ships as mass-casualty targets and (4) ships-other vehicles as weapons (Murphy, 2007, p.55).

Ships as iconic targets: Speaking about ships as iconic targets we mean ships that are important and symbolic to the state the attack is unleashed (Murphy, 2008, p.200). However, there are few if any cargo ships these days that are so closely linked to a state or to be representative of that state so as the attack on them would be seen as an assault on the flag state. Only naval warships and few cruise ships (for example *Queen Mary 2* and *Queen Victoria*) are yet iconic ambassadors of their state, and as such are drawing the attention of terrorists (Murphy, 2007, p.56).

Ships-offshore installations as economic targets: Ships that when assaulted may interrupt the economic activity of the target-state, such as oil tankers and oil rigs, characterized as economic targets (Murphy, 2008, p.201-207). The overall target is oil, and tankers are vital element of oil industry’s critical infrastructure. Additionally, the simultaneously attacks to several oil tankers when they passed through international straits, could block the straits for a long period of time and disrupt the oil market (several ships sunk close together and not a small number of ships or only one). In order to achieve severe repercussions, terrorists need to decrease the world’s oil supply considerably, by devastating one or more refinery, production facilities or oil and gas terminals. However, successful attacks on economic targets could under specific conditions have serious consequences for the world economy, as a result of international commerce system’s sensitivity to disruptions (Murphy, 2007, p.56-57).

Ships as mass-casualty targets: A potential mass-casualty target characterized any ship that is transporting a large number of passengers (Murphy, 2008, p.207-212). Mass-casualty target is a category of maritime terrorism that a few people want to talk about, but a successful attack to such a ship and particularly if the ship itself constituted a prestige target, could serve the terrorists purposes very well. After the assault in the *Achille Lauro*, terrorist analysts have been waiting such an attack on a cruise ship. Cruise ships are well built and very hard to sink, but a *Limburg*-style attack could result serious numbers of dead and injured passengers which would be an extremely satisfying outcome for any terrorist group. Moreover, cruise ships are an excellent opportunity for terrorists to achieve a mass hostage-taking although it would be more difficult to be accomplished than an attack in an aircraft, because the number of passengers and crew are considerably larger than the number of terrorists (Murphy, 2007, p. 57-58).

Ships-other vehicles as weapons: Terrorist groups may use a ship as a potential weapon and for example may place explosives onboard and detonate it on or offshore (Murphy, 2008, p.212-213). Furthermore, a ship can be used as a weapon by be driven into port facilities or another ship, probably one that has volatile cargo (Murphy, 2008, p.230).

Donna Nincic claims that a ship can be used both as an agent of proliferation and as a Weapon of Mass Destruction (WMD). There are three broad ways in which this can take place: (1) terrorist merchant shipping "fleets", (2) the ship as an agent of proliferation, (3) and the ship as a WMD. Terrorist groups have taken advantage of all these circumstances inherent in the maritime domain. Some terrorist groups operate limited levels of maritime capacity, they even have used innocent ships in support of their operations, and a lot of ships carrying Dangerous Maritime Cargoes (DMCs) have been hijacked (Nincic, 2005, pp. 622-623).

Ships of concerns: Terrorist shipping "fleets": Many terrorist groups possess and operate their own merchant fleet while others exploit less creditable charterers and flags of countries under which their vessels can avoid financial charges or restrictive regulations. In addition, a lot of terrorist groups have different levels of maritime expertise which are varying from place to place. Even though we have increased concerns about these varying maritime skills, there is poor evidence about any of these terrorist networks if they are willing to develop the capability to launch an iconic, remarkable and economically disruptive attack such as were engaged on September 11 (Nincic, 2005, p. 623).

The ship as an agent of proliferation: Many terrorists exploit the knowledge of underworld's illegal activities and in particular of illicit maritime smuggling which include narcotics, arms and even humans. Hence, they make use of innocent merchant ships in order to transport Chemical – Biological – Radiological – Nuclear (CBRN) weapons and other various materials. There exist great concerns that maritime terrorists could take advantage of the "know how" from seaborne smugglers that operate in ocean "highways".

Maritime domain is characterized by many technological developments that have taken place in order to facilitate the global trade. These maritime economic efficiencies give unique opportunities to terrorist groups. For example, containerization has introduced huge economic efficiencies because has revolutionized the industry by allowing general cargo of different sorts to be placed in a single box. Hence, containerization has become very common in merchant vessels. Nevertheless, less than 1% of containers worldwide are inspected (Richardson, 2004). While there are nowadays some measures to increase security and to guarantee that nothing has been added to the container after the inspection and the sealing, such as tamper-proof security seals, yet there not always reliable examined (Broder, 2004). With this huge amount of containers in movement, travelling around the world's ports, and with so few if any physically examined, there exist a great opportunity for terrorists to smuggle weapons, people or even CBRN ingredients, making the merchant vessel a potential agent of proliferation (Nincic, 2005, p. 624).

The ship as WMD: Firstly, a vessel from its own could transformed to a WMD by hiding in the ship a "dirty bomb" or explosive devices, which could contain CBRN ingredients, and then to detonate them when the target is close enough. Secondly, there are highly dangerous cargoes such as Liquefied Natural Gas (LNG) or Liquefied Petroleum Gas (LPG) that if detonated could be as catastrophic as the assaults on New York. They could also be hijacked for blackmail if terrorists do not want to explode them.

Talking about dangerous cargoes there are two different types of them. Traditional WMD (uranium, anthrax, sarin, plutonium) or ordinary-everyday materials like LPG, LNG, ammonium nitrate and so on that are "dual-use", having both civilian and WMD applications (Nincic, 2005, p. 625). The ship as a WMD weapon can be used with the following ways: (1) the ship as a delivery system: a radiological device in a shipping container; (2) dangerous maritime cargoes: changing our conception of WMD; (3)

additional DMCs: ammonium nitrate and liquefied petroleum gas; (4) risks to DMC vessels: hijacking and suicide bombing; (5) sleeper agents and "embedded" suicide attacks; and (6) suicide boat attacks.

2.6 Factors that Contribute to Maritime Terrorism

Terrorist groups use the maritime environment to a varying extent. The most effective exploitation of the sea from terrorists has been done due to operational necessity. For example, when they wanted to protect their supply lines or when they needed to land forces alongside. Those terrorists that failed to use these kinds of imperatives have generally leaved behind their maritime activities.

The primary motivator for pirates is opportunity but for seaborne terrorists is necessity. But necessity alone cannot ensure success to terrorist groups. According to Martin Murphy (2007, p.46) seven major factors contribute to the effective operation of a terrorist group at sea: (1) legal and jurisdictional weakness, (2) geographical necessity, (3) inadequate security, (4) secure base areas, (5) maritime tradition, (6) charismatic and effective leadership, and (7) state support. Later on, Murphy (2008, p.359) added another eighth factor, the promise of reward.

Murphy supports that the factors that contribute to both piracy and maritime terrorism are considerable overlapping each other. These eight factors interact with each other and sometimes one predominates over the others depending on the circumstances, but all of them are usually present, even in different degree, when terrorists operating at sea.

Legal and jurisdictional weakness: Some states are giving coverage to terrorist groups by providing them with convenient bases either on land or in their territorial waters, for political convenience. Furthermore, many states that are weak, have scarcity of proper means to chase after terrorists or they lack motivation, that is why their territorial waters consist a refuge. Moreover, due to the fact that terrorists use flags of convenience, from countries that provide them cover, authorities of many states do not have rights to inspect the vessels onboard. That permits, in a legal sense, terrorist groups use vessels for their illegal activities.

Geographical necessity: Almost always, geography determines necessity. If a terrorist group operates in a land region they do not need to use sea and consequently they will not invest in a maritime capability as another terrorist group that operating in regions where the sea is strategically critical. There are many cases of terrorist groups, that geographical necessity has enabled the creation of their maritime capabilities in order to substitute their vulnerabilities.

Inadequate security: Inadequate security is a given for any insurgency to succeed since state security activity can have a huge effect on the insurgencies using terror. Some terrorists are fighting with the local authorities for long periods and neither has been able to overcome the other. Both can achieve local sea superiority to carry out specific operations. While others terrorist groups let the state security to achieve almost complete control over the sea areas it regarded as vital to its interests, reduced coastal raiding to negligible levels and imposed severe restrictions on insurgencies maritime logistical activity. Terrorists who need to move or relocate personnel and supplies by sea, benefit from underinvestment in maritime security by local authorities and poor international security cooperation between all the states.

Secure base areas: All terrorist groups need secure base areas. That means bases that terrorists can plan their next moves, have their logistical support, where they can rest or can be trained. For those terrorists operating at sea the situation is more difficult in contrast with their counterparts who have land bases, because people cannot leave for long periods at sea and depend on the reliable operation of boats to travel on it. If a state destroys the base of a terrorist group, this will seriously restrict the terrorists' maritime options and will result on less effective maritime activity. However, an organization's decisiveness affects how it copes with the catastrophe of its base.

Maritime tradition: Because the sea is an alien environment, if terrorist groups want to operate outside a port or a harbour in unsafe waters, then it is necessary to have maritime capabilities and proper maritime training, otherwise they must be in a position to exploit the maritime community for its skills and support. Some terrorist groups acquire skills and capabilities from their cooperation with smugglers while others enjoy close connections with seafaring tradition. The second emerges either because some groups draw their members from indigenous families with old seafaring traditions that have wide knowledge of the maritime environment, which give them plenty capabilities to operate as maritime terrorists, or because some other groups enjoy a close nexus among smugglers, fishermen, militants and ordinary tradesmen, who together establish a strong community, united by ties of blood relationships and caste. This strange relationship between terrorists and different kinds of maritime community may indicates a chronic and deep-rooted relationship between piracy and maritime terrorism, in which terrorists that use terror for political ends may also demonstrate piratical behavior (Murphy, 2007, p. 48-49).

Charismatic and effective leadership: A charismatic and effective leadership, which is exercised with unflinching determination can succeed in dealing with many obstacles. There are many terrorist groups that they have no apparent affinity with the sea and operate inland, even in areas with desert and mountains. These groups have no pressing to operate at sea and launch attacks in a maritime environment because they lacked experience, capabilities and maritime tradition upon which to draw. However, some of them succeeded to mount effective maritime attacks such as al-Qaeda, due to the organizational ability of their charismatic strategist, who was probably able to exploit maritime experience from the maritime environment for the practical expertise he needed. Nevertheless, if such a leader be captured or killed his absence will be a major damage and his replacement will not be easy (Murphy, 2007, p. 49-50).

State support: Terrorist groups receive substantial assistance from diverse states via the provision of arms, bases or both, or even by be provided with operatives equipped with the capabilities and the proper experience to discover unrecognized opportunities and resources for them. State support can balance presumed weakness or gaps in terrorists' capability and can enable a terrorist group to launch major maritime operations which would not be able to undertake without continuing external support (Murphy, 2007, p. 50).

Promise of reward: Both terrorists and pirates operate at maritime environment with the ambition and the promise of reward. Richardson (2007, p.75-80) identifies two types of targets in terrorist activities. On the one hand he recognizes long term objectives which can be comprehended through political change and on the other hand he points out short term objectives such as taking revenge, wreaking disorder, demanding concessions or strengthening internal cohesion. Terrorists can accomplish long term goals by using the maritime domain only to support operations on land, because revolutions and wars are not won at the sea (Corbett, 1988, p. 16). Hence, the focus must be on lighten the secondary motivation that can be accomplished at sea. This focus is reinforced by the acceptance that terrorists' long term goals are often not able to be reached or unsatisfactorily defined. In general, terrorism fails either because the policy question is unsufficiently clarified or because terrorists' political direction and terrorist application lacks mutual understanding. Gray (1995-6, p.32) has expressed it properly, "As for the political vision that should propel the entire process, it may lack practical connection to behaviour in the field (for example, in the case of of a united Ireland for the IRA). Given the fact that most terrorists lack of experience in the maritime environment, this linkage is sigificantly weak when it comes to maritime operations and that is why not many terrorists operate succesfully to the sea. However, as Richardson (2007, p.80) claims short term goals can be accomplished at sea and he categorizes them in three groups, revenge, renown and reaction.

Revenge can be found everywhere amongst terrorists (Crenshaw, 1981, p. 394). Terrorist have an unspeakable need to make their victims experience all the feelings and the pain that they have felt and have suffered symbolically, politically or economicaly through killings or acts of humiliation. Renown is mainly about publicity but also for glory. Terrorists seek for the regard by their supporters or peers when they are launcing a successful attack. The more impudent the assault or the more symbolic the target, the greater the glory (Richardson L. , 2007, pp. 94-95). At last, reaction display that the enemy takes them seriously. However, a maritime attack is unlikely to provoke a great reaction as terrorists have little or no presence there.

Additionally, Peter Chalk (2008, p.21), believes that the modest but yet highly discernible spike in terrorist incidents over the last years and the shift of focus on the maritime environment, have their origins in five main factors. At first, many of the vulnerabilities that led to a rise in the proportion of pirate attacks, like slack port security, insufficient littoral supervision, a large number of maritime targets and the immense dependence of the world’s main chokepoints, also apply to terrorism. The littoral states allocate the existing resources to land based security measures. In turn terrorist groups can exploit the weakness and the gaps that exist in the security of coastal states in order to move, hide and launch attacks in a way that is not possible on land.

Secondly, there is a huge expansion of commercial activities in the maritime domain. Enterprises that specializing in water-sports, scuba-diving, sailing lessons and marine equipment has provided terrorists with the necessary maritime training to build strong maritime capabilities and resources for operating at sea. It is common, members of terrorist groups are registering in diving companies so as to facilitate assaults against marine targets (Chalk, 2008, p.22).

Thirdly, terrorists can take advantage of the maritime environment to cause major economic destabilization as alternate means. The global maritime trade is based on “just in time, just enough”. Terrorists try to disrupt the whole base of these structure with the ultimate purpose to trigger enormous fiscal effects in particular if they achieve to impose a restriction on a major commercial port. Nevertheless, it is extremely difficult to achieve decisively disruptions because on the one hand the major global ports are highly secure and expansive, and even if a terrorist group could find a way to succeed, vessels could be fairly easily diverted to alternative terminals; on the other hand, very few if any chokepoints are actually nonsubstitutable. However, even if it is not possible a lasting disruption in the global economy, temporary, localized economic and fiscal damage may occur (Chalk, 2008, p.22-25).

Fourthly, maritime terrorism constitutes a further means of imposing mass casualties as a coercive punishment on enemy audiences. Cruise ships and passenger ferries are especially vulnerable because they cater to large numbers of people who are confined in a single physical space and provide to the extremists a high-prestige, iconic target to attract considerable media attention (Chalk, 2008, p.25-26).

Finally, the containerization of the global maritime trade offers terrorists a perfect coverage for the transportation of weapons and personnel in two critical respects. At first, the maritime trading system want to keep costs low and turnover high. So the transportation system is designed to be as accessible and flexible as possible and there are no strong motives to enact expansive security measures. Secondly, the highly complex nature of containerization, combined with the inadequate inspections, creates a great amount of openings for terrorist infiltration (Chalk, 2008, 26-29).

2.7 Obstacles to Success of Maritime Terrorism

It is crucial not to overestimate about the threat from maritime terrorism. While many may make assessments and warn about the potential grave knock-on effects on global trade and the present danger of maritime terrorism for developed economies, implementing attacks in the maritime environment is an option that presents so many problems that the majority of terrorist groups probably would prefer an equivalent act on land. Below, we will quote some of the problems that were faced by terrorist groups (Murphy, 2007, p.71).

Even the terrorists themselves recognize that the results of attacks that have been launched at the maritime realm, in term of publicity have been narrowed. The unusual demands of the sea environment make assaults large enough for the media. Scenarios like the sinking of a passenger ferry or a cruise ship, the mass killing of citizens of developed states, the bombing of a warship, spectacular attacks on the global maritime transport system and the delivery of CBRN weapons to a major port are more feasible on land than at sea (Murphy, 2007, p.69).

In order to succeed in sea, terrorists must have a long-last training in navigation, coastal piloting and other maritime lessons, because they are not used to the sea, even if they have close connections with maritime tradition. All their attacks must take account many maritime details such as wind, sea state, underwater obstacles and many other weather and water elements (Pelkofski, 2005, p. 22). Difficulties in the surveillance of the targets, little if any practicing in their attacks patterns, no testing of the weapons in combination with the unpredictable marine environment, are making maritime operations more difficult than terrorist groups want. Maritime operations demand complex plans and sophisticated execution, special knowledge and many marine skills in contrast to terrorists who try to keep things just as simple as possible. There are so many targets in the maritime environment which are so inadequate secured that they are very attractive to terrorist groups (Sinai, 2004, p. 62). However, in general, these targets are insufficiently accessible, if we take account of the difficulties given above, and they are not within their priorities (Murphy, 2007, p.69-70).

Speaking about ships as iconic targets, the most distinguished maritime targets are warships which are vulnerable to terrorists' attacks but after the incident at US Cole, now all ships are taking security measures to avoid such kinds of assaults and so they are more secure. Talking about mass casualties the first thing that are coming to our mind are cruise ships and ferries. Cruise ships are implementing strictly security measures to passengers, to their luggage even to their own personnel. In addition, they have designed their ships' structure to resist in a crash with a small boat manned by a suicide bomber. On the other hand, ferries do remain highly vulnerable (Murphy, 2007, p. 70).

Moreover, in theory is believed that large ships can be used as weapons against other large ships or ports but in reality something like that is very difficult since there exist considerable obstacles. Targets like oil and gas platforms, terminal and others fixed economic targets at sea have even more difficulties in overcoming security mesaures and the proportions points that a terrorist attack on installations like these has not yet succeeded.

There exists always the alternative of raiding land targets form the sea, because on land there are many fixed economic targets (pipelines, oil terminals, refineries etc.), mass casualties targets (shopping malls, hotels etc) which are not properly secured and few law enforcement bodies have maritime capabilities. Finally, an assault at the sea has not the same effect as on land because of the surface of the sea that is not as static as land and simultaneously the moving sea targets are more difficult to be accurate aimed.

The possible conflation and the tactical nexus between piracy and terrorism are the main worries for states, global organizations and major shipping interests around the world. The fear which exists is that terrorist groups by working together or by subcontracting out missions to pirates, will finally manage to overcome the operational constraints in the maritime environment (Chalk, 2008). However, it is important to distinguish between piracy and maritime terrorism and any suggestion of possible nexus between them should be viewed with caution. There is no evidence that they have a collusion or that they will (Murphy, 2008, p. 387). There exists a very thin line between piracy and terrorism and there are certain factors which are drawing this line (Panda, 2009) (More about the possible nexus but also the distinction between piracy and terrorism at Appendix A). Consequently, because of the fact that a possible nexus between piracy and terrorism is not easy to occur and at the same time there are so many obstacles that prevent terrorist groups from succeed in their operations, terrorists will try to continually advance their methods in order to achieve their goals by overcoming these barriers. Therefore, it is critical for the terrorists to adjust their tactics, modus operandi and sometimes even their weapon systems. The terrorist groups that would be more sophisticated, will exploit the dependence on electronic means of commerce and communication with virtual attacks, involving anonymous cyber assaults so as to accomplish their efforts.

3 Maritime Industry and Cyber Risks Analysis

3.1 Maritime Industry as a Critical Infrastructure

"*Today, around 90% of world trade is carried by the international shipping industry. Without shipping the import and export of goods on the scale necessary to sustain the modern world would not be possible.*" These words were spoken by Koji Sekimizu, IMO Secretary-General addressing the IMO Council, meeting for its 28th Extraordinary Session at IMO Headquarters in London.

The maritime industry may be one of the oldest in the world and the maritime sector sustains society and most of all the global economy through the continuous, free flowing movement of people and vital goods. A sector as open and as frictionless as possible where effective processes have reduced inventory – holding to a very minimum, hence the phrase "just enough – just in time" (Raymond, 2006, p. 239). The urgency of the maritime sector for states and economies is clearly demonstrated by available data.

ENISA in its 2011 report noted that 52% of the goods trafficked in 2010 were carried by maritime transport, compared to 45% a decade earlier. The report further noted that approximately "90% of EU external trade and more than 43% of the internal trade take place via maritime routes." 3 and 5% of EU Gross Domestic Product (GDP) are contributed by industries and services belonging to the maritime sector.

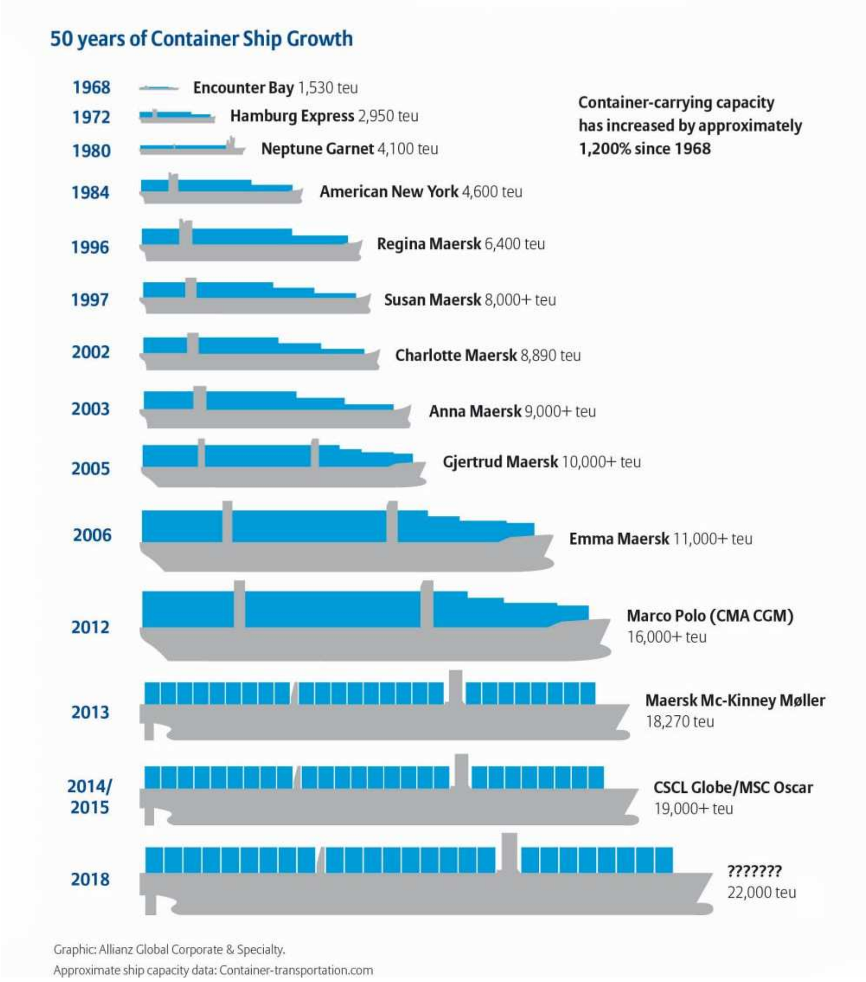
A terrorist attack that will disorganize the continuous flow of maritime goods would have a colossal negative impact, from both an economic and security perspective. This impact would be felt worldwide but it would affect particularly EU and US. According to ENISA (2011, p. 3), "the three major European seaports (i.e., Rotterdam, Hamburg and Antwerp) accounted in 2010 for 8% of overall world traffic volume, representing over 27.52 million TEUs." In addition, these ports "carried in 2009 17.2% of the international exports and 18% of the imports." So far as US is concerned, the GAO (2014, p. 4) noted that, as an essential element of US's critical infrastructure, the maritime industry "operates approximately 360 commercial sea ports that handle more than $1.3 trillion in cargo annually."

3.2 The Relationship Between Maritime Security and Cyber Security

The global economy is critically dependent upon maritime movement of cargo and passengers (ENISA, 2011, p. 3). On the other hand, both private and government entities, as well as the aerospace and defense industry, banking and health insurance industries and especially the maritime industry have become increasingly dependent on Information Communication and Technology (ICT), network-centric operations and wireless communication systems, in order to optimize their operations and to process, maintain and report essential information, as computer technology has advanced (GAO, 2012, p. 3). In this digital information age e-enabled vessels, vehicles, infrastructure, communication and management systems are the norm. The critical element that has enabled the pace of contemporary globalization is the impact of digitalization in commerce and services. ICT is used to enable essential maritime operations, from navigation to propulsion, from logistics to network operations and safety management, etc. Although the maritime sector illustrates the most important point of reference for the global economic development, maritime cyber security has received only little if any attention (Masala & Tsetsos, 2015, p. 11). ENISA (2011, p. 3) noted that "the awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent." Future cyber threats will be introduced by hackers, often many kilometers away from their targets, using their ability to cyber-attack any maritime infrastructure and vessel they want with severe consequences for the maritime sector. Allianz Risk Barometer 2016 identifies a lack of robust cyber security, as a significant threat (in 3rd position) to future shipping safety (Allianz, 2016, p. 3). The maritime domain is regarded as being increasing exposed to a major attack. Crews becoming smaller, ships becoming larger (image 2) and a developing dependence on automation all essentially infuriate the risks from hackers disrupting key systems (Allianz, 2015, p. 30). Maritime trade is so crucial, considering the fact that global maritime trade and frictionless functionality of marine infrastructures illustrate a critical condition for global economy. Even small disruptions would seriously restrict the flow of goods and lead to unmeasurable proportions (Masala & Tsetsos, 2015, p. 11).

Maritime security in general pays attention only to "physical" aspects of security and safety. Classic security risks and vulnerabilities emerge in relation to ships, economic assets, cargo, critical maritime infrastructures, people involved and trade flows. Thus gives priority to the prevention or the mitigation of all kinds of accident from which may occur environmental pollution, ship collisions, vessel survivability etc. Given that, maritime security is represented by anti-piracy and anti-terror measures, maritime surveillance, ports and other marine facilities security and avoidance of ship misuse. Both maritime safety and security depend on network-operated systems, ICT, cyber dependent technologies for navigation, engineering, ballast, environmental control and many other purposes, while ports increasingly engage digital logistic system like automated entry and cargo management systems or autonomous cranes (Masala & Tsetsos, 2015, pp. 11-13).

While these cyber systems introduce benefits, they also create risk. Misuse, exploitation and even simple failure of these systems may lead to injuries or deaths, damage the marine environment or disrupt vital trade activity (Michel, Thomas, & Tucci, 2015, pp. 1-2). Cyber security concerns in particular these technologies and processes which has been designed to protect computers, networks and data from cyber criminals. However, cyber security becoming a growing threat. A mixture of individuals and several groups are using computer and networks vulnerabilities in order to damage maritime realm. Cyber threats exist and sensitive maritime assets are prime targets (XL Group, 2013, pp. 1-2).



Graphic: Allianz Global Corporate & Specialty.
Approximate ship capacity data: Container-transportation.com

Figure 2 50 Years of Container Ship Growth (Source: Allianz Global Corporate & Specialty)

3.3 Cyber Risk’s Characteristics

The Institute of Risk Management defines Cyber-risk as “the risk of financial loss, disruption or damage to the reputation of an organization due to any sort of failure of its information technology systems.”

Cyber-risk is much different from conventional maritime risk. Internet has made modern technologies and sophisticated tools that were previously available only to major actors like nation states, available to almost anyone and everywhere, because is very cheap or sometimes total free, is spreading widely throughout society and whoever use it do not need much experience or training (Nordell, 2015). Cyber attackers there is no need to be physically close to their targets and they can load their attacks from almost anywhere, since technology permits assaults to easily cross state and national borders and their operations can be executed at high speed, without risking their lives and simultaneously remain anonymous. Furthermore, attackers may use multiple approaches that combine a variety of techniques, in order to aim at individuals, businesses, critical infrastructures and government agencies (GAO, 2012, p. 6). Moreover, nation states or terrorist groups can now easily enlist non-state agents as proxies and cyber-mercenaries (Nordell, 2015).

In addition, cyber attackers have some crucial advantages. At first, it is very difficult to detect where the attack is coming from and even more difficult to place blame for. Given that, the attackers can easily enjoy plausible deniability. Secondly, it is hard and very expensive for individuals, companies or even states to defend against these sophisticated attacks. Thirdly, the victims of these assaults would usually prefer to keep quiet, so cyber security is becoming more challenging by the absence of any definitive information about the attacks and the hackers are improved as a result. At last, attackers take full advantage of their asymmetric strength and they can achieve great results even if they are small, anonymous groups or individuals (Nordell, 2015).

3.4 Actors

It is very difficult for someone to understand and defend against cyber risk without the proper understanding of the geopolitical and social drivers. According to BIMCO (2016, p. 3), there are many motives both for individuals and organizations to take advantage of cyber vulnerabilities. The following table distinguish actors with examples of the threat posed and the potential consequences, giving extra attention to terrorists.

Table 1 Major Actors and their Motivation and Objectives (Based on BIMCO, 2016)

Group	Motivation	Objective
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo
Opportunists	• The challenge	• Getting through cyber security defenses • Financial gain
States State sponsored organizations **Terrorists**	• Espionage • **Political gain**	• Gaining knowledge • **Disruption to economies and critical national infrastructure** • **Arranging fraudulent transportation of cargo** • **Financial gain (for terrorist purposes)**

All the above groups of actors are functioning and have the necessary skills and requisite resources to threaten the safety and security of vessels and a company's ability to conduct business. Additionally, there is always the possibility for individuals, usually end users, inside the company or onboard a vessel to compromise cyber systems and data unconsciously.

3.5 Categories and Techniques of a Cyber-Attack

Generally, the main two categories of cyber-attacks which affect maritime domain are the following:

Targeted attacks, in which the main and only target of the attack is the maritime company or a ship's system, and

Untargeted attacks, in which there are many potential targets and among them may be a specific maritime company or a ship's system (BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO, 2016, p. 4).

Terrorists actors use both categories in order to attack a potential target. Moreover, the actors of cyber-attacks are using some types of techniques in order to carry out their attacks. BIMCO (2016) divides the techniques into two groups according to where they belong (targeted or untargeted attacks),

Table 2 Techniques of Cyber Attacks (Source: BIMCO, 2016)

Targeted Attacks	**Unargeted Attacks**
Spear – Phishing	Social Engineering
Deploying Botnets	Phishing
Subverting the Supply Chain	Water Holing
	Ransomware
	Scanning

while Rouzer (2015), identifies six main types of cyber-attacks, which are shown in diagram 2. (The definitions of the categories and techniques are given in Appendix C.)

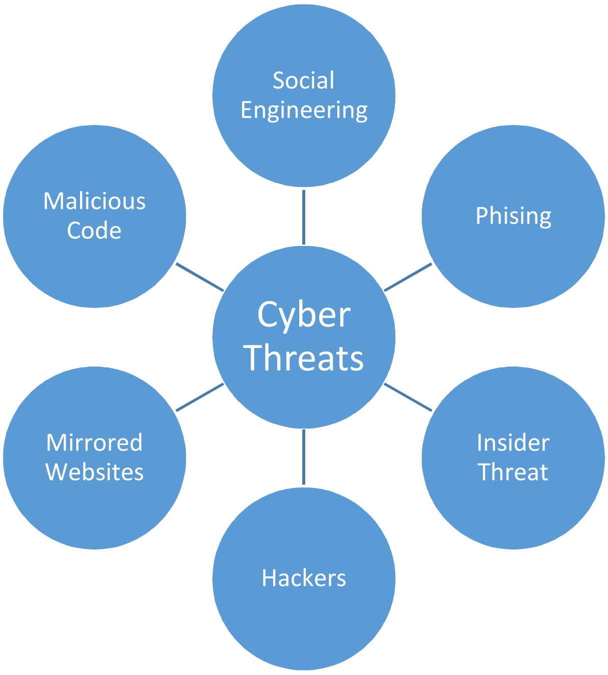


Diagram 1 Techniques of Cyber-Attacks (Source: Rouzer, 2015)

3.6 Stages of a Cyber-Attack

According to BIMCO (2016, pp. 4-5), almost all cyber-attacks are conducted to successive stages and in particular four stages. The duration of the cyber-attack as a whole process depends on the countermeasures applied by the company combined with those onboard ships and at the same time bounded by the motivations and objectives of the attackers. The four stages of a cyber-attack are:

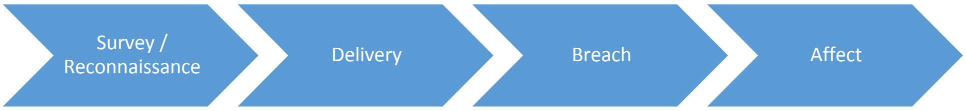


Diagram 2 Stages of a Cyber-Attack

*Survey / Reconnaissanc*e: Acquisition of information through open/public sources (social media, forums, websites, publications, etc.) about the company or the ship in order to prepare a cyber-attack.

Delivery: Access to company's or ship's systems data remotely from the internet and/or from within the company or the ship.

Breach: Depending on the extent of the vulnerabilities and the method used, is the range of the gap that a cyber-attack can achieve to a company or ship system.

Affect: The affection of a cyber-attack on the company or ship system and data.

(The definitions of the stages are given in Appendix C)

3.7 Vulnerabilities

The proliferation of digital technologies and the enlargement and the complexity of ICT and data control systems means that the risk in the maritime domain from cyber threats is growing every single day. These technologies have become essential for the maritime sector and in some cases must comply with the international standards. But while these cyber technologies provide important efficiency advantages for the maritime domain, many new cyber-threats put in danger many critical maritime facilities like vessels, oil rigs, ports etc. These cyber threats may arise from vulnerabilities resulting from inadequate operation, integration, maintenance and design of these systems. Below, we will list the main vulnerabilities of the systems, we will discuss some of them in the following paragraphs (Wildemann, 2015, pp. 1-2) and we will describe some actual incidents that have taken place in the past. The amount of these incidents is unknown and underrepresented, for two major reasons. The first is that there is a trend among the victims to keep such successful attacks secret and the second reason is that many victims are unaware that they have been intruded (CyberKeel, 2014, p. 4).

Vulnerable systems could include, but are not limited to (BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO, 2016, p. 7):

Bridge systems;

Cargo handling and management systems;

Propulsion and machinery management and power control systems;

Access control systems;

Passenger servicing and management systems;

Passenger facing public networks;

Administrative and crew welfare systems; and

Communication systems.

(More details are given in Appendix C)

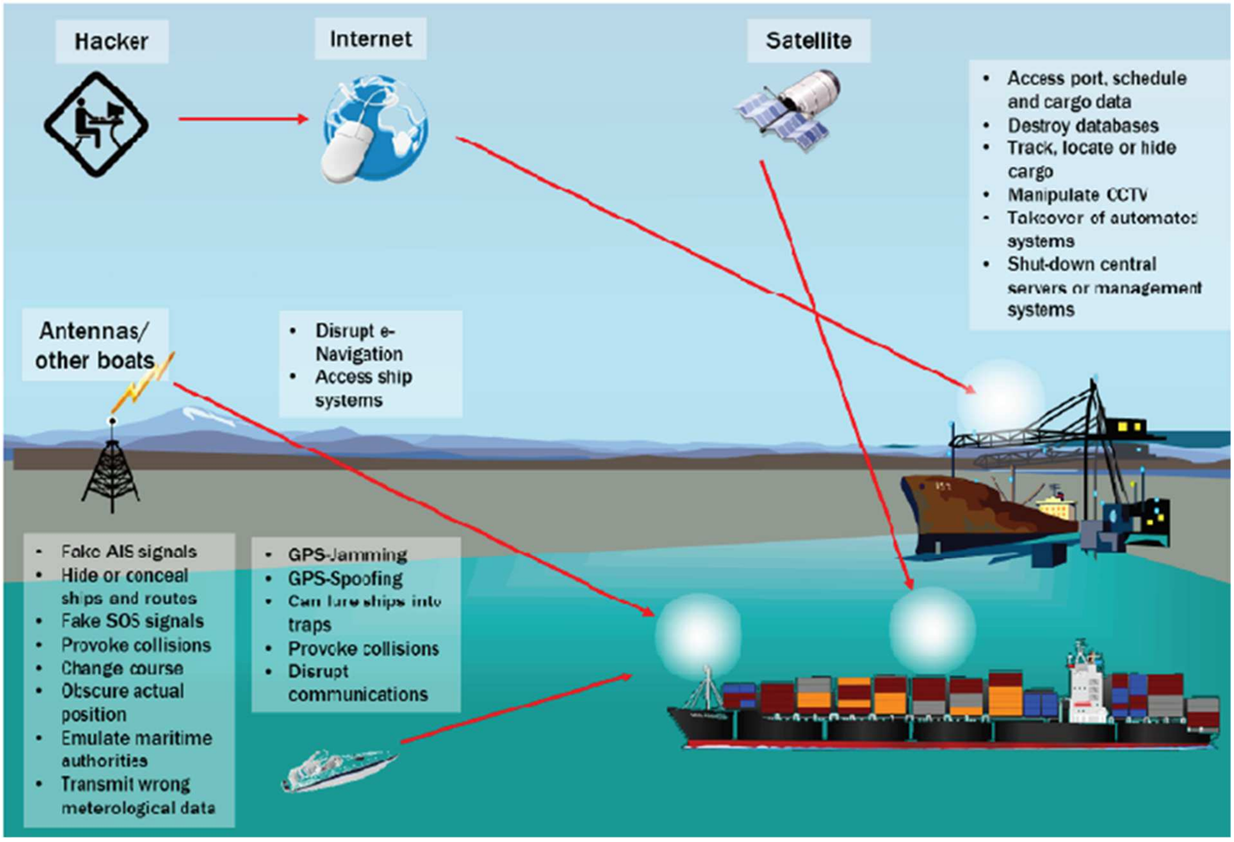

Hacker
Internet
Satellite
• Access port, schedule and cargo data
• Destroy databases
• Track, locate or hide cargo
• Manipulate CCTV
• Takeover of automated systems
• Shut-down central servers or management systems
Antennas/ other boats
• Disrupt e-Navigation
• Access ship systems
• Fake AIS signals
• Hide or conceal ships and routes
• Fake SOS signals
• Provoke collisions
• Change course
• Obscure actual position
• Emulate maritime authorities
• Transmit wrong meterological data
• GPS-Jamming
• GPS-Spoofing
• Can lure ships into traps
• Provoke collisions
• Disrupt communications

Figure 3 Potential Threats against Vessels and Ports by Cyber-Attacks (Source: Enge & Goge, 2016, p.19)

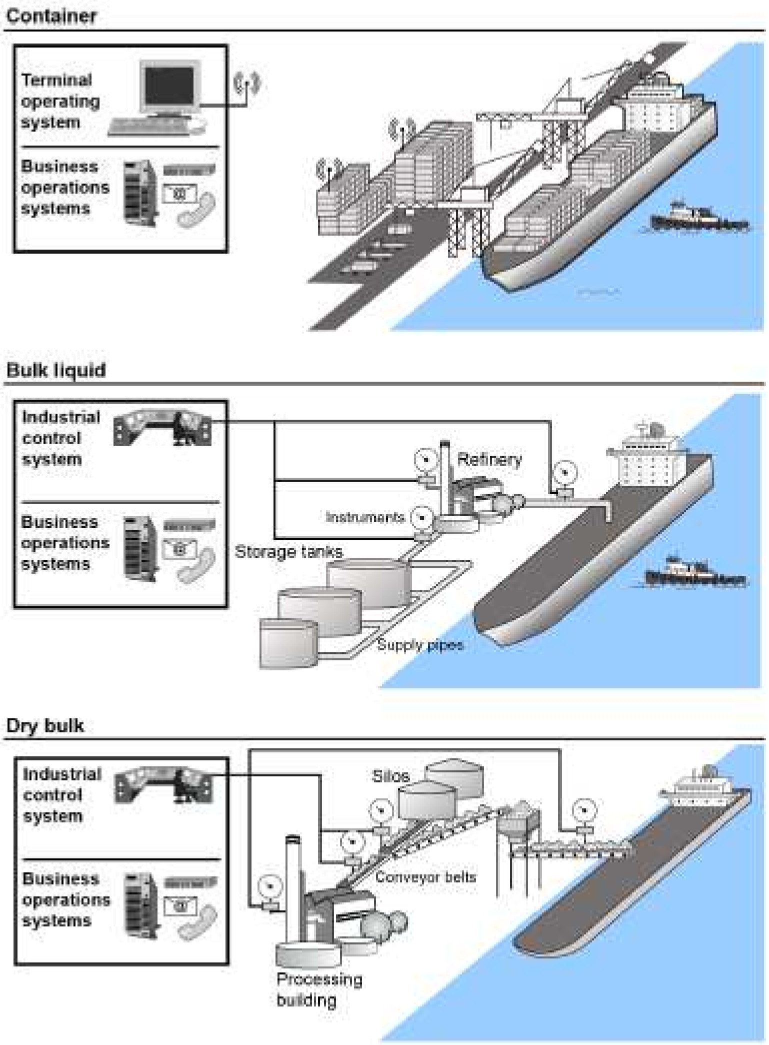
3.7.1 Ports/Harbors

Ports and cargo terminals are maybe the most critical facilities with a major role to international trade. They facilitate the connection between producers and suppliers, distributors and clients, and playing a crucial role for the global economic development since they constitute, at the same time, the entrance and the exit to the global market, intangible economic assets and priceless nerve centers in any supply chain (Masala & Tsetsos, 2015, p. 12). In the following three images 4, 5 and 6, we can see examples of technologies used in maritime port environments (Image 4), cargo operations then and now (Image 5) and an attack surface overview of a contemporary port with its cyber systems which can be exploited (Image 6).

Port of Antwerp used for drug smuggling: In late 2013, Europol made public that the port of Antwerp had been breached by a persistent cyber-attack that was launched by a network of drug traffickers who recruited hackers to assault IT systems in the port of Antwerp in Belgium. The cyber-attack had been ongoing since June 2011 and allowed the hackers to have remote access to the terminal systems and to secure data giving them the location and security details of containers, in which consignments of drugs had been hidden. Then they dispatched their own drivers to retrieve the containers, by means of false papers and a hacked pin code, ahead of the scheduled collection time. Furthermore, they deleted any information about the container's existence after the fact. This activity continued for almost two years, until they had been exposed. There were no major consequences for the port or the companies involved. The fact that criminals or terrorists use containers as a vehicle for the transportations of their operations is more or less known. However, the method was something entirely new and exposed many critical vulnerabilities and something that can be named as "ghost shipping". The potential many terrorist groups acquiring free access to ports, shipping lines and systems that provides the ability to transport any commodity anywhere, without anyone even knowing it is there, is a scary scenario (CyberKeel, 2014, p. 5; CyberKeel, 2014, pp. 7-8; MARSH, 2014, pp. 2-3).

Bypassing Australian Customs: In 2012 it was uncovered a penetration to the cargo systems operated by the Australian authorities, launched by crime syndicates. This intrusion to the systems permitted criminals to have an inner sight about whether their shipping containers were valued as suspicious by the authorities. The repercussion was that when such a container was identified as suspicious, were abandoned by the criminals (CyberKeel, 2014, p. 8).

CyberKeel Container Carrier Penetration Test: In 2014, CyberKeel took a closer look at potential cyber vulnerabilities for the 50 largest container carriers. The tests were quite simple and by no means comprehensive. These simple tests exposed that 37 out of the 50 largest container carriers were vulnerable to these relatively simple intrusion attacks (CyberKeel, 2014, p. 9).


Container
Terminal operating system
Business operations systems
Bulk liquid
Industrial control system
Business operations systems
Refinery
Instruments
Storage tanks
Supply pipes
Dry bulk
Industrial control system
Business operations systems
Silos
Conveyor belts
Processing building

System descriptions

Terminal operating systems

Control container movement and storage in the maritime port, among other things. Examples of data that terminal operating systems could contain include shipping information, cargo categorization, and records of container movement.

Business operations systems

Support the business operations of the terminal, such as communication with customers and preparation of invoices and billing documentation.

Industrial control systems

Facilitate the movement and processing of goods throughout the terminal, including the operation of motors, pumps, valves, signals, lighting, and access controls.

Figure 4 Examples of Technologies Used in Maritime Port Environments (Source: GAO Analysis of Maritime Sector Information)

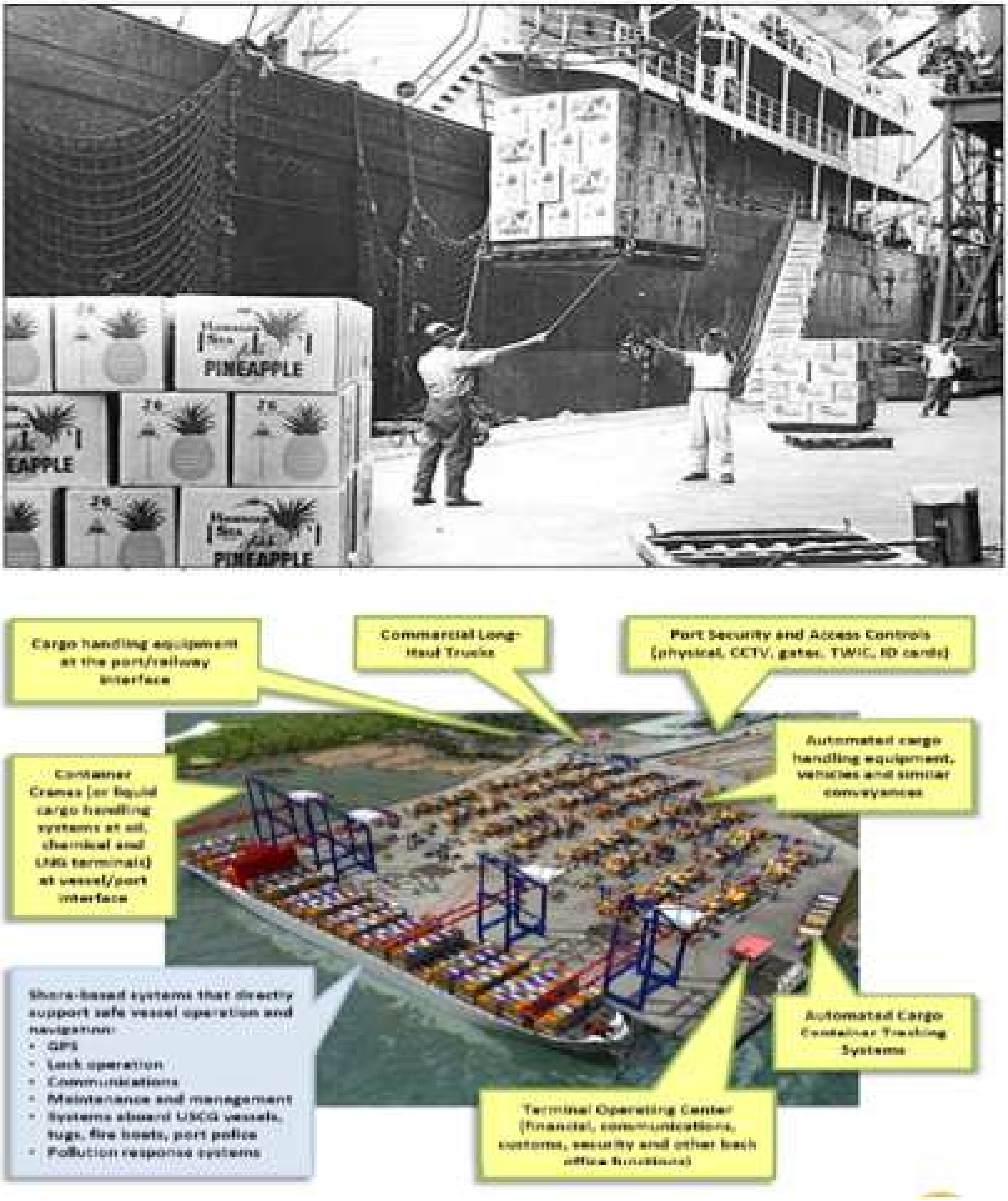

PINEAPPLE
Cargo handling equipment at the port/railway interface
Commercial Long-Haul Trucks
Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)
Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface
Automated cargo handling equipment, vehicles and similar conveyances
Shore-based systems that directly support safe vessel operation and navigation:
• GPS
• Lock operation
• Communications
• Maintenance and management
• Systems aboard USCG vessels, tugs, fire boats, port police
• Pollution response systems
Automated Cargo Container Tracking Systems
Terminal Operating Center (financial, communications, customs, security and other back office functions)

Figure 5 Cargo operations Then and Now (Source: Rouzer, 2015)

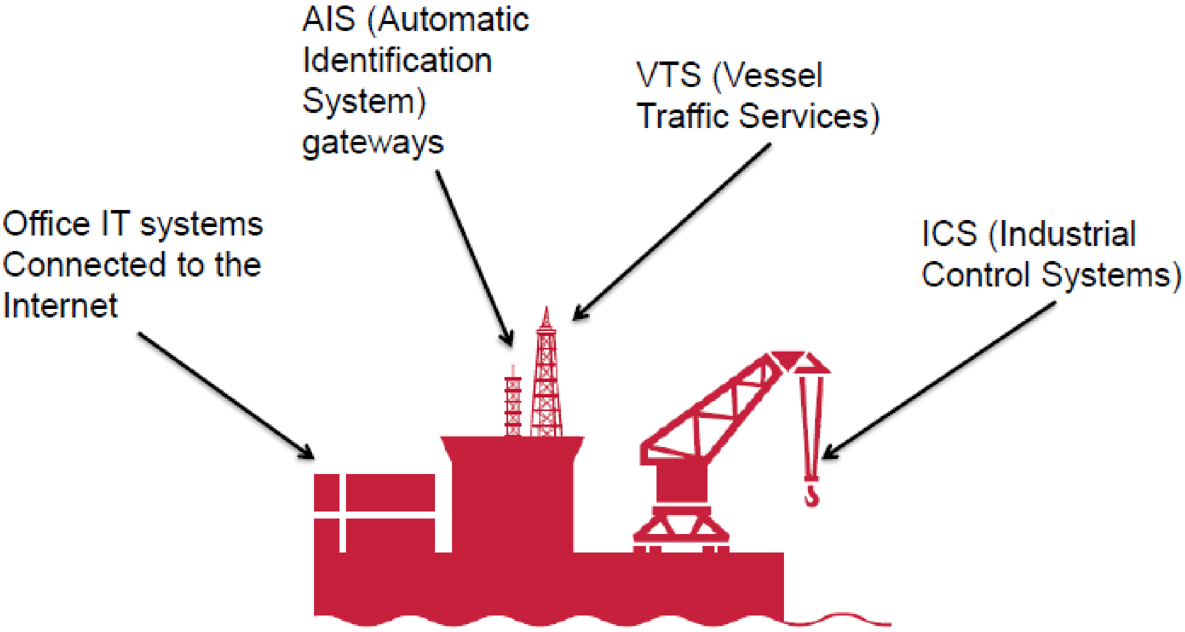

AIS (Automatic Identification System) gateways
VTS (Vessel Traffic Services)
Office IT systems Connected to the Internet
ICS (Industrial Control Systems)

Figure 6 Attack Surface Overview of a Contemporary Port (Source: NCC Group)

3.7.2 Ships

Modern vessels base their operations on the proliferation of sophisticated technology or else their central "brains" which are composed by highly automated and networked communications, operational and navigational systems. These brains can actually run the vessel without any help from human personnel. However, they confront a major problem, that they are extremely vulnerable to cyber-attacks through radio frequency (RF) interference (intentional or unintentional).

GPS spoofing: In July 2013 University of Texas researchers demonstrated that it is possible to take control of the navigational systems of a big, expensive vessel, in order to change vessel's direction just using a cheap electronic GPS "spoofer" built in $3,000 and a laptop. By interfering with its GPS signal and injecting their own radio signals into the vessel's GPS antennas, they cause the onboard navigation systems to falsely interpret vessel's position and heading and simultaneously enabled them to steer the vessel and redirect the course. In addition, ship's GPS systems reported that the ship was moving steadily to his original course (CyberKeel, 2014; Cowie, 2015).

Automatic Identification System (AIS): "…researchers have discovered that flaws in the AIS vessel tracking system can allow attackers to hijack communications of existing vessels, create fake vessels, trigger false SOS or collision alerts and even permanently disable AIS tracking on any vessel" (Wilhoit & Balduzzi, 2013).

The security gap is particularly worrisome because it does not require expensive equipment or impressive hacking capabilities to utilize it. The threat is that terrorist groups could exploit these vulnerabilities to lure vessels into changing its course, seize all communications, cover up their ships with fake IDs, sent out false distress signals to lure vessels into traps etc., which could lead to serious physical consequences and even the paralysis of maritime traffic in a particular area (Masala & Tsetsos, 2015, pp. 16-17).

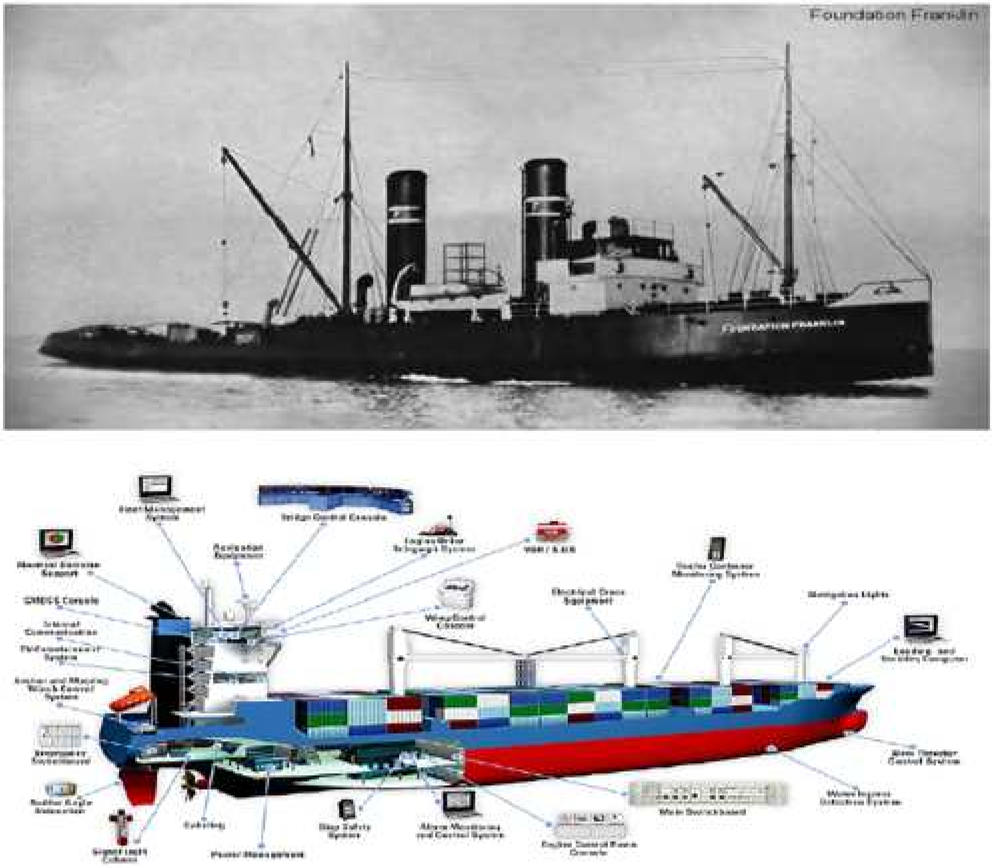


Figure 7 Ships Then and Now (Source: Rouzer, 2015)

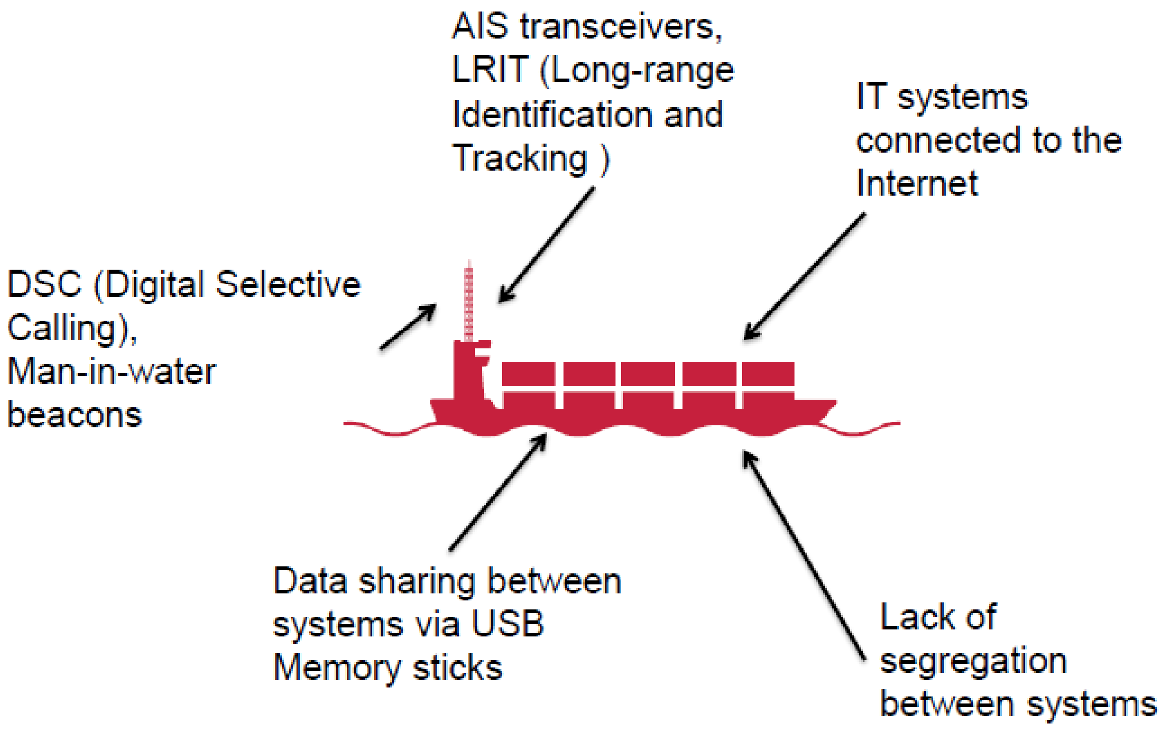

AIS transceivers, LRIT (Long-range Identification and Tracking)
IT systems connected to the Internet
DSC (Digital Selective Calling), Man-in-water beacons
Data sharing between systems via USB Memory sticks
Lack of segregation between systems

Figure 8 Attack Surface Overview of a Contemporary Ship (Source: NCC Group)

3.7.3 Oil Rigs

Hacker caused a floating oil platform located off the coast of Africa to tilt to one side, forcing temporary shutdown. The causes were able to be identified by qualified staff only after a week (Rouzer, 2015). Also a hacked security system in an oil rig in the Gulf of Mexico managed to reduce the oil production to zero for several weeks.

A coordinated attack in critical maritime infrastructures could put companies out of business, limit their availability of energy and resources, lead to productivity losses or generate massive environmental pollution and last but not least to endanger the lives of the personnel working on such platforms (Masala & Tsetsos, 2015, p. 18).

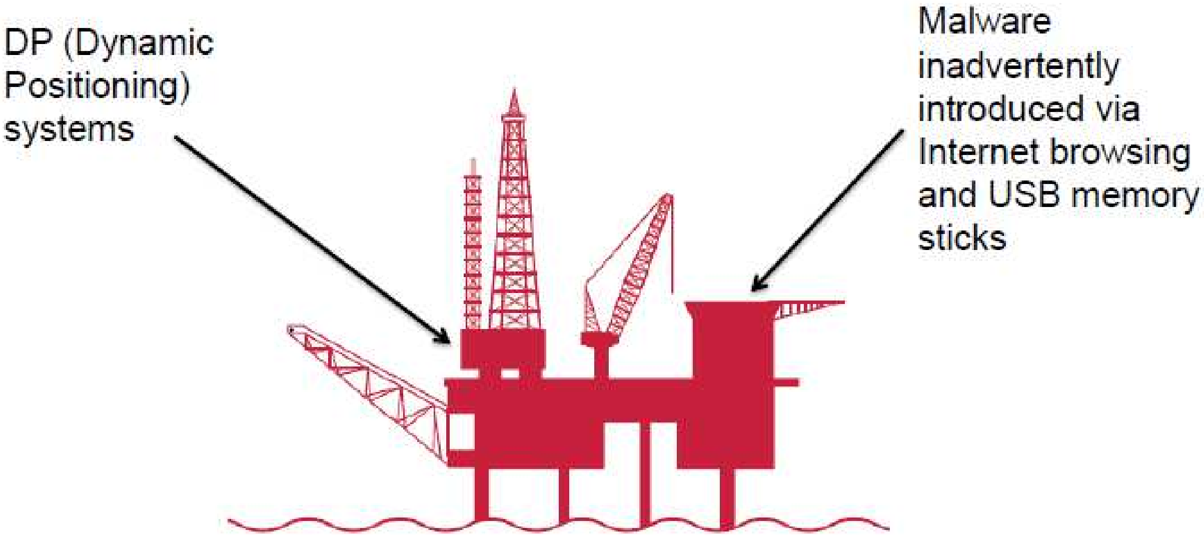

DP (Dynamic Positioning) systems
Malware inadvertently introduced via Internet browsing and USB memory sticks

Figure 9 Attack Surface Overview of an Oil Ring (Source: NCC Group)

3.7.4 Satellites/Navigation

These satellites are designed particularly for the maritime sector in order to provide extensive coverage of world’s sea realm. Real time communication for vessels, cargo surveillance, ship monitoring, voice, video and data exchange are some of the common services included. During 2013, a study was conducted by a security company, which found that SATCOM terminals have critical security issues and almost all devices could be abused. All these vulnerabilities could give to the terrorists control of the ship’s information, devices onboard, weather information etc. (Vulnerable Satellite Equipment in Appendix C).

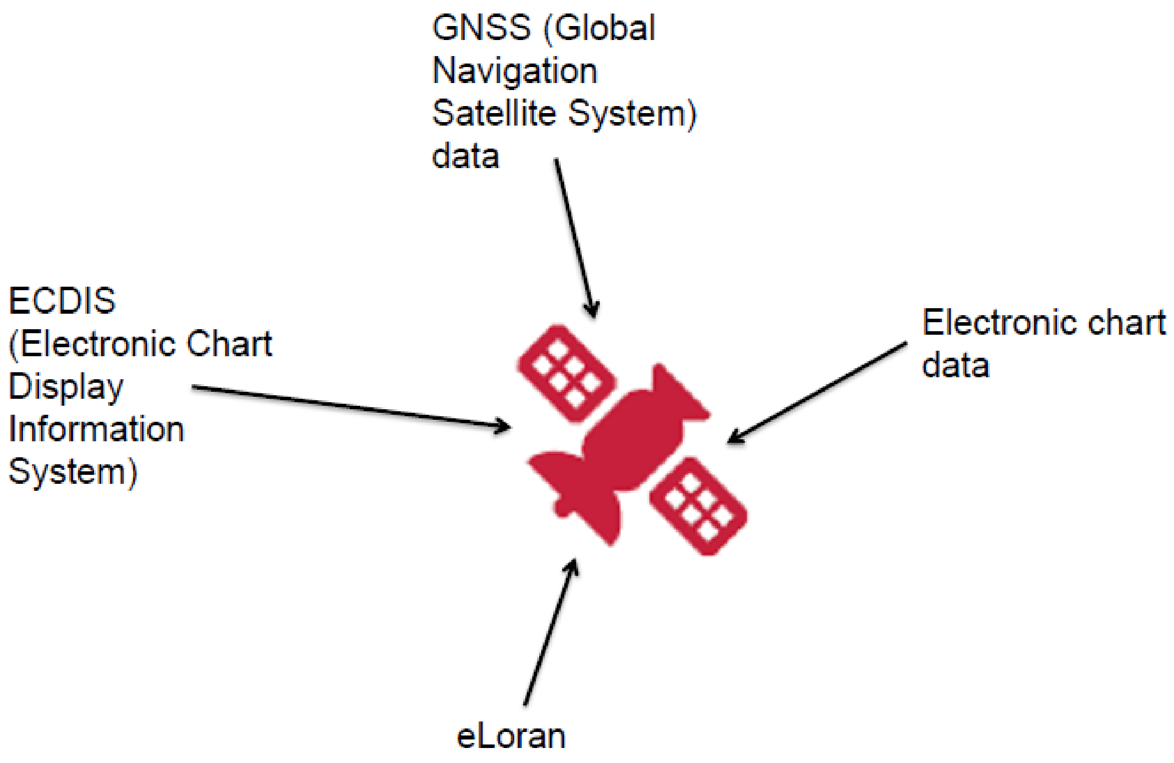

GNSS (Global Navigation Satellite System) data
ECDIS (Electronic Chart Display Information System)
Electronic chart data
eLoran

Figure 10 Attack Surface Overview of a Satellite/Navigator (Source: NCC Group)

3.8 Risk Analysis

We performed a Risk Analysis in order to assess the level of risk associated with cyber maritime terrorism. We began by answering some questions such as “*What can go wrong?*” and “*What is the likelihood and the consequences (impact)?*” To answer these questions, we at first identified terrorist threat scenarios which in turn were filtered and ranked, and, based on qualitative assessment, the probability and impact of each scenario was determined.

3.8.1 Threat Scenario Identification

Identifying terrorist threat scenarios specific to the maritime domain was a two-step process:

(1) First, all key elements of the maritime domain were identified

(2) Threats were identified, using evidence from the literature, and creative speculation about what could happen. Threat identification is, at its essence, a fundamentally creative concept – the more

scenarios identified, the greater the likelihood that plans will be in place to protect against the widest range of potential threats.

3.8.2 Likelihood and Consequences: using a Probability- Impact Matrix

Since we identified as threats as possible, we then organized them in a manner that allows for their practical assessment. We created a simple matrix, in order to present and compare terrorist threats in a simple schematic form, based on the probability of an event occurring and the impact of the event. The following table is an example of the simple risk matrix we used.

Table 3 Example of Risk Matrix

	Probability				
Impact	1	2	3	4	5
1	(1)	(2)	(3)	(4)	(5)
2	(2)	(4)	(6)	(8)	(10)
3	(3)	(6)	(9)	(12)	(15)
4	(4)	(8)	(12)	(16)	(20)
5	(5)	(10)	(15)	(20)	(25)

The numbers 1 through 5 that indicate Probability, run from lower to higher:

(1) 0% to 20% (Lowest probability of occurring)

(2) 21% to 40% (Low probability of occurring)

(3) 41% to 60% (Medium probability of occurring)

(4) 61% to 80% (High probability of occurring)

(5) 81% to 100% (Highest probability of occurring)

Probability is a number from zero (the event will not occur) to one hundred (the event will certainly occur).

The numbers 1 through 5 that indicate Impact, run from lower to higher:

(1) Lowest level of negative impact

(2) Low level of negative impact

(3) Medium level of negative impact

(4) High level of negative impact

(5) Highest level of negative impact

The number in parentheses in the middle of each cell is the risk value:

Risk Value = Probability x Impact

Items with higher risk values are considered the primary threats. Note that it is possible to have an extremely destructive event (Impact = 5) but not a high risk value if the probability of this event occurring is very low (Probability = 1). So events with high impact or high probability can be less of a risk that events with a lower impact and lower probability.

In our color coded table, the green cells represent events with the lowest risk value (RV), the blue cells have low risk values, the yellow cells have moderate risk values; the orange cells have higher risk values and the red cell has the highest risk value. The orange and red cells, therefore, represent events of the most serious concern

We identified fourteen maritime threat scenarios. These scenarios are listed in Appendix C. We prepared the scenarios for use in the Probability-Impact matrix, assigning each scenario both a probability value (1-5) and an impact value (1-5). The assignment of both the probability value and the impact value was based on an assessment of similar events that had occurred in the past, as well on educated hypotheses of what might happen in the future. Obviously, the initially assigned probabilities are subjective probabilities and should be updated and refined by Bayesian techniques as additional information becomes available.

Our results are as follows in the following table (the numbers in each cell refer to the number of the threat scenario in Appendix D).

Table 4 Risk Matrix

	Probability				
Impact	1	2	3	4	5
1	(1)	(2)	(3)	(4)	(5)
2	(2) 1,2	(4)	(6)	(8) 11,12	(10)
3	(3)	(6)	(9)	(12)	(15) 13
4	(4)	(8) 3	(12) 10	(16) 14	(20)
5	(5) 8,9	(10) 4,6,7	(15) 5	(20)	(25)

For ease of use, the table is color-coded to highlight events of similar risk levels:

Green (Risk Values 1-5): Scenarios of lowest risk (4 scenarios)

Blue (Risk Values 6-10): Scenarios of low risk (6 scenarios)

Yellow (Risk Values 11-15): Scenarios of moderate risk (3 scenarios)

Orange (Risk Values 16-20): Scenarios of high risk (1 scenario)

Red (Risk Value 25): Scenarios of highest risk (0 scenarios)

3.8.3 The Importance of Assessment and the Interpretation of Results

The values of the probability (P) and impact (I) that we inserted, were performed in a subjective way. The inserted numbers are considered as relative rankings, rather than absolute values. For example, when a scenario has a probability value of “three”, means that is more likely to occur than a scenario with a probability value of “two” and less likely to occur than one with a probability value of “four”. The same applies to the impact values.

The list that we prepared, must be used as a hierarchical rank of the scenarios, in order to give priority in planning, training and testing. All of them are serious scenarios and must be confronted, but with an order from scenarios with higher probability and impact to scenarios with lower probability and impact.

4 Conclusions

Immediately after the 11 September 2001, the internationally community understood that is liable to being attacked since the use of commercial airliners as terrorists' weapon of choice, made clear that terrorists have the ability to use unconventional means to take advantage of potential weakness in a state's security. The attacks revealed the potential fragility of the transportation systems, which could possibly lead to a breakdown of the global trade system, made clear that terrorists' strategy started to alter towards economic targets and proved that ordinary means of transportation can be transformed into lethal weapons. The maritime realm is one area that rises serious concerns because its ungoverned, its ports and facilities are difficult to secure and is to a high degree open to attacks. The advent of September 11, 2001 rose worries within the maritime domain concerning the possibility for terrorist actions against ships, port facilities by using ships as weapons approximately in the same way that airplanes were used as weapons.

At first, there were expressed fears that the terrorists would made use of piracy sea tactics in order to achieve successful attacks at sea. However, implementing attacks in the maritime environment is an option that presents so many problems that the majority of terrorist groups probably would prefer an equivalent act on land. The main worries for states, global organizations and major shipping interests around the world then shifted to a potential conflation and the tactical nexus between piracy and terrorism. The fear which exists is that terrorist groups by working together or by subcontracting out missions to pirates, will finally manage to overcome the operational constraints in the maritime environment. However, any suggestion of possible nexus between them should be viewed with caution. There is no evidence that they have a collusion or that they will because there exists a very thin line between piracy and terrorism. Consequently, because of the fact that a possible nexus between piracy and terrorism is not easy to occur and at the same time there are so many obstacles that prevent terrorist groups from succeed in their operations, terrorists will try to continually advance their methods in order to achieve their goals by overcoming these barriers. Therefore, it is critical for the terrorists to adjust their tactics, modus operandi and sometimes even their weapon systems. The terrorist groups that would be more sophisticated, will exploit the dependence on electronic means of commerce and communication with virtual attacks, involving anonymous cyber assaults so as to accomplish their efforts.

Recent recorded cases of successful cyber-attacks on ports (the attacks in Antwerp), critical infrastructures (oil rig in the Gulf of Mexico) and single ships (GPS spoofing attacks) require the domain's full attention. The obvious weaknesses of established maritime traffic and communications systems offer great opportunities for malicious actors and highlight present vulnerabilities. Only a coordinated effort by states and civil society decision makers can increase international maritime safety and security standards by imposing norms relating to cyber-conflict and a consensus as to how these norms should apply to address the looming threat of cyber-attacks to maritime trade and commerce. In the future, companies in the maritime domain as well as states should establish preventative actions, countermeasures and procedures to protect critical infrastructure and ships. This can only be achieved if an appropriate risk awareness culture is promoted and cultivated to fit the special challenges posed by cyberspace and the digital information age.

References

Agnihotri, K. K. (2012). Protection of Trade and Energy Supplies in the Indian Ocean Region. *Maritime Affairs: Journal of the National Maritime Foundation of India* , 13-30.

Allianz. (2015). *Safety and Shipping Review 2015.* Munich, Germany: Allianz Global Corporate & Specialty SE.

Allianz. (2016). *Allianz Risk Barometer: Top Business Risks 2016.* Munich: Allianz SE and Allianz Global Corporate & Specialty SE.

Anderson, J. L. (1995). Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 175-199.

Apps, P. (2006, June 18). *Sri Lanka, Tigers Claim Victory in Naval Clash.* Retrieved from NZ Herald: New Zealand: http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=10387114

Benjamin, D., & Simon, S. (2003). *The Age of Sacred Terror: Radical Islam's War Against America.* New York: Random House Trade Paperbacks.

BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO. (2016). *The Guidelines on Cyber Security onboard Ships.* Bagsvaerd, Denmark: BIMCO.

Bohn, M. K. (2004). *The Achille Lauro Hijacking: Lessons in the Politics and Prejudice of Terrorisms .* Dulles, Virginia: Brassey's.

Broder, J. M. (2004, July 27). *At Nation's Ports, Cargo Backlog Raises Security Questions.* Retrieved from New York Times: http://goo.gl/qttk0H

Brookes, P. (2009). The Challenges of Modern Piracy. In M. R. Haberfeld, & Agostino Von Hassell, *Modern Piracy and Maritime Terrorism: The Challenge of Piracy for the 21st Century* (pp. 177-203). Dubuque: Kendall Hunt.

Chalk, P. (2000). *Non-Military Security and Global Order: The Impact of Extremism, Violence and Chaos on National and International Security.* London: Macmillan.

Chalk, P. (2002). *Threats to the Maritime Environments: Piracy and Terrorism.* Santa Monica: RAND Corporation.

Chalk, P. (2006). Maritime Terrorism in the Contemporary Era: Threat and Potential Future Contingencies. *The MIPT Terrorism Annual, 2006*, 21.

Chalk, P. (2008). *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States.* Santa Monica: RAND Corporation.

Chew, F. (2005). Piracy, Maritime Terrorism and Regional Interests. *Geddes Papers 2005*, 73-88.

Conybeare, J., & Sandler, T. (1993). State-Sponsored Violence as a Tragedy of the Commons: England's Privateering Wars with France and Spain. *Public Choice, 77*, 879-897.

Corbett, J. S. (1988). *Some Principles of Maritime Strategy.* Annapolis: Naval Institute Press.

Cowie, T. (2015). *Maritime Insurance Cyber Security - Framing the Exposure.* Zurich: Swiss RE.

Crenshaw, M. (1981). The Causes of Terrorism. *Comparative Politics, 13*(4), 394. doi:10.2307/421717

CSCAP. (2001, 1 1). *Council for Security Cooperation in the Asia Pasific.* Retrieved 2016, from www.cscap.org: http://goo.gl/VhDTcJ

CyberKeel. (2014). *Marine Cyberwatch.* Copenhagen: CyberKeel.

CyberKeel. (2014). *Maritime Cyber - Risks.* Copenhagen: CyberKeel.

Davis, A., & Dyryavyy, Y. (2015). *Maritime Cyber Security: Threats and Opportunities.* Manchester: NCC Group.

Daxecker, U. E., & Prins, B. C. (2013). The New Barbary Wars: Forecasting Maritime Piracy. *Foreign Policy Analysis, 11*(1), 1-22. doi:10.1111/fpa.12014

De Nevers, R. (2007). Imposing International Norms: Great Powers and Norm Enforcement. *International Studies Review, 9*(1), 53-80.

Dear, I., & Kemp, P. (2005). *The Oxford Companion to Ships and the Sea.* Oxford: Oxford University Press.

ENISA. (2011). *Analysis of Cyber Security Aspects in the Maritime Sector.* Heraclion, Greece: European Network and Information Security Agency. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

ESC. (2015). *Maritime Cyber Security White Paper: Safeguarding Data Through Increased Awareness.* Tallinn, Estonia: ESC Global Security. Retrieved from http://www.escgs.com/services/cyber-security/white-papers

Fitton, O., Prince, D., Lacy, M., & Germond, B. (2015). *The Future of Maritime Cyber Security.* Lancaster: Lancaster University. Retrieved from http://eprints.lancs.ac.uk/id/eprint/72696

Fursdon, E. (1996). Sea Piracy - or Maritime Mugging? *INTERSEC, 6*(5), 166.

GAO. (2012). *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage.* Washington: United States Government Accountability Office.

GAO. (2014). *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity.* Washington: United States Government Accountability Office.

Gray, C. S. (Winter 1995-96). On Strategic Performance. *Joint Force Quarterly*(10), 30-36.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). *Maritime Terrorism: Risk and Liability.* Santa Monica: RAND Corporation.

Haimes, Y., Kaplan, S., & Lambert, J. (2002). Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling. *Risk Analysis, 22*(2), 383-397. doi:10.1111/0272-4332.00020

Hansen, K., & Rahman, A. (2014). *Cyber Threat to Ships - Real but Manageable.* Billingstad, Norway: The ABB Group. Retrieved from https://library.e.abb.com/public/b9d267b4767c582f85257ca1003280e9/106_Cyber_threat_to_ships_real_but_manageable.pdf

Herbert - Burns, R., Bateman, S., & Lehr, P. (2009). *Lloyd's MIU Handbook of Maritime Security.* New York: Auerbach Publications, Taylor & Francis Group.

Herbert-Burns, R. (2004). Drawing the Line Between Piracy and Maritime Terrorism. *Jane's Intelligence Review, 16*(9), 30-35.

Hoffman, B. (1998). *Inside Terrorism.* London & New York: Orion & Columbia University Press.

Hoffman, B. (2002). Rethinking Terrorism and Counterterrorism Since 9/11. *Studies in Conflict & Terrorism, 25*(5), 303-316. doi:10.1080/105761002901223

Hong, N., & Ng, A. (2010). The International Legal Instruments in Addressing Piracy and Maritime Terrorism: A critical Review. *Research in Transportation Economics, 27*(1), 51-60. doi:10.1016/j.retrec.2009.12.007

Howarth, S. (1991). *To Shining Sea: A History of the United States Navy 1775-1998.* Norman: University of Oklahoma Press.

IMO (International Maritime Organization). (2016, July 3). *International Maritime Organization*. Retrieved from www.imo.org: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx

Jesus, J. (2003). Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects. *The International Journal of Marine and Coastal Law, 18*(3), 363-400. doi:10.1163/092735203770223585

Joubert, L. (2013). The Extent of Maritime Terrorism and Piracy: A Comparative Analysis. *Scientia Militaria - South African Journal of Military Studies, 41*(1), 111-137. doi:10.5787/41-1-1055

Kaplan, S., & Garrick, J. (1981). On the Quantitative Definition of Risk, Risk Analysis. *Risk Analysis, 1*(1), 11-27. doi:10.1111/j.1539-6924.1981.tb01350.x

Lehr, P. (2007). *Violence at Sea: Piracy in the Age of Global Terrorism.* London: Routledge.

MARSH. (2014). *The Risk of Cyber-Attack to the Maritime Sector.* London: MARSH LLC.

Masala, C., & Tsetsos, K. (2015, October 1). A Demanding Challenge for the Maritime Industry. *Look-Out 2016 Maritime Domain Cyber: Risks, Threats and Future Perspectives*, pp. 11-26.

Menefee, S. P. (1986). Terrorism at Sea: The Historical Development of an International Legal Response. In B. Paritt, *Violence at Sea: An International Workshop in Maritime Terrorism* (pp. 191-220). Paris: International Chamber of Commerce.

Michel, C. D., Thomas, P. F., & Tucci, A. E. (2015). *Cyber Risks in the Maritime Transportation System.* Washington: US Coast Guard.

Murphy, M. (2006). Maritime Threat: Tactics and Technology of the Sea Tigers. *Jane's Intelligence Review*, 6-10.

Murphy, M. N. (2007). Contemporary Piracy and Maritime Terrorism: The Threat to International Security. *The Adelphi Papers, 47*(388), 7-108.

Murphy, M. N. (2008). *Small Boats, Weak States, Dirty Money: Piracy and Maritime Terrorism in the Modern World.* New York: Columbia University Press.

Nadelmann, E. A. (1990). Global Prohibition Regimes: The Evolution of Norms in International Society. *International Organization, 44*(4), 479-526.

Nelson, E. S. (2012). Maritime Terrorism and Piracy: Existing and Potential Threats. *Global Security Studies, 3*(1), 15-27.

Ng, A., & Gujar, G. C. (2008). Port Security in Asia. In W. K. Talley, *Maritime Safety, Security and Piracy* (pp. 257-278). London: Taylor & Francis.

Nincic, D. N. (2005). The Challenge of Maritime Terrorism: Threat Identification, WMD and Regime Response. *Journal of Strategic Studies, 28*(4), 619-644. doi:10.1080/01402390500301020

Nordell, D. (2015). *Cyber and Technology Threats to the Tanker Industry.* London: CSCSS (Centre for Strategic Cyberspace and Security Science).

Panda, R. (2009). *Piracy, Maritime Terror and Policy Response.* New Delhi: Institute for Defense Studies and Analysis (IDSA).

Pelkofski, J. (2005, December). Before the Storm: Al-Qaeda's Coming Maritime Campaign. *U.S. Naval Institute Proceedings, 131*(12), 20-24.

Ranstorp, M., & Wilkinson, P. (2005, 2 23). Introduction. *Terrorism and Political Violence, 17*(1-2), 3-8. doi:10.1080/09546550590520500

Raymond, C. Z. (2006). Maritime Terrorism in Southeast Asia: A Risk Assessment. *Terrorism and Political Violence, 18*(2), 239-257. doi:10.1080/09546550500383225

Rediker, M. (2004). *Villains of All Nations: Atlantic Pirates in the Golden Age.* Boston: Beacon Press.

Richardson, L. (2007). *What Terrorists Want: Understanding the Enemy, Containing the Threat.* New York: Random House Publishing Group.

Richardson, M. (2004). *A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction.* Singapore: ISEAS–Yusof Ishak Institute.

Ritchie, R. C. (1986). *Captain Kidd and the War Against Pirates.* Cambridge: Harvard University Press.

Ronzitti, N. (1990). *Maritime Terrorism and International Law.* Boston: Kluwer Avademic Publishers.

Rouzer, B. (2015). *Evolving Cyber Threats to the Marine Transportation System.* Washington: US Coast Guard.

Santamarta, R. (2014). *A Wake-up Call for SATCOM Security.* Seattle: IOActive.

Sinai, J. (2004). Future Trends in Worldwide Maritime Terrorism. *The Quarterly Journal, 3*(1), 49-66. doi:10.11610/connections.03.1.05

Tomberlin, R. L. (2009). Terrorism's Effect on Maritime Shipping. In M. R. Haberfeld, & Agostino von Hassell, *Modern Piracy and Maritime Terrorism: The Challenge of Piracy for the 21st Century* (pp. 53-63). Dubuque: Kendall Hunt.

Truver, S. C. (2007, April 1). *Mines, Improvised Explosives: A threat to Global Commerce.* Retrieved from National Defence Magazine: http://www.nationaldefensemagazine.org/archive/2007/April/Pages/Minesimprovided2678.aspx

US Department of Defence. (2010). *Joint Publication (JP) 3-07.2 - Antiterrorism.* Washington: US Department of Defence. Retrieved August 2016, from http://www.dtic.mil/doctrine/

Wildemann, P. (2015, September 23). *Cyber-Risk in Marine Transportation.* Washington: FTI Consulting.

Wilhoit, K., & Balduzzi, M. (2013, October 15). *Vulnerabilities Discovered in Global Vessel Tracking Systems.* Retrieved from Security Intelligence Blog 2013: http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-discovered-in-global-vessel-tracking-systems/

XL Group. (2013). *Enviromental Risks: Cyber Security and Critical Industries.* St. Stephen’s Green, Dublin: XL Group plc. Retrieved from http://goo.gl/JcYicM

Appendix A

Maritime Piracy

This Appendix examines maritime piracy. We begin by giving some definitions about maritime piracy, citing a short history of maritime piracy through ages, analyzing the types of the contemporary piracy and discussing some data of the contemporary piracy. We then briefly analyzing the factors underscoring and contribute to piracy, listing the dangers lurking and finally evaluating the challenges of piracy.

A.1 Definitions

Piracy, generally speaking, is nothing else but an illegal act of attacking at sea. While Anderson (1995) defines piracy as "a subject of violent maritime predation in that it is not part of a declared or widely recognized war", Kenny (1936), a British jurist who inspired Anderson, talks about "any armed violence at sea which is not a lawful act of war". The United Nations Convention on the Law of the Sea of 1982 (UNCLOS) gives a narrower and more circumscribed definition which is used frequently by the International Maritime Organization (IMO):

a. any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

   i. on the high seas, against another ship or aircraft, or against persons or property on board such 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 it a pirate ship or aircraft.

In this dissertation the broader definition of IMB is preferred. According to IMB "Piracy is an act of boarding or attempting to board any ship with the apparent intent to commit theft or any other crime and with the apparent intent or capability to use force in furtherance of that act" (International Maritime Bureau).

A.2 Short History of Piracy and the Types of Contemporary Piracy

Piracy in not the dazzling images and beautified stories we watch in the movies and read in the books, although containing a grain of truth in them. The history of piracy begins from ancient times back to the Phoenicians and ends today (Daxecker & Prins, 2013, p. 2-3). However, the increasingly favorable conditions that allowed ships to travel on the high seas, without adequate safety measures, dramatically increased piracy incidents. Piracy became a lucrative business that progressively flourished, sometimes even with the blessing of the great powers of the time (Nadelmann, 1990). Thus, became a useful weapon in the hands of local leaders, in exchange for a share of the spoils (Conybeare & Sandler, 1993).

Howarth (1991) argues that pirates were a plague and while the British was able to protect their trade sea lanes, most countries were not. Seventeenth and eighteenth centuries were piracy's zenith (Dear & Kemp, 2005). But as a response to this increase, states and their political elites tried to delegitimize criminality on global seas and to eradicate piracy with their naval power (Ritchie, 1986; Rediker, 2004; De Nevers, 2007). Piracy almost disappeared, especially after its sponsors close down safe ports (Nadelmann, 1990; Lehr, 2007) but in the late 80s started to rise again. Today piracy is on the rise and constitute a significant threat because can impose civilian casualties, economic harm and even an environmental disaster.

There are three main types of piracy according to IMB. The low-end, the medium-level and the high-end. Talking about low-end piracy means attacks that exploiting soft security measures at many ports and taking place at harbors. These attacks which are characterized as low-level armed robbery, are happening usually next to land, by common maritime criminals, who generally steal cash and valuable items, with the use of small arms like knives, driving small high-speed vessels (Chalk, 2000; Chalk, 2008).

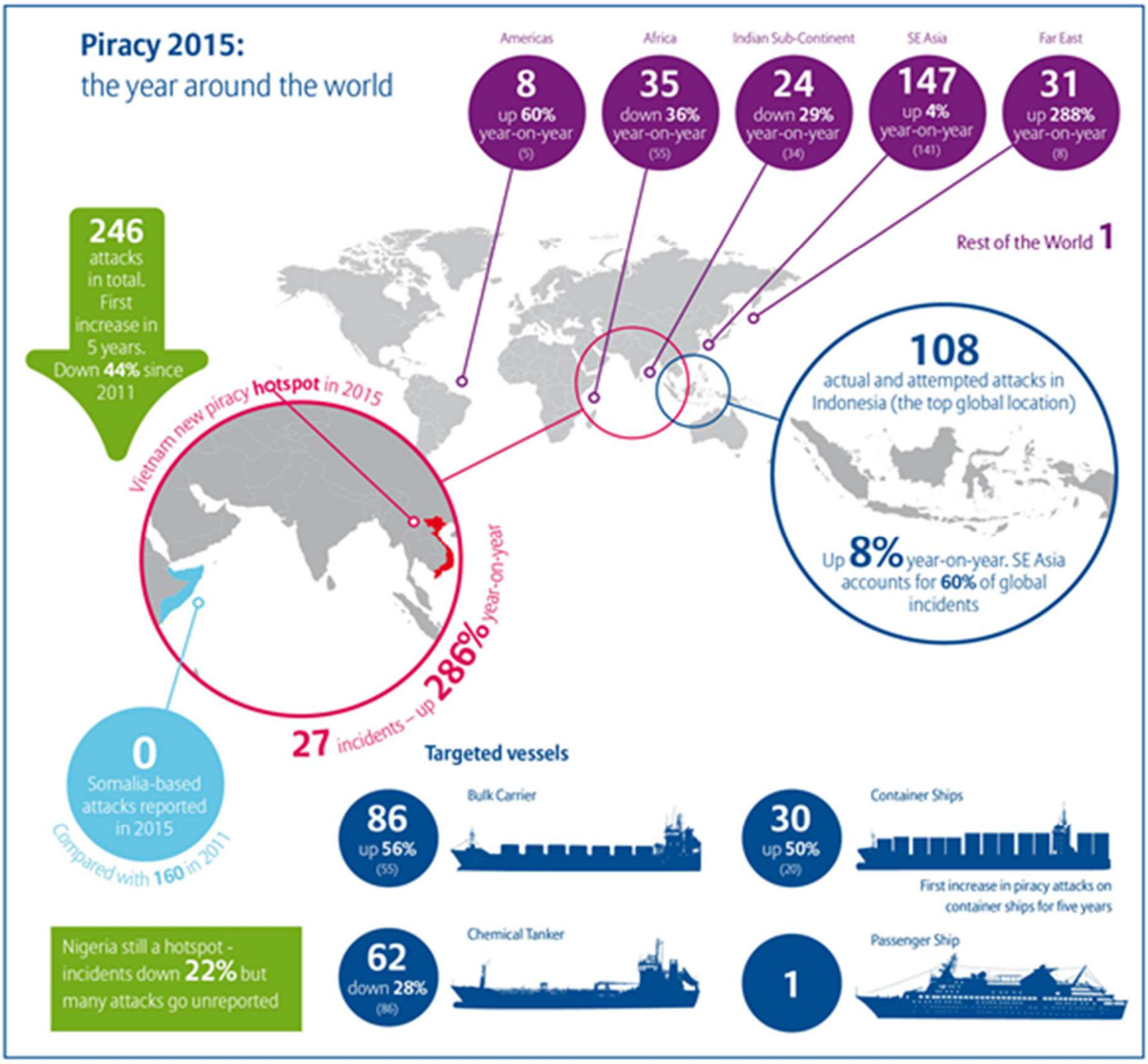
As concern medium-level attacks which are medium-level armed robberies, these are a more serious type of attacks which included looting and robbery of ships, serious injury or murder of the crew of the attacked vessels by violent thefts, gangs or organized syndicates who operate from a “mother ship” with the use of contemporary arsenal (Chalk, 2000; Chalk, 2008).

Finally, the last type of piracy includes the completely theft of vessels and then their conversion to another type of ship for illegal trading. The high end type consists by major criminal assaults, by heavily armed syndicates, well-resourced and thoroughly planned, in conjunction with land based operatives (Chalk, 2000; Chalk, 2008).

A.3 Contemporary Maritime Piracy

A total of 246 actual or attempted pirate incidents were registered around the world in 2015, increased compared with 2014 as reported by the International Chamber of Commerce's International Maritime Bureau (IMB) annual piracy report. According to AGCS's Safety Shipping Review for 2016, which focuses on key developments in maritime safety and analyzes shipping losses (of over 100 gross tons) during the 12 months prior to December 31, 2015, the centralization of pirate attacks remains great in

Southeast Asia, particularly in the waters around South China, Indochina, Indonesia, Philippines and Vietnam as a new hotspot, which accounted for almost 60% of all global incidents occurred during 2015 (Images A.1-A.2).



Source: Allianz Global Corporate & Specialty Safety & Shipping Review 2016

Figure 11 Annual Piracy Report for 2015 by IMB (Source: Allianz Global Corporate & Specialty Safety & Shipping Review 2016)

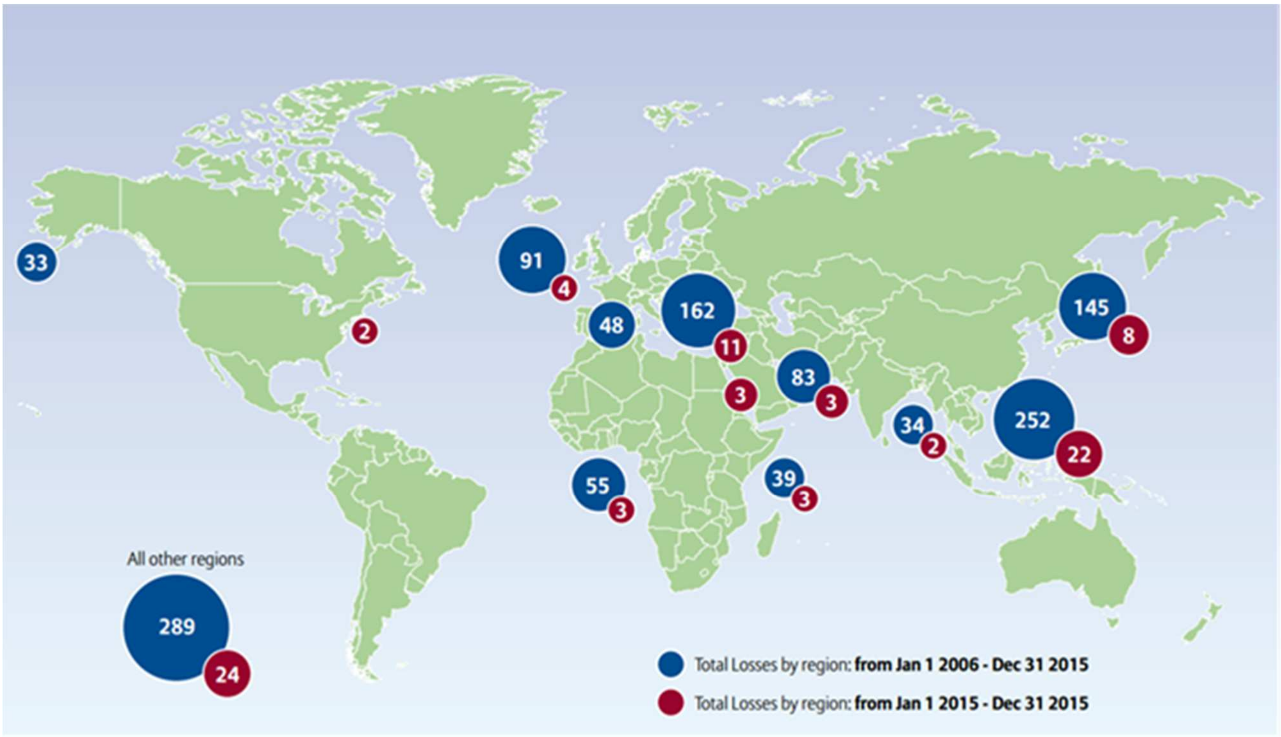

33
91
4
2
48
162
11
3
83
3
145
8
34
2
252
22
55
3
39
3
All other regions
289
24
● Total Losses by region: from Jan 1 2006 - Dec 31 2015
● Total Losses by region: from Jan 1 2015 - Dec 31 2015

Figure 12 Total Losses by Region in AGCS's Safety Shipping Review for 2016 (Source: Lloyd's List Intelligence Casualty Statistics. Data Analysis & Graphic: Allianz Global Corporate & Specialty)

A.4 Factors that Contribute to Piracy, Dangers and Challenges of Piracy

As reported by Lehr (2007) the reemergence of piracy in the late 1980's emanated from two incidents in the broadest sense of the word. In the first place the end of the Cold War which marked by the end of the support and the decrease of the political control of superpowers to inferior states. This in turn weakened state's ability for adequate maritime security. Simultaneously the globalization has brought a rapid increase in international business and trade in particular through the sea routes.

Although Lehm only mentions two broader factors, Chalk (2008) argues that the inception of maritime piracy nowadays occurs partly as a result of seven factors. At first the extensive increase in commercial maritime traffic and as a consequence the crowded sea lanes in combination with the large number of ports globally, offer pirates a wide range of charmed options. Second because of the nature of the chokepoints where ships become vulnerable as they reduce their speed, increase the danger of an attack. Third, the Asian financial crisis transformed many people to pirates and constrained the funding for the monitoring of many coastlines. Fourth, as a consequence of 11 September the difficulties of maritime surveillance grew substantially and furthermore increased the funds for land based homeland surveillance. Fifth, low level coastal and port-side piratical activity grew up as a result of soft security measures. Sixth, corruption in all levels even in high-level officials combined with failed states. And last but not least the development of new and sophisticated methods of pirate attacks because of the global proliferation of small arms.

The dangers and the consequences of contemporary piracy, as Chalk (2008) writes, are many and can be analyzed in four levels which are basic, economic, political and environmental. The direct threat of innocent lives or the well-being of the citizen of different countries constitute the basic level. Secondly, the enormous economic impact because of the repeated frauds, stolen cargos, delayed trips and energy losses. High-level official's corruption can sap regime legitimacy so piracy is playing a vital political role. Finally, pirates can cause huge environmental disaster if for example destroy an oil tanker.

The huge extent of the surveillance area which consists of open waters, large coastlines and enormous distances, and as a result the increased reaction time constitute the main challenges for all the efforts against piracy. Apart from the fact that the reasons above prevent the efforts of the navies to arrest pirates at sea, at the same time deficient legal systems permit them to escape the trial. The solution includes the combined efforts of the shipping industry and national navies apace with private security measures in order to deter the pirates (Agnihotri, 2012).

A.5 Link Between Maritime Piracy and Maritime Terrorism

Piracy is a serious threat to global seafaring trade as incidents all over the world are increased. Opposite to this rise, incidents of maritime terrorism have been in the lowest point, over the past ten years. Due to the 9/11 attack in New York, as a more dramatic form of terrorist assault, and the possibility of a nexus between terrorism and piracy, reawakens the fear that an occupied mean, in this case a vessel, could be used either as delivery platform for WMD, either as a weapon itself if it has a hazard cargo (Joubert, 2013).

The possible conflation and the tactical nexus between piracy and terrorism are the main worries for states, global organizations and major shipping interests around the world. The fear which exists is that terrorist groups by working together or by subcontracting out missions to pirates, will finally manage to overcome the operational constraints in the maritime environment (Chalk, 2008). According to Murphy (2008) there are some people in the international community who assume that the two parties will cooperate so as the terrorists learn from pirates how to operate at sea, while Brookes (2009) believes that piracy already provides terrorists funding for ashore and land-based terrorist activities and at the same time there is an ongoing relationship between crime gangs and terrorist groups (Tomberlin, 2009). In the contrary Murphy (2008) and Chalk (2008) argue that there is no supportable and credible evidence of the postulated convergence between maritime piracy and terrorism and such a nexus remains questionable. The possibility pirates and terrorists working together is limited, as the main objectives of the two parties differ (Joubert, 2013). However, the implications of such a specter affect the international stability and it is important to learn if terrorists have acquired the knowledge and the operational "how to" from piracy (Nelson, 2012). Additionally, Nelson (2012) supports that there is an impeding danger, due to the fact that is difficult to distinguish a piracy act from a terrorist attack, to identify by mistake a terrorist assault as a piracy incident.

A.6 Distinction Between Maritime Piracy and Maritime Terrorism

It is important to distinguish between piracy and maritime terrorism and any suggestion of possible nexus between them should be viewed with caution. There is no evidence that they have a collusion or that they will (Murphy, 2008, p. 387). There exists a very thin line between piracy and terrorism and there are certain factors which are drawing this line (Panda, 2009). The distinction is obscure in at least three dimensions: (1) ends, (2) means and (3) effects (Chew, 2005, p. 75). First, in terms of ends, means motives or aim, while piracy is usually driven by financial gain maritime terrorism do so to achieve certain political motivations (Herbert-Burns, 2004, p. 30). However, terrorist groups may conduct operations at sea for the promise of reward in order to fund their political ends through piracy but in a strategic view to remain terrorists. Moreover, aims affects the choise of targets and while terrorists choose ships with a symbolic value, with higher causalties or for a potential use as a weapon, pirates choose vessels according to their value and vulnerability (Nelson, 2012). Secondly, in terms of means, pirates are generally associated with and make use of simple and basic tactics and capabilities, while terrorists are associated with more sophisticated tactics and capabilities (Herbert-Burns, 2004, p. 32). Thirdly, in terms of effects, terrorists usually try to achieve a strategic effect in a more global field in terms of objectives and simultaneously seek attention and publicity, while pirates traditionally confined themselves to the tactical level, in a more local-regional field, trying to avoid attention (Herbert-Burns, 2004; Chew, 2005, p. 75; Nelson, 2012, p. 24). To conclude, piracy and terrorism are not two discrete dimensions but they present a complex piracy-terrorism continuum, as shown in the Diagram 1 (Chew, 2005, p. 75). The grey zone is the “nexus” between piracy and maritime terrorism where certain groups operate.

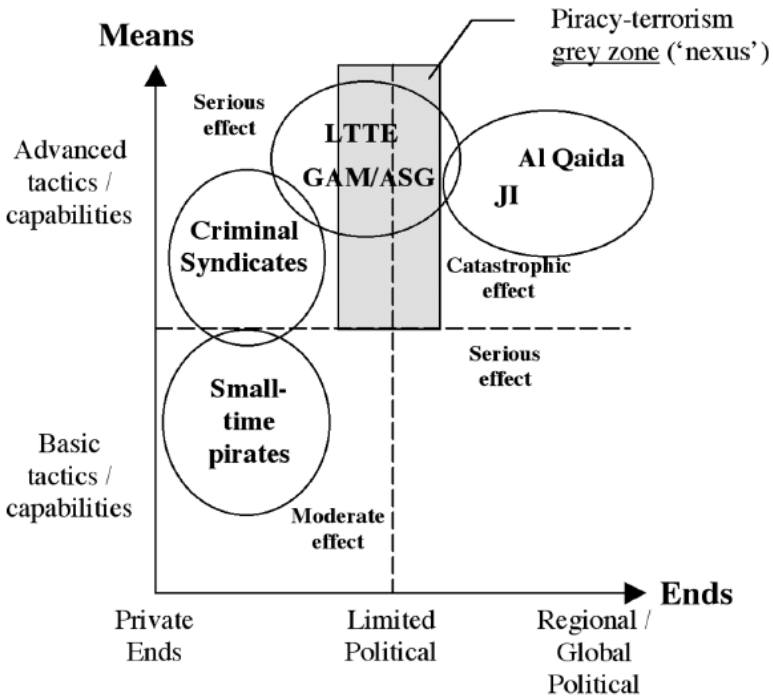


Diagram A.1 2D Piracy - Terrorism Continuum (Source: Chew, 2005:75)

Appendix B

Table B.1 High Profile Maritime Terrorist Incidents, 1961-2004 (Source: Greenberg, Chalk, Willis, Khilko & Ortiz, 2006)

Incident	Group	Deaths	Remarks
Hijacking of Santa Maria (1961)	Portuguese and Spanish rebels	N/A	The Santa Maria, a 21,000-ton cruise ship owned by Companhia Colonial of Lisbon, was hijacked by a group of 70 men led by Captain Henriques Galvao (a Portuguese political exile) to bring global attention to the Estado Novo in Portugal and related fascist regime in Spain. The vessel was on a holiday cruise in the southern Caribbean and its more than 600 passengers were held for 11 days before Galvao formally surrendered to the Brazilian navy. The incident constitutes the first modern-day hijack at sea.
Use of a Cypriot- registered coaster, Claudia, to transport weapons to Ireland (1973)	Provisional Irish Republican Army (PIRA)	N/A	Claudia was intercepted by the Irish Navy while attempting to land a consignment of weapons intended for PIRA. On board were five tons of munitions that included 250 Soviet-made assault rifles, pistols, mines, grenades, and explosives. The vessel was owned by Gunther Leinhauser, a West German arms trafficker, which said that PIRA had given him a “shopping list” of required materiel and that the “order” had been filled by Libya.
Hijacking of Achille Lauro (1985)	Palestine Liberation Front (PLF)	1	Cruise ship hijacked in an attempt to coerce the release of 50 Palestinians being held in Israel. The perpetrators were eventually detained in Sicily. Person killed was Leon Kling-hoffer, a German, wheelchair-bound tourist, who was captured by the world’s media as he was pushed overboard.
Targeting of cruise ships on the Nile River (1992–1994)	Al-Gama’a alIslamiyya	N/A	The group targeted at least four cruise ships during these two years as part of its general effort to undermine the Egyptian tourist sector (a key contributor to the country’s economy).
Hijacking of a Turkish passenger ferry in the Black Sea (1996)	Chechen rebels	N/A	Nine rebel gunmen held 255 passengers hostage for four days during which they threatened to blow up the captured ferry in order to bring international attention to the Chechen cause; the abductors eventually sailed the vessel back to Istanbul where they surrendered.
Suicide bombing of the USS Cole (2000)	Al Qaeda	19	The bombing took place while the Cole was refueling at the Yemeni port of Aden. The assault involved 600 pounds of C4 explosive that was packed into the hull of a suicide attack skiff. Those killed were 17 U.S. sailors, 2 terrorists. In addition to the 17 sailors who were killed, another 39 were injured.

Incident	Group	Deaths	Remarks
Suicide bombing of the M/V Limburg (2002)	Al Qaeda	3	The attack involved a small, fiberglass boat packed with 100–200 kg of TNT rammed into the tanker as it was preparing to take on a pilot-assisted approach to the Ash Shihr Terminal off the coast of Yemen. The Limburg was lifting 297,000 barrels of crude at the time of the strike, an estimated 50,000 of which spilled into the waters surrounding the stricken vessel. Those killed were 1 crewman and 2 terrorists.
Use of Karine A to transport weapons for anti-Israeli strikes (2002)	Palestinian Authority (PA)	N/A	Karine A, a 4,000-ton freighter, was seized in the Red Sea on January 3, 2002. The vessel was carrying a wide assortment of Russian and Iranian arms, including Katyusha rockets (with a 20-kilometer range), antitank missiles (LAW and Sagger), long-range mortar bombs, mines, sniper rifles, ammunition, and more than two tons of high explosives. The US$100 million weapon consignment was linked directly to Yasir Arafat and was allegedly to be used for attacks against Jewish targets in Israel and the Occupied Territories.
Hijacking of the M/V Penrider, a fully laden shipping fuel oil tanker from Singapore to Penang in northern Malaysia (2003)	Gerakan Aceh Merdeka (GAM)	N/A	This is one of the few instances where GAM has directly claimed responsibility for a maritime attack. The group took three hostages (the master, chief engineer, and second engineer), who were eventually released after a $52,000 ransom was paid.
Use of the Abu Hassan, an Egyptian- registered fishing trawler, to transport weapons and training manuals to assist militant strikes in Israel	Lebanese Hezbollah	N/A	The Egyptian owner of the trawler was recruited by Hezbollah and trained specifically to carry out maritime support missions. The vessel, which Israeli naval commandos intercepted 35 nautical miles off Rosh Hanikra near Haifa, was being used to ferry a complex weapon and logistics consignment, consisting of fuses for 122mm Qassam rockets, electronic time-delay fuses, a training video for carrying out suicide strikes, and two sets of CD-ROMs containing detailed bomb-making information.
Attacks against the Khawr Al Amaya oil terminal (KAAOT) and Al Basrah oil terminal (ABOT), Iraq (2004)	Jamaat al-Tawhid	3	The attacks were claimed by al Zarqawi as a follow-up to the 2000 Cole and 2002 Limburg strikes (using the same small-craft, suicide modality) and appeared to be part of an overall strategy of destabilization in Iraq (the terminals were shut down for two days, costing nearly US$40 million in lost revenues).
Bombing of the Philippine SuperFerry 14 (2004)	Abu Sayyaf Group (ASG), combined with elements from Jemaah Islamiyah (JI) and the Rajah Soliaman Revolutionary Movement (RSRM)g	116	Attack involved 20 sticks of dynamite that were planted in a hollowed-out television set. The bomb set off a fire that quickly spread throughout the ship due to the lack of an effective internal sprinkler system. Of the 116 fatalities, 63 have been identified (at the time of writing) and 53 remain unaccounted for. The incident has been listed as the most destructive act of terrorism in maritime history and the fourth most serious international incident since September 11, 2001.
Suicide attack against the Port of Ashdod, Israel (2004)	Hamas, al-Aqsa Martyr's Brigade	10	The attack took place at Ashdod, one of Israel's busiest seaports, and involved two Palestinian suicide bombers from Hamas and the al-Aqsa Martyr's Brigade. The perpetrators had apparently been smuggled to the terminal inside a commercial container four hours before the operation. Some speculation remains that al Qaeda assisted with logistics of the strike.

Appendix C

Definitions

Techniques of Cyber-Attacks

Social Engineering: A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

Phishing: Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that an individual visits a fake website using a hyperlink included in the email.

Mirrored Website / Water Holing: Establishing a fake website or compromising a genuine website in order to exploit visitors.

Malicious Code / Ransomware: Malware which encrypts data on systems until such time as the distributor decrypts the information.

Scanning: Attacking large portions of the Internet at random.

Spear-Phishing: Similar to phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.

Deploying Botnets: Botnets are used to deliver Distributed Denial of Service (DDoS) attacks.

Subverting the Supply Chain: Attacking a company or ship by compromising equipment or software being delivered to the company or ship.

Stages of a Cyber-Attack

Survey / Reconnaissance: Open/public sources used to gain information about a company, ship or seafarer which can be used to prepare for a cyber-attack. Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring the actual data flowing into and from a company or a ship.

Delivery: Attackers may attempt to access company and ship systems and data. This may be done from either within the company or ship or remotely through connectivity with the internet. Examples of methods used to obtain access include:

Company online services, including cargo or consignment tracking systems

Sending emails containing malicious files or links to malicious websites to seafarers

Providing infected removable media, for example as part of a software update to an onboard system, and

Creating false or misleading websites which encourage the disclosure of user account information by seafarers.

Breach: The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack. It should be noted that a breach might not result in any obvious changes to the status of the equipment. Depending on the significance of the breach, an attacker may be able to:

Make changes that affect the system's operation, for example interrupting the display of chart information on ECDIS

Gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists

Achieve full control of a system, for example a machinery management system.

Affect: The motivation and objectives of the attacker will determine what affect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

Access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access

Manipulate crew or passenger lists, or cargo manifests. This may be used to allow the fraudulent transport of illegal cargo

Disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.

Onboard Systems

Cargo Management Systems: Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore. Such systems may include shipment-tracking tools available to shippers via the internet. Interfaces of this kind make cargo management systems and data in cargo manifests vulnerable to cyber-attacks.

Cargo Control Room (CCR) and its equipment

Level Indication System

Valve Remote Control System

Water Ingress Alarm System

Ballast Water Systems

Gas liquefaction.

Bridge Systems: The increasing use of digital, networked navigation systems, with interfaces to shore side networks for update and provision of services, make such systems vulnerable to cyber-attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks. A cyber incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

Positioning systems (GPS, etc.)

Electronic Chart Display Information System (ECDIS)

Dynamic Positioning (DP) systems

Systems that interface with electronic navigation systems and propulsion/maneuvering systems

Automatic Identification System (AIS)

Global Maritime Distress and Safety System (GMDSS)

Radar equipment

Voyage Data Recorders (VDRs)

Other monitoring and data collection systems.

Propulsion and Machinery Management and Power Control Systems: The use of digital systems to monitor and control onboard machinery, propulsion and steering make such systems vulnerable to cyber-attacks. The vulnerability of such systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

Engine governor

Power management

Integrated control system

Alarm system

Emergency response system.

Access Control Systems: Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic “personnel-on-board” systems.

Surveillance systems such as CCTV network

Bridge Navigational Watch Alarm System (BNWAS)

Shipboard Security Alarm Systems (SSAS)

Electronic “personnel-on-board” systems.

Passenger Servicing and Management Systems: Digital systems used for property management, boarding and access control may hold valuable passenger related data.

Property Management System (PMS)

Medical records

Ship passenger/seafarer boarding access systems

Infrastructure support systems like Domain Naming System (DNS) and user authentication/authorization systems.

Passenger Facing Public Networks: Fixed or wireless networks connected to the internet installed on board for the benefit of passengers, for example guest entertainment systems. These systems should be considered as uncontrolled and should not be connected to any safety critical system on board.

Passenger Wi-Fi or LAN internet access

Guest entertainment systems

Communication.

Administrative and Crew Welfare Systems: Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email. They can be exploited by cyber attackers to gain access to onboard systems and data. These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

Administrative systems

Crew Wi-Fi or LAN internet access, for example where seafarers can connect their own devises.

Communication Systems: Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defense mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data.

Satellite communication equipment

Voice Over Internet Protocols (VOIP) equipment

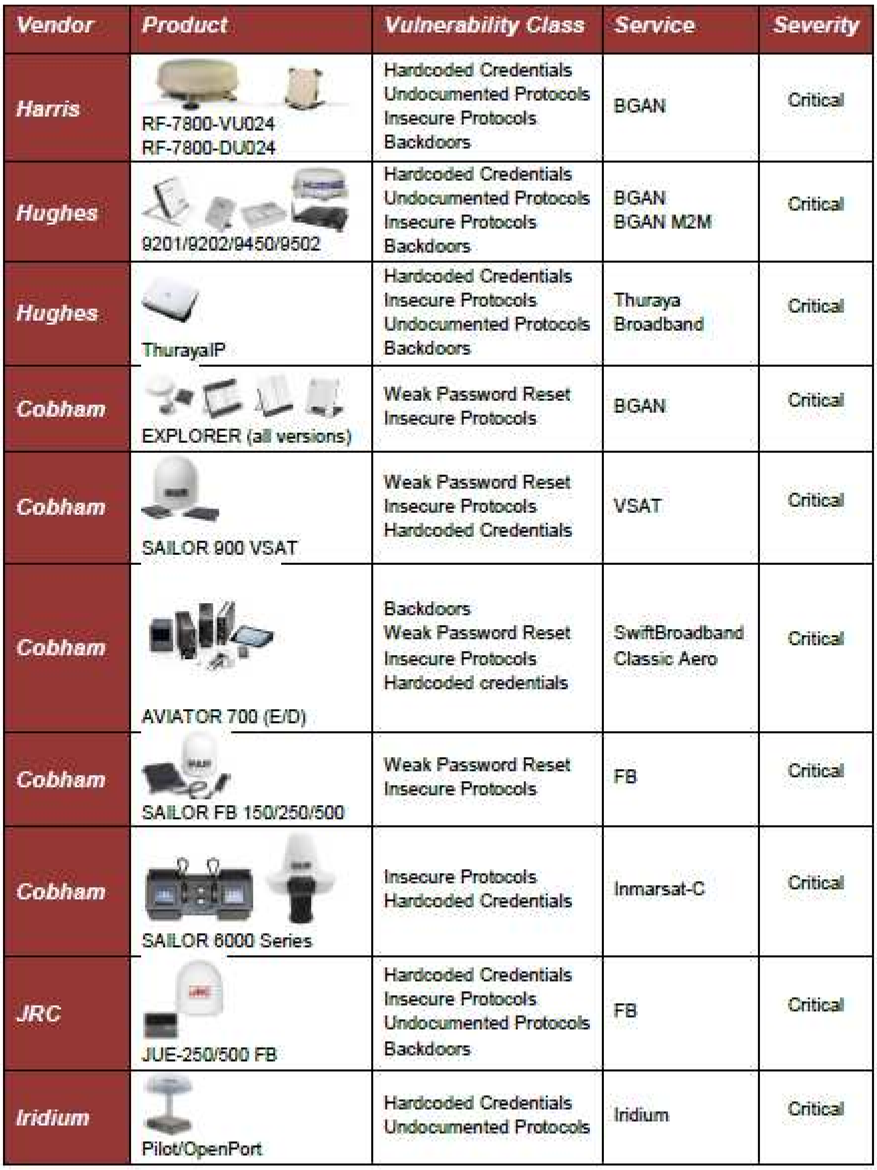
Wireless networks (WLANs)

Public address and general alarm systems.

(All the above definitions retrieved from BIMCO, CLIA, ICS, INTERCARGO, & INTERTANKO, 2016)

Vulnerable Satellite Equipment

Table C.1 Vulnerable Satellite Equipment (Source: IOActive, 2014, p. 7)



Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Appendix D

Threat Scenarios List

The list includes some identified threats. Also included is a rating of the probability of the event occurring (P) and its impact (I), should the event occur. Both are coded on a scale of 1 to 5, five being more probable/higher impact.

Table D.1 Threat Scenario List

#	Event	P	I	RV
1	Attack ship's navigation systems and cause a crash in port: This is a scenario where the ship thinks it is in a position according to latitude and longitude that is false. It could cause a collision, but that is not highly probable.	1	2	2
2	Attack ship's navigation systems and cause a crash in a terminal: This is a scenario where the ship think it is in a position according to latitude and longitude that is false. It could cause a collision, but that is not highly probable.	1	2	2
3	Attack ship's navigation systems to use it to ram another ship in port, cause traffic jam. If the one which is rammed carrying DMC, could cause a serious explosion.	2	4	8
4	Attack ship's navigation systems, one carrying WMD, which explodes as rammed into another ship in port, to cause a traffic jam in port. Depending on the size and the amount of WMD it carries, the damage could be significant.	2	5	10
5	Attack cruise ship's navigation systems and cause a crash. The destruction could cause mass casualties.	3	5	15
6	WMD/DMC in container explodes remotely, sinks ship at entrance to port: The damages from such a scenario varies from port to port.	2	5	10
7	WMD/DMC in container explodes remotely, sinks ship at entrance to port: This scenario has the objective of destroying terminal facilities.	2	5	10
8	Attack ship's access control systems. Missile fired from one ship to the port.	1	5	5
9	Attack ship's access control systems. Missile fired from one ship to another in port.	1	5	5
10	Attack ship's bridge systems of an oil tanker, cause oil spill. The spill caused could be disastrous, taking many days to clean up and closing down a harbor.	3	4	12
11	Cyber-attack to disrupt vessel traffic service, possibly stop port traffic. Easily to be executed, but without great damage.	4	2	8
12	Cyber-attack to disrupt terminal operating system. Easily to be executed, but without great damage.	4	2	8
13	Cyber-attack to disrupt cargo management systems. Smuggle weapons, explosive devices and terrorists in containers to attack from within terminal. The destructiveness of this scenario depends on the amount and the type of weapons that are smuggled.	5	3	15
14	Attack ship's or ports' passenger servicing and managements systems to allow terrorists in, as port security inspection team. Unlimited access to terrorists anywhere on the terminal and surrounding vessels. They might smuggle in an explosive device and/or weapons.	4	4	16